10400 Detrick Avenue
Kensington, MD 20895-2484
(240) 627-9425

ADMINISTRATIVE AND REGULATORY COMMITTEE

May 16, 2022
4:00 p.m.
YouTube Link: https://youtu.be/jhxUYNEslWk

Approval of Minutes:

Action Items:

Date Posted: May 13, 2022

Minutes

HOUSING OPPORTUNITIES COMMISSION OF MONTGOMERY COUNTY
10400 Detrick Avenue
Kensington, Maryland 20895
(240) 627-9425

Administrative and Regulatory Committee Minutes

March 21, 2022

For the official record of the Housing Opportunities Commission of Montgomery County, an open meeting of the Administrative and Regulatory Committee was conducted via an online platform and teleconference on Monday, March 21, 2022, with moderator functions occurring at 10400 Detrick Avenue, Kensington, Maryland beginning at 4:00 p.m. There was a livestream of the meeting held on YouTube, available for viewing here . Those in attendance were:

Present
Frances Kelleher, Chair – Administrative and Regulatory Committee
Pamela Byrd – Commissioner

Absent
Linda Croom – Commissioner

Also Attending

Kayrine Brown, Acting Executive Director
Darcel Cox
Elliot Rule
Billy Buttrey
Rita Harris
Heather Grendze, Associate General Counsel
Lynn Hayes
Timothy Goetzinger
Jessie Joseph

IT Support
Aries Cruz, IT Support

Commission Support
Patrice Birdsong, Spec. Asst. to Commission

APPROVAL OF MINUTES

The minutes of the February 24, 2022 Administrative and Regulatory Committee meeting was approved upon a motion by Commissioner Byrd and seconded by Commissioner Kelleher. Affirmative votes were cast by Commissioners Kelleher and Byrd. Commissioner Croom was necessarily absent and did not participate in the vote.

DISCUSSION/ACTION ITEMS

1. **Public Housing Agency Plan (PHA):** Authorization to Submit the Fiscal Year 2023 Annual Public Housing Agency Plan

Elliot Rule, Management Compliance Analyst, provided an overview requesting the Administrative and Regulatory Committee to recommend to the full Commission authorization of the Acting Executive Director, or her designee, to submit the Fiscal Year 2023 (FY'23) Annual Public Housing Administrative Plan to the Department of Housing and Urban Development (HUD).

Staff addressed Commissioners questions. A motion was made by Commissioner Byrd and seconded by Commissioner Kelleher, to recommend to the full Commission, at the April 6, 2022 meeting, approval of the updates to the Public Housing Plan for submission to HUD. Affirmative votes were cast by Commissioners Kelleher and Byrd. Commissioner Croom was necessarily absent and did not participate in the vote.

2. **Violence Against Women Act (VAWA):** Authorization to Submit Proposed Revisions to HOC's Violence Against Women Act Policy and Related Revisions to the Housing Choice Voucher Administrative Plan

Elliot Rule, Management Compliance Analyst, provided an overview requesting the Administrative and Regulatory Committee to recommend to the full Commission to adopt the proposed revisions to HOC's Violence Against Women Act (VAWA) Policy, and related revisions to the Housing Choice Voucher Plan.

Staff addressed questions of the Commissioners. A motion was made by Commissioner Byrd and seconded by Commissioner Kelleher to recommend that the Commission, at the April 6, 2022 monthly meeting, to adopt the proposed revisions to HOC's Violence Against Women Act Policy and related revisions to the Housing Choice Voucher Administrative Plan. Affirmative votes were cast by Commissioners Kelleher and Byrd. Commissioner Croom was necessarily absent and did not participate in the vote.

3. **Housing Choice Voucher Administrative Plan:** Approval of Revisions to Chapter 2, 10, and 11 of the HOC Housing Choice Voucher (HCV) Administrative Plan and Authorization for the Acting Executive Director to Implement the Revisions

Darcel Cox, Chief Compliance Officer, introduced Jessie Joseph, Management Compliance Analyst, who provided an overview of the request to the Administrative and Regulatory Committee to recommend to the full Commission the adoption of the proposed revisions to HOC's Administrative Plan's Table of Content, Chapters 2, 10 and 11, governing the Housing Choice Voucher Program.

A motion was made by Commissioner Byrd and seconded by Commissioner Kelleher to recommend that the Commission, at the April 6, 2022 monthly meeting, adopt the proposed revisions to HOC's Housing Choice Voucher Administrative Plan. Affirmative votes were cast by Commissioners Kelleher and Byrd. Commissioner Croom was necessarily absent and did not participate in the vote.

A motion was made by Commissioner Byrd and seconded by Commissioners Kelleher to adjourn the meeting. Affirmative votes were cast by Commissioners Kelleher and Byrd. Commissioner Croom was necessarily absent. The adjourned at 4:31 p.m.

Respectfully submitted,

Kayrine Brown
Acting Secretary-Treasurer

/pmb

Deliberation and/or Action

M E M O R A N D U M

TO: Housing Opportunities Commission of Montgomery County
Administrative and Regulatory Committee

VIA: Kayrine V. Brown, Acting Executive Director

FROM:

Staff: David Brody	Division: Information Technology	Ext. 9449
Irma Rodriguez	Division: Information Technology	Ext. 9415
Karlos Taylor	Division: Information Technology	Ext. 9454

RE: Presentation and Discussion of HOC's Response to Management Letter Comments in the FY 2021 Audited Financial Statements

DATE: May 16, 2022

STATUS: **Consent _____ Deliberation ___X___ Status Report____ Future Action_____**

OVERALL GOAL & OBJECTIVE:

To respond to and address comment by HOC's auditors, CliftonLarsonAllen, LLP ("CLA") during the completion of the fiscal year 2021 audited financial statements for which CLA identified a deficiency in internal control that did not rise to the level of a significant deficiency or material weakness. CLA viewed this as an opportunity to strengthen HOC internal controls and improve the efficiency of IT operations.

BACKGROUND:

CliftonLarsonAllen, LLP delivered Unqualified Audited Financial Statements for fiscal year 2021 and the Commission approved them at its meeting on November 3, 2021. Though unqualified, CLA issued a Management Letter, which identified deficiencies and provided recommendations to strengthen internal controls for Information Technology operations.

For your reference and discussion are the following attachments:

I. CLA Management Letter;
II. HOC Cyber Incident Response Plan to respond to Disaster Recovery/Business Continuity Plan; and
III. Information Technology Strategic Plan;
IV. Data Classification Guidelines.

Attachment I: CLA Management Letter Comments.

The Management Letter contained four bulleted comments. Management responded by resolving two of the four items and a detailed summary of staff's initial response were included with the final audited financial statements. The first addressed outdated operating system upgrade, which was remediated by upgrading or removing obsolete workstations from use. The second committed to review user access and termination on a monthly basis to ensure that no terminated employees remained active on the network.

Attachment II: HOC Cyber Incident Response Plan to respond to Disaster Recovery/Business Continuity Plan

The HOC Cyber Incident Response Plan will act as a guide and framework for responding to significant cyber security incidents. Additionally, the document defines those who will be responsible to manage and mitigate such incidents.

A cyber incident response plan is a critical component of an organization-wide disaster recovery/business continuity plan. Given the rising incidence of cyberattacks, such as malicious code or viruses and ransomware, it is vital for IT departments to be able to identify, investigate and mitigate these incidents swiftly and efficiently in order to protect data and maintain business operations.

The primary elements of the HOC Cyber Incident Response Plan include guiding methodology and principles; response team; response methodology and procedures; communication and escalation plan and procedures; incident response capability for training and validation; incident response metrics collection and reporting; incident response plan supporting playbooks; and incident workflow/process.

Generally, each of these sections outlines various definitions, requirements and/or considerations, processes and/or procedures necessary for a concerted incident response. Regarding Response Team, the member composition, roles and responsibilities of the various interdependent groups which must work together to manage the incident response process are identified and defined.

Attachment III: Information Technology Strategic Plan

This Information Technology Strategic Plan ("Strategic Plan") articulates clear vision and objectives and sets a roadmap to attain and maintain the strategy, and additionally defines metrics by which the IT Division can quantify its success in meeting stated goals. The strategic plan will be effective July 1, 2022 and span a five-year period from FY2023 to FY2028. Moreover, it will supersede the 2016 Information Technology Strategic Plan presented to CLA in the fiscal year 2021 audit cycle.

The Strategic Plan includes discussion of HOC's Mission and Vision, IT Division's mission and values, IT Division's strengths, trends in information technology and society, which inform and shape decision-making and primary work, and strategic initiatives, including objectives, relevance, action plans and measurable outcomes.

The five IT Division strategic initiatives outlined are:

1. Innovate and integrate administrative systems;
2. Enhance technology systems and services;
3. Provide excellent, secure, and compliant IT and services;
4. Foster partnerships and collaboration; and
5. Develop and empower our talent.

In the development of these strategic initiatives, the IT Division recognizes its role as a key partner for sustaining business operations and supporting and advancing the work of HOC, particularly as HOC moves forward through a changing landscape of post-pandemic society and work environment.

Attachment IV: Data Classification Guidelines

The Data Classification Guidelines are designed to explain security requirements while storing sensitive information outside of HOC's secured network infrastructure. Authorized users who extract, post, or use sensitive information must ensure that the security of the storage location, web application, or service is

commensurate with the level of security protection required for the data and obtain approval from their supervisors.

It is critical that users understand and adhere to these guidelines in order to protect HOC's sensitive information once it is outside of HOC's secured systems, since the threat of unauthorized access or inappropriate use increases as a result. Users will be required to read and acknowledge this document in conjunction with the Technology and Acceptable Use Policy and Information Security Assurance Policy.

The major provisions of the guidelines address classification of system risk level designations and appropriate data use. System risk level designations, which range from 0-3, are based on the increasing sensitivity of the data maintained or processed by each system or application. When users understand system risk level designations, they can understand how sensitive that data is within the system and evaluate how they must proceed with extracting, posting, using and storing the data outside HOC's secured environment accordingly. Appropriate data use sets forth how users must ensure that the level of system risk designation corresponds appropriately with level of data sensitivity, defines the levels of sensitive information and approved risk level by storage category or device and consequences for violations.

The Data Classification Guidelines are referenced in the following sections of the Information Security Assurance Policy:

- Section 2.9 *"Handling Sensitive Information"*
- Section 3.4 *"Confidentiality and Secure Handling"*
- Section 9.2 *"Bring Your Own Devices"*
- Section 9.3 *"Terms and Conditions"*

In addition to Attachment II – IV, discussed above and attached to the memorandum, the following policies were developed. Each will be discussed separately and the Administrative and Regulatory Committee will be asked to support staff's recommendation for approval by the Commission.

1. Technology Policy and Acceptable Use Policy
    a. Approval of Information Technology and Acceptable Use of Information Technology Infrastructure and Resources Policy to reflect Current Processes and Risks.
2. Information Security Assurance Policy
    a. Approval of IT Security Assurance Policy to Incorporate Changes in Systems Infrastructure, New Technologies, and User Environment to Reflect Current Processes and Risks,
    b. Approval of HOC Telework Policy.

ISSUES FOR CONSIDERATION:

Does the Administrative and Regulatory Committee wish to join staff's recommendation to the Housing Opportunities Commission of Montgomery County to accept HOC's response to address Management Letter comments by CLA for the FY 2021 annual Agency audit and the accompanying supporting documentation?

TIME FRAME:

For discussion by the Administrative and Regulatory Committee at its meeting on May 16, 2022. For formal Commission action on June 8, 2022.

STAFF RECOMMENDATION & COMMISSION ACTION NEEDED:

Staff recommends that the Administrative and Regulatory Committee join staff's recommendation to the Housing Opportunities Commission of Montgomery County to accept HOC's response to address Management Letter comments by CLA for the FY 2021 annual Agency audit and the accompanying supporting documentation.

Management
Housing Opportunities Commission of Montgomery County
Kensington, Maryland

In planning and performing our audit of the financial statements of Housing Opportunities Commission of Montgomery County (the Commission) as of and for the year ended June 30, 2021, in accordance with auditing standards generally accepted in the United States of America, we considered the Commission's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Commission's internal control. Accordingly, we do not express an opinion on the effectiveness of the Commission's internal control.

However, during our audit we became aware of a deficiency in internal control that did not rise to the level of a significant deficiency or material weakness. This matter is an opportunity to strengthen your internal controls and improve the efficiency of your operations. Our comment and suggestion regarding this matter is summarized below. A separate communication dated November 3, 2021, contains our written communication of significant deficiencies and material weaknesses in the Commission's internal control. This letter does not affect our report on the financial statements dated November 3, 2021, nor our internal control communication dated November 3, 2021.

INFORMATION TECHNOLOGY CONTROLS

Testing of policies and procedures related to information technology identified certain areas for improved controls to mitigate the risk of current technological vulnerabilities more effectively.

- The IT Strategic Plan, IT Technology Policy and Information Security Policy have not been updated in several years. Policies, procedures and strategic documents should be reviewed/updated on an annual basis in order to evaluate whether they reflect current processes, risks, and leading practices. Outdated policies and procedures can create conflict between processes actually occurring and written procedures.

  We recommend the Commission update the IT Strategic plan, IT Technology and Information Security Policies to reflect current processes and risks.

- The Commission is still running six workstations with Windows 7, which was no longer supported as of January 14, 2020. When an operating system reaches "end-of-life" it is likely that the vendor is no longer issuing patches for security vulnerabilities, leaving them vulnerable to cyber-attacks.

  We recommend the Commission proactively seek out these six remaining workstations which are still running Windows 7 and upgrade them to a current, supported operating system as soon as possible.

- The Commission does not have a formal Disaster Recovery/Business Continuity Plan in place. Response to a disaster or business continuity issue could result in unacceptable levels of downtime, uncoordinated or duplicated recovery efforts, mixed messaging in communication, and inappropriate direction of remaining resources.

  We recommend the Commission develop an organization-wide Disaster Recovery/Business Continuity Plan that outlines a disaster recovery team, team member roles, contact information, communication plans, evacuation plans, and alternate sites both short-term and long-term.

- One terminated user was still showing on the listing of active users on Active Directory. An offboarding request form was processed, however due to human error the account was not initially disabled. Terminated employee accounts could remain active and be inappropriately accessed by the individual or a malicious attacker. This account has since been disabled once the Commission learned of the oversight.

  We recommend the Commission conduct periodic user access reviews of the network and compare against a listing of terminated users to insure no terminated users still maintain account access.

MANAGEMENT RESPONSE

Strategic Plan/Technology Policy/ IT Security Policy
HOC IT is working with a third party vendor to update the IT Strategic plan in conjunction with the technology and IT security policies. The new strategic plan, technology policy and IT security policy will incorporate changes in systems infrastructure, new technologies and user environment to reflect current processes and risks. It is anticipated that these updates will be completed by the end of November 2021.

Outdated Operating System/Upgrade
HOC IT upgraded one of the six remaining workstations that were still running Windows 7 to Windows 10, which is the current, supported operating system. The other five workstations were removed from use. This issue has been resolved.

Disaster Recovery/Business Continuity Plan
HOC IT is working with a third party vendor to develop an organization-wide Disaster Recovery/Business Continuity Plan which includes all the recommended elements. This plan is being developed in conjunction with the updated technology and IT security policies. It is anticipated that the document will be completed by the end of December 2021.

User Access/Termination Review
HOC IT conducts user access and termination reviews on a monthly basis. This finding resulted from human error and is an outlier.

* * *

We will review the status of this comment during our next audit engagement. We have already discussed this comment with various Commission personnel, and we will be pleased to discuss it in further detail at your convenience, to perform any additional study of this matter, or to assist you in implementing the recommendations.

This communication is intended solely for the information and use of management, the Board of Commissioners, and others within the Commission, and is not intended to be, and should not be, used by anyone other than these specified parties.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Baltimore, Maryland
November 3, 2021

Information Technology Division
Cyber Incident Response Plan

Last Revision:

April 2022

Table of Contents

Housing Opportunities Commission OF MONTGOMERY COUNTY

10400 Detrick Avenue
Kensington, MD 20895-2484
(240) 627-9400

HOUSING OPPORTUNITIES COMMISSION OF MONTGOMERY COUNTY INFORMATION TECHNOLOGY INCIDENT RESPONSE PLAN

1.0 Overview

Cyber incident response has become an important component of information security programs. Cyber security attacks have become not only more numerous and diverse, but also more damaging and disruptive. New types of cyber security attacks and techniques emerge frequently, resulting in novel security incidents that may catch an organization off guard if unprepared. Preventive activities based on the results of risk assessments and other proactive measures can lower the number of incidents an organization may experience, but not all incidents can be prevented. An incident response capability is, therefore, necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating any weaknesses that were exploited, and restoring Information Technology ("IT") services and operations.

This document provides plans for information system incident handling at the Housing Opportunities Commission ("HOC") of Montgomery County, particularly for analyzing incident-related data and determining the appropriate response to each incident.

2.0 Scope

The incident response plan is applicable to all cyber security-related incidents that involve HOC owned facilities, networks, assets, people, and/or data. In the event an incident involves HOC owned data residing on non-HOC owned networks or assets (i.e., partner or supplier networks), incident response policy elements established in contractual agreements shall serve as an extension to this policy but shall not infer additional risk mitigation ownership, if otherwise stated in the contractual agreement.

3.0 Control Framework Alignment

The incident response program is aligned to the National Institute of Standards and Technology's ("NIST") Computer Security Incident Handling Guide SP 800-61 Revision 2 and NIST's Cyber Security Framework ("CSF").

4.0 Guiding Methodology and Principles

The following sections outline the methodologies and principles that serve as the foundation of the incident response program for the organization.

4.1 Events, Incidents, and Breaches

An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This plan addresses only adverse events that affect the c onfidentiality, integrity, or a vailability of information systems, and not those caused by natural disasters, power failures, etc.

A security incident is a violation or imminent threat of violation of workforce privacy and security policies, computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

- A user clicks on a link in a phishing email, which results in a ransomware attack, making data/systems inaccessible due to encryption until a fee or ransom is paid;
- Users are tricked into opening a document sent via email that is malware; running the tool has infected their computers and established connections with an external host;
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services;
- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash;
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.

A breach occurs when an attempted security event or incident is successful in accessing sensitive data, including but not limited to Personally Identifiable Information ("PII") and/or Protected Health Information ("PHI"). Depending on the type of data breached, remediation could include internal/external notification to employees, clients, and government entities.

4.2 Need for Incident Response

Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security incidents occur. One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology), so that the appropriate actions are taken and a determination can be made if a breach has occurred. Incident response helps personnel to minimize loss or theft of information and disruption of services caused by incidents. Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger

protection for systems and data. An incident response capability also helps with dealing properly with legal issues that may arise from and during incidents.

4.3 Law Enforcement Notification

Notification of external parties and law enforcement may be necessary and a legal requirement. Title 18 U.S.C. §2258A requires any provider of an "electronic communications service" or "remote computing service" to report information about the employee, including identity, email and IP address, or any other identifying information, to the National Center for Missing and Exploited Children if child pornography is discovered. In addition to these reporting requirements, employers have been found liable in a civil lawsuit for failing to report child pornography found on an organization issued or controlled asset.

Category	Definition
Evidence of Child Exploitation or Pornography	Immediate notification of law enforcement will be conducted for any incident involving child pornography or exploitation.
Terrorism	Immediate notification of law enforcement will be conducted for any incident with the possibility of terrorism implications.
Other	The incident risk management group will determine the impact and risk to the organization if law enforcement was to be notified of the incident.

Table 1 – Incident Categorization Requiring Law Enforcement Notification

The organization will leverage forensic services to determine if evidence of child pornography or explicit material resides on HOC-owned assets.

4.4 Federal or State Government Notification

Notification of federal and/or state government agencies will be performed based on the requirements listed below.

Organizational leadership and staff are responsible for identifying a loss, which may require notification of clients.

Additionally, follow applicable vendor, client, and customer agreements that require notification of a breach as appropriate.

Many organizations have specific notification requirements as outlined in their Outside Counsel Guidelines. These may include methods of communication (telephone, secure email, postal mail, etc.).

Reference additional communication plans managed by the organization's Executive Team, Legal Counsel, and/or Public Relations group, as appropriate.

The incident response team will ensure the appropriate level of management is notified in a timely manner based on escalation procedures outlined in the CSIRP. Incident escalation will be based on

incident severity and incident classification and will include escalation to senior leadership, legal counsel, and the board of directors. All escalation points will be captured in the incident timeline and include any specific guidance directed by senior management.

In addition, incidents should be reported to the FBI's Internet Crime Complaint Center ("IC3"), unless otherwise advised against by legal counsel. Reporting to the FBI's IC3 provides information that is analyzed for investigative and threat intelligence purposes to law enforcement.

Notification of federal and/or state government agencies will be performed based on the requirements listed below.

State	Requirements
Maryland State	Notification if breach of PII meeting the requirements listed in Maryland statute § Md. Code Com. Law § 14-3501 et seq. Effective January 1, 2008: The provisions governing maintenance of Personal Information ("PI") are applicable to any Entity maintaining information on MD residents, whether or not organized or licensed under the laws of MD. Notification to impacted employees or consumers if data breach meets definition of statute of personal information. Notification Timing: The notification required shall be given as soon as reasonably practicable, but no later than 45 days after the business concludes the investigation, consistent with measures necessary to determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system Notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation or jeopardize homeland or national security. Notification shall be given as soon as reasonably practicable but not later than 30 days after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security. Notification Method [one of the following]: ● Written notice sent to the most recent address of the individual in the records of the business; ● Telephonic notice, to the most recent telephone number of the individual in the records of the business; or ● Electronic mail to the most recent email address of the individual in the records of the business, if the individual has expressly consented to receive email notice. Except for breaches involving loss of information that permits access to an email account only, notification shall include: ● To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of PI were, or are reasonably believed to have

	been acquired; ● Contact information for the business making the notification, including the business's address, telephone number, and toll-free telephone number, if one is maintained; ● The toll-free telephone numbers and addresses for the major consumer reporting agencies; and ● The toll-free telephone numbers, addresses, and Web site addresses for (i) the Federal Trade Commission; and (ii) the state Attorney General, along with a statement that the individual can obtain information from these sources about steps the individual can take to avoid identity theft. For breaches involving loss of information that permits access to an email account only (and no other PI), the Entity may provide notice in electronic or other form that directs the individual whose PI has been breached promptly to: ● C hange the individual's password and security question or answer, as applicable; or ● T ake other steps appropriate to protect the email account with the business and all other online accounts for which the individual uses the same username or email and password or security question or answer. ● The notification may be given by a clear and conspicuous notice delivered to the individual online while the individual is connected to the affected email account from an IP address or online location from which the business knows the individual customarily accesses the account, but otherwise may not be given to the individual by sending notification by email to the email account affected by the breach. If the Entity demonstrates that the cost of providing notice would exceed $100,000, or that the affected class of individuals to be notified exceeds $175,000, or the Entity does not have sufficient contact information to give notice, Substitute notice shall consist of all of the following: ● Email notice to an individual entitled to notification, if the business has an email address for the individual to be notified; Conspicuous posting of the notice on the Entity's Web site, if the Entity maintains a Web site; and Notification to statewide media. Personal Identifiable Information ("PII") Definition: An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: ● Social Security Number, individual taxpayer identification number, passport number, or other identification number issued by the federal government; ● Driver license number or state identification card number; ● Account number, credit card number, or debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account; or ● H ealth information, including information about an individual's mental health; ● H ealth insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self–insured, that permits access to an individual's health information; or

	• B iometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or • A username or email address in combination with a password or security question and answer that permits access to an individual's email account. "Encrypted" means the protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data. PI does not include (i) publicly available information that is lawfully made available to the general public from federal, state, or local government records; (ii) information that an individual has consented to have publicly disseminated or listed; or (iii) information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act ("HIPAA").
Other	If a data breach or system compromise meets the notification requirements relevant to the state of residence of each compromised record.
Federal (Health and Human Services)	If a data breach or system compromise of protected health information (PHI) meets the notification requirements of HIPAA Notification Rule 45 C.F.R. §164.408.
Notice – Legal Disclaimer	
The above information should not be considered legal advice. Always seek advice from legal counsel in determining breach notification legal requirements.	

Table 2 – External Notification Guidance

4.5 Confidentiality

The CSIRT team members will, in the course of their duties, be exposed to highly sensitive and confidential information. Team members are expected to maintain a high level of confidentiality of any information that is learned as part of their team duties. Senior team leadership will provide guidance on what information could be shared to employees outside of the team.

4.6 Preservation of Digital Evidence

Preserving critical digital evidence and artifacts during a security incident is an essential component of the response process, as it ensures that incident handlers can attempt to identify key details of the incident. These key details include attempting to determine:

- Initial access method;
- Persistence methods;
- Command and control mechanisms; and

- Lateral movement methods.

To ensure preservation of these key artifacts, actions need to occur as part of the incident response and triage process. These actions include halting any further changes (disk changes) on in-scope hosts and preserving or acquiring a memory image of in-scope hosts*.

Notice – Memory Analysis
** As threat actors utilize fileless attacks over other methods, memory analysis becomes of greater importance.*

Preservation recommendations:

Servers

- If possible, utilize snapshot mechanisms within storage or virtualization platforms to create a copy of the hosts storage volumes with an emphasis on the system drive.
- If there is reasonable belief that a server may be executing malicious code for command and control or fileless malware, a live response capture that includes a memory dump is recommended.
- During an incident classified above Level 1, archive logging of authentication events is recommended to prevent loss of information. This archival process would include MS Active Directory ("AD") domain controllers.

Workstations

- If there is reasonable belief that a workstation is part of the incident, utilize containment mechanisms to prevent hosts from communicating with other hosts instead of powering off the system (e.g., pulling the plug).
- If the workstation is believed to possibly be the threat's initial access vector into the environment, consider performing a live response capture of the host that includes a memory dump.

Notice – Forensic Collection
Once IT staff have been trained on host collection methods, general guidance for evidence preservation should follow the strategy of "when in doubt, perform a collection." Unneeded collections can be deleted later, if determined to be irrelevant to the investigation.

The primary objective for gathering digital evidence during an incident is to support the resolution of the incident. Other objectives include documenting the incident and the possibility of providing evidence to support a legal proceeding. To support the possibility of legal proceedings, all digital evidence needs to be collected in industry standard methods that provide a level of chain of custody and integrity validation of logical artifacts. Detailed documentation should be kept for all digital evidence.

- Principle of "best evidence" will be followed. "Best Evidence" is a legal principle that holds the original copy of a document as superior evidence. Within digital forensics, this is the original copy

or the initial image or other logical artifact.

- Imaging of physical drives will utilize a write blocker to ensure the integrity of the source.
    - The original image will have a hash created followed by the digital signature of the hash.
    - The image and the digital chain of custody will be stored in the "best evidence" repository.
    - The physical drive will have its chain of custody preserved by storing it in a secure storage facility.
- All physical artifacts including media, drives, phones, and computers will be collected utilizing a chain of custody process that includes the use of applying a physical chain of custody form to the physical object.
- All logical artifacts including items such as event logs, firewall logs, and other system log data once extracted, will have the following actions taken to ensure the integrity of the evidence.
    - Creation of a digital chain of custody/integrity verification by creating a hash of the logical artifact followed by the digital signing of the hash. Storing the digital chain of custody along with the source artifact in the "best evidence" repository.
    - Storage of the source logical artifact in the "best evidence" repository.
    - Examination activities will be conducted on forensically verified copies of the "best evidence".

Notice – Chain of Custody
**Physical evidence chain of custody form is located in the Incident Response and Business Continuity G-suite shared drive*

4.7 Analysis versus Containment/Eradication and Recovery Competing Priorities

The analysis and containment components of a phased incident response are key when the organization needs to develop a full understanding of the incident. Shifting too quickly to eradication or recovery without a period of containment monitoring can result in failed containment. Some aspects of the compromise or breach may not be fully understood, allowing the attackers an opportunity to reestablish their access or continue executing their actions on objectives.

Monitoring the effectiveness of the containment is a critical step prior to shifting to eradication and finally, recovery. Senior business leadership will likely be focused on recovery and the incident response team will have competing priorities. Based on these competing priorities, there may be the need for short- and long-term containment strategies to allow the eradication and recovery of critical services.

HOC's competing priority strategy will be:

- Reinforce reasoning with senior leadership during an incident that adequate time needs to be allocated for analysis of the incident for proper scoping, identification, impact determination;
- Creation of containment strategies that comprise both short- and long-term tactics and techniques;
- Eradication and recovery only after monitoring of containment effectiveness.

4.8 Response Methodology – Live Response versus Dead Box Forensics

The rapidly evolving pace of cyber-attacks has changed the standard practices that drove incident response and digital investigations of the less interconnected world of 20 years ago. Past practices in many cases were driven by the seizure and analysis of a single PC or server, which would then have its hard drive imaged and dead box forensics would commence (after waiting the 4-8 hours for the image and processing to occur) to determine what happened or what the individual did. The size of modern hard drives and the inability to remove flash-based storage from numerous laptops mandates the use of other artifact collection techniques. Also, imaging a 1 TB SSD drive with a write blocker to a fast storage device with a high-end collection system on average consumes 4-6 hours. Processing the image with standard commercial forensics tools would consume an additional 6-8 hours depending on the level of processing.

To respond, analyze, and contain modern attacks, digital evidence and artifact collection needs to occur at a much more rapid pace. Live response techniques have been developed to provide tactics and techniques to rapidly collect key digital artifacts from in scope systems to quickly provide answers to important analysis and containment strategy questions. Network forensic capabilities also play a key role in quickly determining system scope and confirming actions of systems post compromise. Log collection and analysis from cloud-based services are also essential in many instances.

To meet the demands of modern incident response, the following response methodology will be utilized:

- Utilization of live response collection tools and techniques to aid in the quick investigation and scoping of the incident, including the ability to collect remotely from multiple systems simultaneously;
- Utilization of network forensics to aid in the scoping and analysis of the incident;
- Dead box forensics will be conducted when live response methods will not meet the needs of the investigation.

To support these response methodologies, the following capabilities should be provided within the information security program:

- Development and continued support of a network forensics capability that includes:
    - Network communication telemetry collection and storage within an analytics platform.
- Development and continued support of a live response capability for MS Windows hosts that includes the following:
    - Ability to collect key digital artifacts from suspect systems;
    - Ability to initiate live response individually on suspect systems and from a centralized process to facilitate collection from numerous systems;
    - Key digital artifacts include;
        - Windows event logs,
        - Windows registry hives,
        - Windows evidence of execution artifacts,

        - Windows scheduled tasks,
        - Web browsing history and cache,
        - Master file table,
        - Volatile memory,
    - Hash Creation;
        - Shasum,
        - MD5deep/Hashdeep,
        - PowerShell can also be used to extract hashes of files,
            - For example, Get-filehash - Algorithm SHA256 (path/file),
    - Recommended tools for live response collection include:
        - KAPE
            - URL: https://www.kroll.com/en/services/cyber-risk/investigate-and-respond/kroll-artifact-parser-extractor-kape
        - FTK Imager (Disk and Memory Imaging)
            - https://accessdata.com/product-download/ftk-imager-version-4-5

Dead box forensics still has its place, but during the rapid time constraints typically given in the analysis and containment phases of modern incidents, this type of analysis will not be feasible. Live response techniques combined with network forensics will allow an organization to meet these time constraints. Dead box forensics will still be utilized to provide additional artifact gathering and analysis in a parallel work stream to the live response techniques as needed.

4.9 Outside Parties

HOC may choose to discuss incidents with other groups, including those listed below, for assistance in resolving technical issues. Additionally, the Incident Response Team may need to communicate with outside parties regarding an incident such as contacting law enforcement, fielding media inquiries, and seeking external expertise. The Information Security Officer leads all incident response activities and the liaison with upper management, clients, law enforcement, and other organizations. All communication to outside entities outside of contracted vendors and service providers will be approved by the Chief Technology Officer. The team will document all contacts and communications with outside parties for liability and evidentiary purposes.

i. Data Network and Internet Service Providers – HOC may need assistance from its ISP in blocking a major network-based attack or tracing its origin.

ii. Owners of Attacking Addresses - If attacks are originating from an external IP address space, incident handlers may want to talk to the designated security contacts for the organization to alert them to the activity or to ask them to collect evidence.

iii. Third-Party Forensics Provider – HOC may need assistance from a specialized third-party provider to assist with computer forensics.

iv. Application Providers and Software Vendors - Incident handlers may want to speak to a software vendor about suspicious activity. This contact could include questions regarding the significance

of certain log entries or known false positives for certain intrusion detection signatures, where minimal information regarding the incident may need to be revealed. More information may need to be provided in some cases—for example, if a server appears to have been compromised through an unknown software vulnerability. Software vendors may also provide information on known threats (e.g., new attacks) to help organizations understand the current threat environment.

v. Law enforcement* involvement - Involving law enforcement may take place when sensitive information pertaining to PII and PHI is involved during a security breach. With the help of federal investigators and outside forensic firms, HOC can have an investigation done to determine if a breach has resulted in data loss.

Notice – Law Enforcement Involvement
**Consultation with Breach management team should occur prior to engaging law enforcement as organization staff may unwittingly become agents of law enforcement.*

5.0 Response Team

A computer security incident response team ("CSIRT") is a functional entity that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening.

HOC's Cybersecurity Incident Response Team is composed of a distributed team of technical and business leaders organized into functional groups based on their role in the incident response process. The following sections define the structure of each group with supporting roles, responsibilities, and communication structure. Current team membership along with contact information is maintained in the appendix of the plan.

5.1 Incident Detection & Coordination Group

This group will function as the core of the incident response team, orchestrating detection and response activities in accordance with the incident response plan. Key responsibilities include primary incident detection, declaration, orchestration, and incident escalation.

Roles

Role	Responsibility
Security Analyst	Detection
Incident Handler	Declaration, Coordination, coordination of incident groups, post-incident review, coordination of recovery. Primary incident handler, coordination of the incident groups.
IT Director	Top level security leader/decision maker.
Scribe	Track incident documentation, timeline, document artifacts, craft status messages, and create the incident report.

Table 3 – Incident Detection & Coordination Group Definitions

Role Assignment: Reference Cybersecurity Incident Response Team Internal Contact List, located in the Incident Response and Business Continuity G-suite shared drive.

5.2 Incident Risk Management Group

This group will serve in an advisory role that provides guidance for risk based decision-making and influences the actions of the incident response teams. This group comprises broad advisory areas such as legal and Talent Management as well as business leaders and data owners that can provide guidance on the handling and disclosure of incidents regarding specific sensitive data areas.

Roles:

Role	Responsibility
External Legal Counsel	Provide guidance on data breach notification requirements and regulations, reviews external notification communications. Provides guidance on communication and coordination with law enforcement agencies if necessary
Human Resources	Provides guidance on incidents involving inappropriate usage by employees and guidance on breach notification process for employees
Business Unit Leaders	Provide guidance and feedback on incident impact on relevant business areas
Cyber Insurance Carrier	Provide guidance and feedback on loss coverage and outside service availability
Risk Management	Provide guidance and feedback to the incident response risk management group on overall risks to the organization
Public Relations	Managing communication with the public and media as necessary. Acts as a point of contact for any media inquiries.

Table 4 – Incident Risk Management Group Definitions

Role Assignment: Reference Cybersecurity Incident Response Team Internal and External Contact Lists, located in the Incident Response and Business Continuity G-suite shared drive.

5.3 Incident Operational Support Group

This group will be responsible for providing operational support for incident response activities. The nature of the supported activities ranges from technical actions to business process execution needed to achieve incident response activities. This group will also provide services needed to recover from the incident.

Role	Responsibility
Physical Security	Aid with access to secured locations and supports inquiries of physical security video or building security log data
IT Support Teams	Aid with discovery, containment, and eradication tasks in support of the incident response team
Corporate Communications	Provide support with communication to business units and employees related to impact to IT services during incident
Business Support Groups	Provide support for determining impact and scope of incident
Data Owners	Aid in determining data sensitivity and potential loss or corruption

Table 5 – Incident Operational Support Group Definitions

Role Assignment: Reference Cybersecurity Incident Response Team Internal and External Contact Lists, located in the Incident Response and Business Continuity G-suite shared drive.

5.4 Incident Communication

This group is responsible for the timely and accurate communication to external parties including reporting agencies, affected parties, public notification, and other applicable entities.

Role	Responsibility
Corporate Communications (HOC Legislative and Public Affairs)	Managing communication with public and employees in terms of breach notification if necessary and acts as a point of contact for any media inquiries.
3rd Party Breach Management (Cyber Insurance Carrier)	Contracted outside party responsible for performing breach notification based on information from public and corporate communications

Table 6 – Incident Communication Definitions

Role Assignment: Reference Cybersecurity Incident Response Team Internal and External Contact Lists, located in the Incident Response and Business Continuity G-suite shared drive.

5.4 Incident Decision Authority Delegation

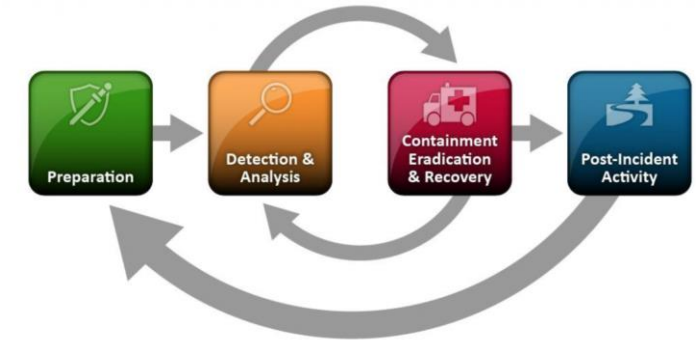
The table below outlines the delegation that has been assigned to the roles listed to provide timely decision making during an incident. Without timely decisions, attackers may have the opportunity to continue exfiltration of data, which is the unauthorized transfer of data from a computer by an unauthorized person or malware software, or remain hidden in the environment.

Role	Authority Delegation
Incident Handler	Declaration of incident including impact and severity, plus containment strategy decisions including service suspension.
IT Director	Includes all authority delegated to principal incident handler and authority to make immediate incident handling decisions when communication with the risk management team would delay an immediate response to a change in containment effectiveness or possible imminent risk of data destruction by threat actor.

Table 7 – Incident Decision Authority Definitions

6.0 Response Methodology and Procedures

6.1 Preparation



Incident response preparation begins prior to an incident to ensure effective and successful incident handling. The primary goals of this phase include establishing incident response teams, creation of contact directories, creation of reporting/documentation templates, and defining communication plans and procedures. Secondary goals include training of the incident response team and enablement of the incident response team with appropriate tools and technologies.

Additionally, prior to an incident, HOC must ensure that the following is clear to IT personnel:

- What actions to take when an incident is suspected?
- Who is responsible for responding to an incident?

This phase also includes achieving training objectives for the incident response team members based on the listed requirements in the incident response capability section. Conducting annual validation via tabletop exercises, as an example, are also part of this phase.

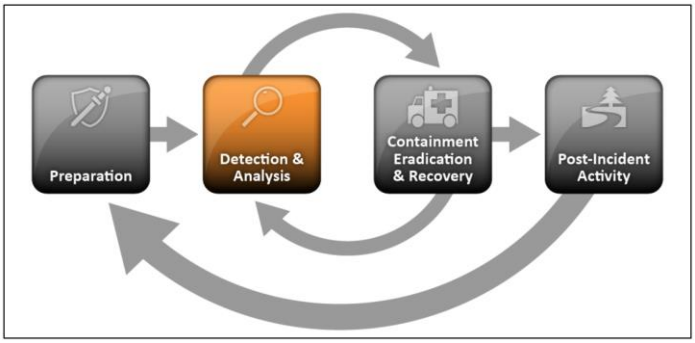
Critical documentation useful during an incident response should be always available to responders and critical personnel. Critical documentation includes:

- Inventory of critical systems and applications that support core business operations,
    - Map and understand the assets, systems, and networks that support core business processes and assign a business priority to each. This process can aid in prioritization during recovery efforts;
- Network Documentation,
    - Develop and maintain accurate network diagrams that detail interconnections, IP Addressing, and gateway networks.

Critical documentation will be stored on/using the below available services:

- The Incident Reporting folder contained within the IT Policies and Procedures Shared Drive.

6.2 Detection and Analysis



An event may be discovered in many ways, including employee notification, intrusion detection system, endpoint security suites, or automated correlation by a security information event management ("SIEM") platform. As part of this phase of incident response, the security team needs to assess whether the event is something that needs to be categorized as an incident. Determination of whether the event is an incident is based on several factors including successful unauthorized access, impact on availability, loss of confidentiality based on a breach of data, or violation of acceptable use policies.

As part of incident declaration, the incident needs to be categorized based on the defined taxonomy along with severity determination. Also, determination if the incident involves any of the defined data classifications (PII/PHI/PCI/IP). [*Note: PCI is payment card information.]* These items will be determined as part of the analysis component of this phase.

Other activities within the detection phase include verification that detection tools and processing are working as expected and verification that security events are analyzed and escalated to incidents when appropriate.

The primary detection capabilities at HOC include:

- Firewalls at Internet Edge – Palo Alto PA-5220 X 2;
  - IPS and other threat detection controls – Palo Alto PanOS NGFW
- Endpoint Security – Malwarebytes EDR;
- E-mail Security Google – G-Suite with Ironscales Anti-Phishing and SysCloud Data Loss Prevention (DLP) and Anti-Virus (AV);
- Network Detection and Response – TBD, discussing with vendors.

The analysis component of this phase includes determination of incident severity, scope, impact, and if defined data classification types are affected. Primary objectives of analysis include determining scope, impact, and severity of incident. Secondary objectives include all analysis tasks that provide the underlying data to support the determination of the primary objectives.

The analysis phase needs to complete the following objectives before proceeding to containment:

Primary Objectives:

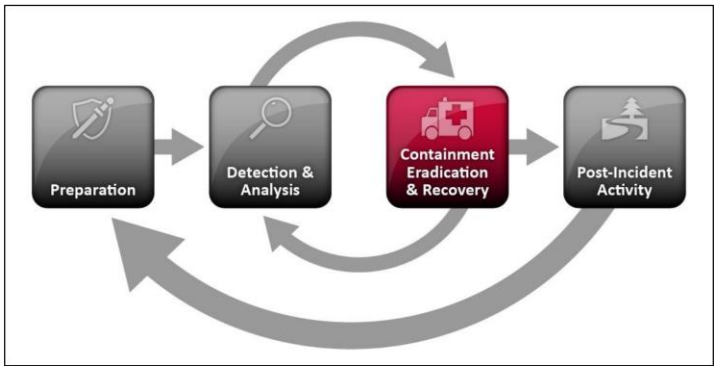
- Determination of scope:
  - What hosts, network segments, cloud services, accounts (identity), and other resources or services are involved in the incident?
  - Is there data that meets the classified data listed in scope?
- Determination of impact:
  - How are the in-scope hosts, networks, accounts, and cloud services affected by the incident?
- Determination of severity:
  - Based on scope and impact, determine appropriate severity.

Secondary Objectives:

- What hosts and network segments are in scope of the incident, and what containment capabilities/methods exist to contain the incident?
- What is the incident taxonomy?
- What indicators of compromise (IoCs) have been discovered based on analysis tasks?

The final major task of the analysis phase is the initiation of incident reporting/tracking documentation. This documentation will support the tracking of the incident, support status and notification requirements, and will be analyzed as part of the root cause and lessons learned activities.

6.3 Containment, Eradication, and Recovery



Containment, eradication, and recovery are essential components of any incident resolution. Eradication and recovery will not be effective if containment fails. Moving to eradication or recovery sub-phases without proper monitoring of containment efficacy will likely result in failed containment. Some aspects of the compromise or breach may not be fully understood, allowing the attackers an opportunity to reestablish their access or continue their exfiltration of data.

Monitoring the effectiveness of the containment is a critical step prior to shifting to eradication and finally, recovery. As discussed in the guiding methodologies and principles section, senior business leadership will likely be focused on recovery, which will likely result in competing priorities. Based on these competing priorities, there may be the need for short- and long-term containment strategies to allow the eradication and recovery of critical services.

The containment sub-phase needs to meet the following objectives before proceeding to eradication:

Primary Objectives:

- Stopping the proliferation of the incident;
- Command and control communications utilized by attackers have been identified and blocked;
- Terminating any exfiltration of data, if occurring, or blocking any attempts at exfiltration.

Containment strategies include the following:

- Edge Network Perimeter:
  - Utilizing network edge firewall (PaloAlto 5220 X 2) to block communication to command and control, exploit server, or other external entity;
  - Removal of policies allowing public access to applicable services and protocols.

- Internal Network:
  - Utilize internal firewalls (Windows HBFW) to block communication between network segments;
  - Disconnecting sections of the network;
  - Switch-based port IP Access Control Logs ("ACLs");
  - Private Virtual Local Area Networks ("VLANs");

- Endpoint:
  - Utilize Host-Based Firewalls (HBFW) to block unwanted or malicious traffic
  - Application blacklisting
  - Policy modification on advanced endpoint security agent

Monitoring containment effectiveness is the next critical component. Prior to shifting to the eradication sub-phase, a period of monitoring needs to occur.

The eradication sub-phase needs to complete the following objectives before proceeding to eradication:

Primary Objectives:

A. All artifacts/malware related to the incident have been removed or remediated;

B. All hosts and services have been hardened, patched, or compensating controls applied;

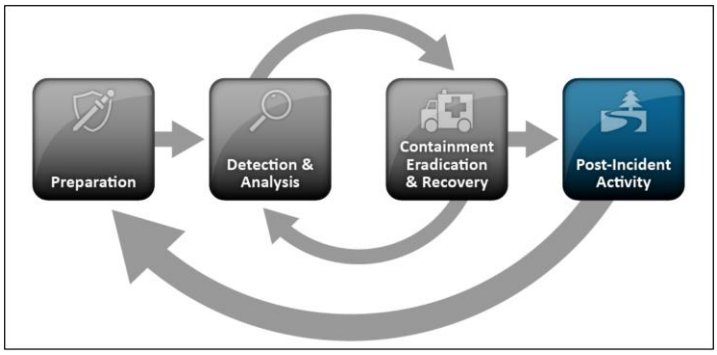
C. Re-imaging of systems that cannot be “cleaned” has been initiated. System is no longer “up”.

Recovery strategies and techniques will vary depending on the type of incident and impact to the environment. For recovery of complete systems and services, refer to HOC's disaster recovery plan.

Below is a high-level listing of some possible recovery methods:

- Remediate or implement compensating controls for all vulnerabilities discovered as part of the incident;
- If the system was compromised and full forensic analysis will not be completed, a full re-imaging of the system is recommended. Re-install clean images of the operating system;
- Installation of vendor security patches;
- Forced change of all passwords of impacted accounts;
- Reconnect portions of the network, if disconnected as part of the containment phase;
- Conduct a vulnerability scan of the compromised machine/system before reconnecting to the network;
- Reconnect to the network.

6.4 Post-Incident Activity



Post-incident activities include performing root cause analysis, incident reporting and metric collection, and conducting a lesson learned review.

Root cause analysis should include the following:

- Review of digital artifacts including live response, network forensics, and cloud services;
- Review of detection systems for possible indicators of attack/incident;
- Review of all incident documentation;
- Determining if the incident is a recurrence of a previous incident;
- Evaluating the difference between initial severity and impact assignment and the final severity and impact assignment;
- Documenting measures, if any, that could have prevented the incident.

The lessons learned session should have the following topics discussed:

- What security improvement recommendations should be implemented based on the method(s) of attack?
- Are there sections in the incident response plan that need to be modified or updated?
- How well did the incident response team perform the following actions?
    - Is there training that needs to be conducted to remediate a skillset deficiency of the incident response team?
    - Was communication and escalation timely and appropriate?
- Were the containment strategy and techniques effective?
- Are there additional tools or resources that would have aided in the detection, analysis, containment, or eradication of the attack?

Completing the incident documentation and determining if follow-up reporting needs to occur should also be completed. Within the appendix of the plan, there is a listing of the required items to be included with the incident report. Final determination of external communication and notification should be discussed within the incident risk management team. Items to be considered include reporting of the incident to FBI ISC, updates to public relations representatives, or if there are breach notification requirements.

Based on the lessons learned session, perform any incident response plan updates or initiate security improvement items agreed upon by the organization's information security and leadership teams.

The final item within the post-incident activities will be the digital artifact and evidence retention requirements. The retention period will be defined on several factors, including but not limited to incident severity, and if the incident involved any of the classified data types. HOC's legal counsel or engaged third-party incident response team will provide guidance and recommendations for retention.

7.0 Communication and Escalation Plan and Procedures

7.1 Internal Communication

As part of incident response management, HOC should have an established escalation and notification process. Notification escalation will be established for the following key personnel within the organization. Notification escalation for external entities is addressed in the next section. The incident handler is responsible for communicating incident status to the incident response team. Updates to other key personnel may be delegated to other team members.

Key Personnel:

- Executive Director
- Chief Financial Officer
- General Counsel
- Chief Technology Officer
- Deputy Executive Director
- Director of Human Resources

Contact Methods:

Status updates and other escalation notifications will be communicated by email (unless possible system compromise is believed), phone call, and text. The HOC contact directory is provided in the appendix. If possible, system compromise is suspected, an out-of-band communication method will be utilized for electronic communication instead of email.

If necessary, out of band communication (such as AlertMedia, yet to be acquired), will be utilized if the aforementioned communication methods are unavailable. All members of the CSIRT team will have their Signal/Gmail handle listed in the CSIRT team contact directory/spreadsheet. The out-of-band communication service will be utilized during any incident where there is a risk that the threat actors may have control over email or other internal communication systems.

Notifications:

Incidents including any of the listed data classification definitions below must be communicated immediately with the CTO, CCO, HelpDesk and Security Breach Group, as laid out in the HOC Information Security Assurance Policy ("ISA Policy") as well as the incident risk management group. The risk management group will communicate with human resources, legal representatives, public relations, and senior business leadership to determine notification requirements and strategy.

Notifications for level 1 severity incidents will be handled through standard incident ticketing systems. Level 2 and 3 severity incidents will follow the status update methods listed below for the initial notification of the incident.

Status Update Intervals:

Status updates will be provided to incident response team members and to key personnel based on the following table:

Incident Severity Level	Status Update
Level 1	Email updates or updates to incident ticketing system daily until incident is resolved
Level 2	The incident operation support group will provide status updates via email, text, and phone to the larger incident response team and key personnel every 4 hours until the incident is resolved.
Level 3	The incident operation support group will provide status updates via phone or video conference (war room) to the larger incident response team and key personnel every 2 hours until the incident is resolved. Update interval can be reduced to every 4 hours when effective containment is achieved.

Table 8 – Incident Update Cadence

For internal contacts, reference Cybersecurity Incident Response Team Internal and Contact List, located in the Incident Response and Business Continuity G-suite shared drive.

7.2 External Communication and Notification

External communication to law enforcement, breach notification designees, or media will all be managed by the incident risk management group. Communications to external incident response partners involved in incident response activities is not considered external communication.

For level 2 and 3 severity incidents, the incident risk management group will coordinate all communication with cyber insurance and outside legal counsel, if applicable. External communication and notification of cyber insurance carriers (CFC Underwriting) should be evaluated if reasonable belief by IR team leadership that impact of incident will exceed $10,000 in losses, or in remediation/recovery costs. If contact and subsequent support is requested from a cyber insurance carrier, a breach manager will be assigned to Customer to aid in providing advice for forensic services and advice on breach notification, if applicable.

Notice – Cyber Insurance
Cyber insurance carriers can take between 24 and 96 hours to respond with assignment of a breach coach/manager (lawyer specializing in cybercrime). After assignment of a breach manager, an authorized incident response/forensic provider will be engaged. Typically, there is another 8–24-hour delay before the incident response provider will begin to perform consulting activities. *Based on these expected delays, it is recommended to perform an immediate notification of the cyber insurance provider to expedite the process as much as possible.*

For external contacts, reference the Cybersecurity Incident Response Team External Contact List, located in the Incident Response and Business Continuity G-suite shared drive.

Notice – Law Enforcement
FBI Notification: Submitting an FBI IC3 complaint/submission is highly recommended for any significant ransomware incident. The FBI will likely have additional undisclosed details of tactics and motives of the threat actors. In addition, notification of law enforcement is listed as a mitigating factor for consideration of civil enforcement by the US Treasury department ransomware advice.

Law enforcement notification and communication will follow the guiding methodologies and principles criteria.

All media requests or communication will be directed towards the public relations representative of the incident response team. The public relations representative is the only authorized company entity that will communicate with the media.

External Notification Requirements

Type	Requirement
PII	If a data breach or system compromise meets the notification requirements specified in the Maryland Identity Theft Enforcement and Protection Act. Bus. & Com. Code §§ 521.002, 521.053, breach or system compromise meets the notification requirements relevant to the state of residence of each compromised record. Security Breach Notification Laws (ncsl.org)
PHI	If a data breach or system compromise of protected health information (PHI) meets the notification requirements of HIPAA Notification Rule 45 C.F.R. §164.408
PCI	If a data breach or system compromise meets the notification requirements defined in PCI-related contracts for payment card brands, acquirers, or other entities, or if required by law
Child Pornography	Immediate notification of local law enforcement. Receive guidance/instruction from law enforcement on how to secure / preserve affected system(s) until law enforcement will take ownership of data.

Table 9 – External Notification Requirements

Law Enforcement and Federal Contact Information

Type of Crime	Law Enforcement Agency	Contact Information
Computer or network intrusion, Password trafficking, Internet fraud	National Cybersecurity and Communications Integration Center	(888)282-0870 info@us-cert.gov
Computer or network intrusion, Password trafficking, Internet fraud, Ransomware	US Secret Service, Baltimore, MD	(443)263-1000
Computer or network intrusion, Password trafficking, data breach, Internet fraud, Ransomware	FBI, Baltimore, MD Office	(410)265-8080 tips.fbi.gov
Computer or network intrusion, Password trafficking, Internet fraud, Child exploitation.	IC3: Internet Crime complaint Center (IC3)	IC3 Website
Breach of PHI	U.S. Department of Health and Human Services	HHS.gov

Table 10 – Law Enforcement and Federal Contact Information

Cyber Insurance Contact Information

Vendor	Limits	Contact Information
Everest Reinsurance	Limit: 5 million Retention (deductible): $250,000 (or higher)	Telephone # 908-604-3000

Table 11 – Cyber Insurance Contact Information

Internet Service Provide Contact Information

Vendor	Web Portal	Contact Information
MCG Fibernet DTS		NOC # 240-777-2999

Table 12 – ISP/Critical Service Contact Information

7.3 Escalation Procedures

As additional incident-related information develops during the IR process, additional escalation and notification may be necessary if an incident is reclassified to a high severity or is determined to involve defined data classifications.

8.0 Incident Response Capability – Training and Validation

The incident response plan will be exercised on an annual basis, with a level 2 or 3 incident fulfilling the requirement if the incident response plan was followed. If no level 2 or 3 incidents occurred during the year, tabletop exercises will be conducted. The tabletop exercises will include the full CSIRT team and key leadership and legal representatives. The tabletop exercises will include two of the listed incident taxonomy definitions. The exercise should be an immersive experience with all listed participants in a hands-on cross-functional scenario.

Requirements and objectives of exercise:

- Assess ability of incident response team to effectively;
    - Detect, triage, and perform analysis of incident,
    - Perform data loss impact and classification, and severity of incident scenario,
- Use and validation of relevant playbooks;
- Validation of incident response plan communication plan;
- Validation of incident response plan notification plan;
- Gather gaps and improvements for the incident response plan and playbooks.

In addition to tabletop exercises, refresher training will be provided to the incident response team members and potential first responders. This refresher training will be focused on a review of the guiding principles, artifact collection techniques, and containment strategies and tactics. The training should also include practice exercises of collecting artifacts and performing malware triage techniques.

Any HOC personnel with the role designation of incident handler, including individuals slated to function in the role of incident commander, are required to attend continuing education. The continuing education will be relevant to incident response in the domains of detection, response, or another investigative/forensic related topic.

9.0 Incident Response Metrics Collection and Reporting

To provide additional data and discussion points to the post incident activity phase, incident metric collection and reporting is a key element. Metrics provide valuable information used in determining the effectiveness of an organization's detection and response capabilities. Without metrics, it is very difficult to make a quantitative assessment of how effective HOC's CSIRT team is.

The following key elements should be included in the incident response metric collection process:

- Time from compromise to discovery (dwell time);
- Time from incident alarm to triage;
- Incident severity and classification;
- Incident taxonomy;
- Detection method;

- Time for containment and containment method(s);
- Time for eradication and eradication method(s);
- Artifact collection methods utilized (live response/dead box forensics);
- Time to recover and total time to resolve incident;
    - Include summary of recovery methods utilized and if any recovery methods were not working.

As part of the post-incident activities, the primary incident handler will compile the supporting information and submit it to the Chief Technology Officer.

Incident response management reporting will occur at the end of the annum during years when major incidents occur. This reporting will highlight all incidents for the past year and provide summary information for the following:

- Listing of quantities of incident taxonomy for all known/recorded incidents;
- The average time for detection (dwell time);
- Time from detection to incident initiation/analysis tasks;
- Listing of times for resolution by incident taxonomy/type;
    - Include details for each phase
- Summary of significant items from lessons learned in terms of improvement areas for process, tools, or training;
- Incident severity and classification.

The information security manager will be responsible for compiling all incident metric documents and summarizing the results into a report to submit to the Chief Technology Officer or the designee.

10.0 Incident Response Plan Supporting Playbooks

IR Playbook Overview

A playbook is defined as a set of steps describing actions to be executed, with input and expected output data to be collected. Depending on the output data collected on a step, there could be further sub-steps taken. Having pre-built playbooks is a critical component of a security program, as they provide consistent actions taken for defined incident scenarios. The playbooks also ensure that critical steps are not missed during a rapidly evolving incident. Defined playbooks also allow for automation and orchestration of certain steps.

Goals of each playbook should be:

- It is relevant and clearly defined to the incident scenario/taxonomy;
- It provides detailed, well documented, process and procedures;
- It focuses on the incident phases of analysis, containment, eradication, and recovery;

- It focuses on dealing with the consequences of an incident and not its causes;
- It is reviewed and understand by the incident response team and Security Operations Center (SOC) personnel;
- It provides guidance on competing priorities of analysis, containment, and recovery;
- It provides guidance on digital evidence and artifact collection and if full forensics (dead box) is recommended;
- It provides guidance on when notification of internal and external parties is recommended;
- It is reviewed and updated on a recurring basis;
- It specifies rules for involving third parties, such as external experts, insurance companies, forensics specialists, government agencies, etc.

IR Playbook Scenarios

The following playbooks have been defined for the listed incident taxonomies:

- Ransomware;
- Malware;
- Distributed Denial-of-Service ("DDoS");
- Business Email Compromise;
- Unauthorized Access.

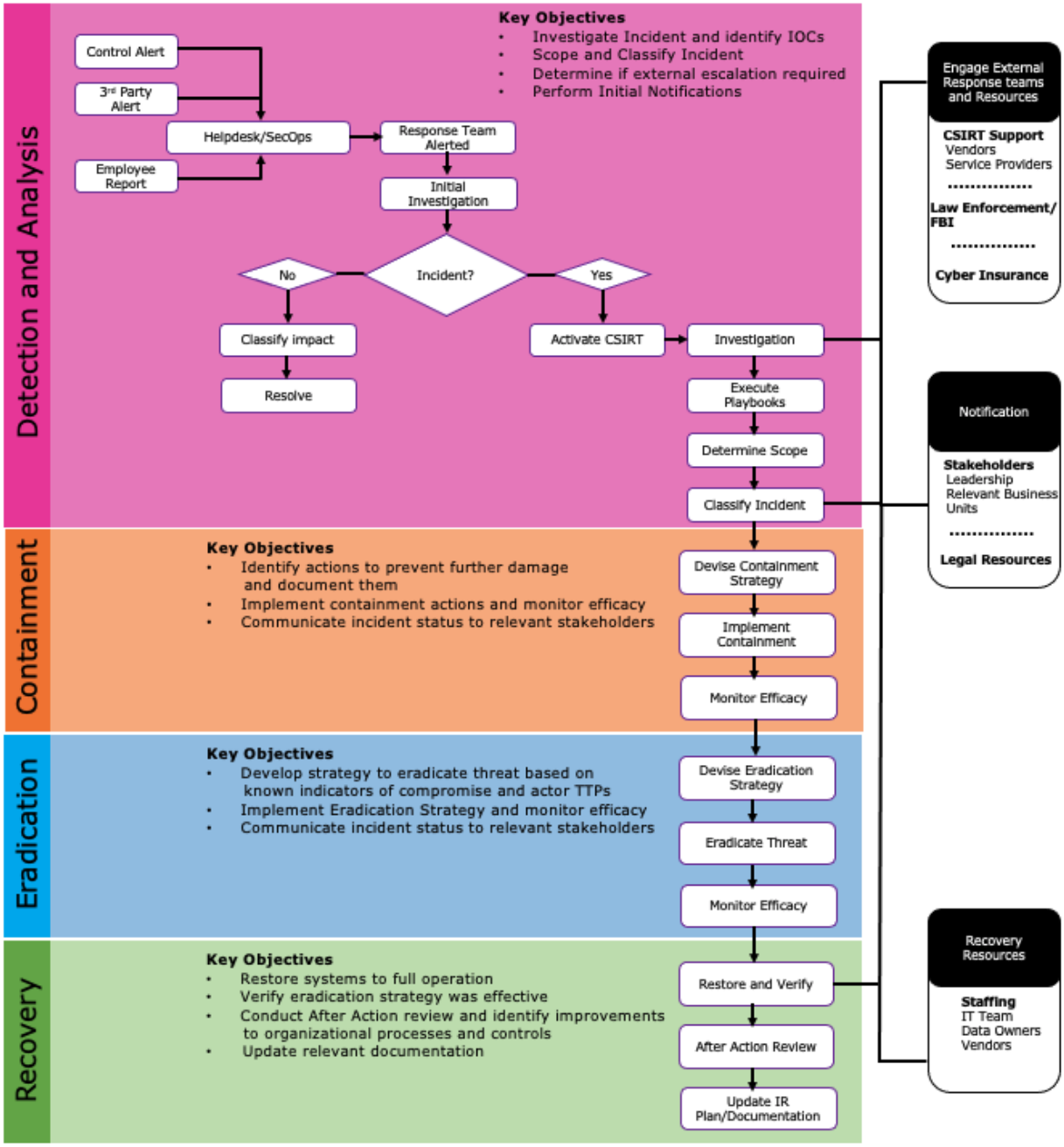
Reference IR Playbooks, located in the Incident Response and Business Continuity G-suite shared drive.

Notice – Cyber Incident Response Playbooks
HOC's Incident Response playbooks are external to this document and can be accessed via the organization's document repository.

11.0 Incident Workflow/Process

The following section utilizes the processes, structure, and definitions listed in the CSIRP to provide a workflow for "working" an incident. This is a generic workflow and certain types of incidents may have small variances that will be addressed in the playbook for that incident type.

Figure 1 – Incident Workflow Flowchart



Step 1: Detection and Analysis	
Perform discovery and analysis to aid in assessing the following:	
Task	**Description**
Determine type incident	Based on incident taxonomy, what is the type of incident?
Determine scope (hosts/services/accounts)	Conduct discovery and analysis to document hosts and services involved in incident (document quantities, as well)
Determine scope (data classification/loss)	Conduct discovery and analysis to document classification of data involved in incident and if there is potential for data loss (document quantities as well)
Playbook execution	Determine appropriate playbook and execute workflow / steps

Step 2: Assess Functional Impact			
Select functional severity based on Functional Impact			
Symbol	**Functional Impact**	**Description**	**Recommended Severity**
H	High	Cannot provide a critical service to any user	High/Level 3
M	Medium	Lost ability to provide an essential or deferred service. Reduced ability to provide a critical service.	Medium/Level 2
L	Low	Minimal effect: can still provide all critical, essential, or deferred services to most users, but has lost efficiency	Low/Level 1
N	None	No effect in ability to provide all services to all users	Low/Routine

Step 3: Assess Data Classification Impact			
Select one or more informational impact levels based on the incident's impact on the confidentiality, integrity, and availability of data based on HOC's Data Classification Guidelines.			
Symbol	**Data Impact**	**Description**	**Recommended Severity**
C	Confidential	Incidents involving exposure or possible exposure of personally identifiable information (PII), payment card information (PCI), protected health information (PHI), or other data that could lead to critical losses if disclosed or corrupted.	High/Level 3
P	Public	Incidents involving data within the public domain	Low/Routine
U	Unclassified	Incidents involving data not classified into one of the other two classifications above. This data will be treated as if it were potentially confidential until a data owner formally classifies it.	Medium/Level 2
N	None	Incidents involving no perceived exposure of data.	Low/Routine

Step 4: Assess incident Severity					
Use the table below to assist with determining incident severity based on Functional Impact and Data Classification.					
		Severity Level			
Functional Impact	**High**	3	3	3	3
	Medium	3	2	2	2
	Low	3	2	1	1
	None	3	2	1	1
		Confidential	**Unclassified**	**Public**	**None**
		Data Classification			

Step 5: Assess Incident Severity		
Select incident severity based on impact to the organization, scope, and data involved		
Summary		**Details**
HIGH/ LEVEL 3	▪ Lost ability to provide a critical service ▪ Confidential data has been compromised ▪ Potential risk to reputation	▪ Significant impact to reputation ▪ May significantly impact IT production operations, that can cause productivity issues for employees, partners, or customers ▪ Recovery requires resources out of IT Division. ▪ Legal counsel must be involved.
MEDIUM/ LEVEL 2	▪ Moderate impact to organization ▪ Lost ability to provide an essential or deferred service ▪ Involves information that may be confidential, but has not yet been confirmed	▪ Could result in limited impact to reputation ▪ Could cause limited impacts on IT production operations that can cause limited productivity issues for critical system users ▪ Recovery requires resources outside of IT Division, or requires extended time to resolve ▪ Some impact on critical services/applications ▪ Legal counsel must be involved.
LOW/ LEVEL 1	▪ Minor or no impact to organizations critical services; can still provide all critical services to most users ▪ Little or no risk to confidential information (PCI, PHI, PII, IP) ▪ Recovery does not depend on resources outside of the IT team	▪ Could not result in impact to reputation ▪ No or minor impact on productivity ▪ No impact on production operations ▪ No Impact on critical services/applications ▪ Does not threaten loss of privacy, confidential, or proprietary data

Step 6: Perform Notification – Internal		
Perform notification based on incident severity and data loss potential		
Recipients		**Details**
HIGH/ LEVEL 3	▪ IT Leadership ▪ CSIRT Risk Team ▪ IT Operations	▪ Provide notification to the recipients listed and provide details regarding: o Impacted hosts/services/account o Potential data loss assessment ▪ Include classification of data if applicable ▪ Provide update through email, out of band, and phone ▪ Establish war room/conference bridge ▪ Status updates every two (2) hours until severity is lowered, or containment/eradication has occurred
MEDIUM/ LEVEL 2	▪ IT Leadership ▪ IT Operations	▪ Provide notification to the recipients listed and provide details regarding: o Impacted hosts/services/account o Potential data loss assessment ▪ Include classification of data if applicable ▪ Provide update through email, out of band, and phone ▪ Establish war room/conference bridge ▪ Status updates every four (4) hours until severity is lowered, or containment/eradication has occurred
LOW /LEVEL 1	▪ IT Operations	▪ Provide notification to the recipients listed and provide details regarding: o Impacted hosts/services/account o Potential data loss assessment ▪ Include classification of data, if applicable ▪ Provide update through email ▪ Status updates every day until incident is closed

Step 7: Perform Notification/Escalation – External	
Perform external notification based on incident severity and applicable needs	
External Parties	**Recommended Circumstance**
▪ 3rd Party Incident Response / Forensics	▪ When an incident exceeds capabilities or expertise of the internal CSIRT team. Also, if scope of incident is significant making additional capacity a requirement.

▪ FBI / Law Enforcement	▪ FBI Notification: Submitting an FBI IC3 complaint/submission is highly recommended for any significant ransomware incident. The FBI will likely have additional undisclosed details of tactics and motives of the threat actors. In addition, notification of law enforcement is listed as a mitigating factor for consideration of civil enforcement by the US Treasury department ransomware advice.
▪ Cyber Insurance	▪ Notification for all severity 3 (High) classified incidents and/or if data loss of PII/PHI data is possible/probable
▪ External Legal Expertise	▪ Notification for incidents that exceed expertise/capabilities of internal/organizational legal teams ▪ Note: cyber insurance commonly assigns a breach manager who is legal counsel
▪ Other	▪ Contact to example external parties below may be warranted to ensure the party is available to assist /etc. o Managed server providers o External IT VARs that assist with key IT technology

Step 8: Cont'd Detection and Analysis

Cont'd discovery and analysis in order to determine the following

Task	Description
Determine C2 methods	Conduct analysis with focus on C2 IoCs discovery
Determine lateral movement methods	Conduct analysis with focus on lateral movement methods IoCs discovery
Determine impacted accounts (if applicable)	Conduct analysis with focus on determining all impacted/abused accounts within environment
Determine persistence methods	Conduct analysis with focus on persistence methods IoCs discovery

Step 9: Notification Event

Perform notification if new information is available and/or status update window is met. Use established communication processes to communicate the current situation to cyber security team, applicable organizational leadership, and other applicable parties.

Step 10: Containment

Conceive and implement containment strategies, monitor to confirm containment.

Task	Description

Document/communicate containment strategies	CSIRT team meets and determines containment strategies and monitoring methods
Implement containment	CSIRT team and IT operational support team implements containment strategies
Monitor containment	CSIRT team and IT operational support team monitors containment

Step 11: Notification Event

Perform notification informing appropriate groups of containment actions and new information if available. Use established communication processes to communicate the current situation to the cyber security team, applicable organizational leadership, and other applicable parties.

Step 12: Eradication

Conceive and implement eradication strategies, monitor to confirm eradication.

Task	Description
Document/communicate eradication strategies	CSIRT team meets and determines eradication strategies and monitoring methods
Implement eradication	CSIRT team and IT operational support team implements eradication strategies
Monitor eradication	CSIRT team and IT operational support team monitors eradication

Step 13: Notification Event

Perform notification informing appropriate groups of eradication actions and new information, if available. Use established communication processes to communicate the current situation to the cyber security team, applicable organizational leadership, and other applicable parties.

Step 14: Recovery

Conceive and conduct recovery strategies and tasks. Continue to monitor to confirm containment and eradication.

Task	Description
Conceive/document/communicate eradication strategies	CSIRT team and IT operational support team meets and determines recovery strategies and tasks
Conduct recovery	IT operational support team with the support of the CSIRT conducts recovery

Step 15: Notification Event

Perform notification informing appropriate groups of recovery actions and new information if available. Use established communication processes to communicate the current situation to the cyber security team, applicable organizational leadership, and other applicable parties.

Conduct recurring notifications (status updates) during the duration of the recovery effort at the defined intervals for the incident severity.

Step 16: Post Incident Activity	
Conduct post incident activities outlined below.	
Task	**Description**
Conduct after-action meeting	CSIRT team and IT operational support team meets to discuss incident including: ▪ What tools, trainings, or process change could have prevented the incident, mitigated impact, or resolved the incident sooner ▪ What worked well? ▪ What needs to be improved upon? ▪ What stakeholder support was integral to incident response success? ▪ What can incident staff or management improve upon? ▪ What information gaps remain in the investigation?
Complete incident documentation	Complete incident documentation as listed in the CSIRP.

Step 17: Notification Event
Perform final notification informing appropriate groups of incident close-out and summary of after-action meeting.

PLAN REVISION

Revision	*Date*	*Summary of Changes*	*Approved by*
1.0	3-21-2022	Document Creation	
1.1	5-6-2022	Addressed CLA requested revisions as of 5/4/2022	

Appendix

Incident Response Plan Supporting Frameworks and References

IR Plan Supporting References

NIST Cyber Security Framework - Framework for Improving Critical Infrastructure Cybersecurity v1.1

Applicable Controls: Respond (RS): RS.RP-1, RS.CO-1, RS.CO-2, RS-CO-3, RS.CO-4, RS.CO-5, RS.AN-2, RS.AN-3, RS.AN-4, RS.AN-5, RS.MI-1, RS.MI-2, MS.MI-3, RS.IM-1, RS.IM-2

URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST Special Publication (SP) 800-171 Revision 1 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Applicable Controls: 3.6 Incident Response – 3.6.1, 3.6.2, 3.63

URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

NIST Special Publication (SP) 800-53 Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations

Applicable Controls: IR-1 Incident Response Policy and Procedures, IR-2 Incident Response Training IR-3 Incident Response Testing, IR-4 Incident Handling, IR-5 Incident Monitoring, IR-6 Incident Reporting, IR-7 Incident Response Assistance, IR-8 Incident Response Plan, IR-9 Information Spillage Response, IR-10 Integrated Information Security Analysis Team

URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST Special Publication (SP) 800-61 Revision 2 - Computer Security Incident Handling Guide

URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST Special Publication (SP) 800-86 Revision 1 - Guide to Integrating Forensic Techniques into Incident Response

URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

US CERT Incident Management

URL: https://www.us-cert.gov/

HOC Cybersecurity Incident Response Team
(Reference *Section 5.0 "Response Team")*

Title	Current Staff	Telephone	Email
Executive Director	**Kayrine Brown (Acting)**	**240-627-9589**	**kayrine.brown@hocmc.org**
Chief Technology Officer	Karlos Taylor	240-627-9545	karlos.taylor@hocmc.org
Director of Risk Management	John Broullire	301-922-5129	john.broullire@hocmc.org
Chief Financial Officer	Timothy Goetzinger (Acting)	240- 528-4836	timothy.goetzinger@hocmc.org
Chief Compliance Officer	Darcel Cox	240-627-9427	darcel.cox@hocmc.org
Manager of Technical Operations	David Brody	240-627-9449	david.brody@hocmc.org
General Counsel	Aisha Memon	240-627-9740	aisha.memon@hocmc.org

Information Technology Division
Strategic Plan
FY2023 – FY2028

Effective Date:
July 1, 2022

Housing Opportunities Commission OF MONTGOMERY COUNTY

10400 Detrick Avenue
Kensington, MD 20895-2484
(240) 627-9400

HOUSING OPPORTUNITIES COMMISSION OF MONTGOMERY COUNTY INFORMATION TECHNOLOGY ("IT") DIVISION STRATEGIC PLAN

INTRODUCTION

According to Gartner: An IT strategy articulates clear vision and objectives and sets a roadmap to attain and maintain the strategy. The IT strategy should:

- Support existing business/operational priorities and enable achievement of new priorities;.
- Be anchored in core values and principles and balance visionary thinking with pragmatic operational realities;
- Provide an initial statement of direction to guide activity in all aspects of IT; and
- Be an on-gong process that needs continual refinement.

We believe it only right then to begin with the Vision and Mission of the Housing Opportunities Commission of Montgomery County ("HOC") itself for the purpose of ensuring alignment with priorities of the business, which we must play such a critical role in supporting.

HOC VISION: It is our vision that everyone should live in quality housing that is affordable, with dignity and respect. At HOC we believe this vision can be achieved by ensuring amenity rich, community-connected housing for all of Montgomery County's residents where all people can reach their fullest potential. We believe supportive programs, delivered through mission-aligned partnerships, help our customers improve their economic status, remain stably housed and reach the goals they hold for themselves and their families.

HOC MISSION: The Mission of HOC is to provide affordable housing and supportive services that enhance the lives of low- and moderate-income families and individuals throughout Montgomery County, Maryland so that:

- No one in Montgomery County lives in substandard housing;
- We strengthen families and communities as good neighbors;
- We establish an efficient and productive environment that fosters trust, open communication and mutual respect; and
- We work with advocates, providers and community members to maintain support for all of the work of the Commission.

The rapidly changing and innovative ways individuals are communicating and collaborating are demanding new technologies to be designed, acquired and delivered. It is paramount that we continue to lead by leveraging best practices, new information, and communication technologies in order to ensure the mission and vision of HOC may be achieved. This demand means that the Information Technology Division must increase the pace at which we offer, adapt and sunset services in order to meet these evolving demands.

Our strategic planning process utilized the following methodology:

- Review of current applications and infrastructure and determine opportunities for improvement to support HOC performance management and decision making;
- Assess current IT infrastructure, applications, and service delivery;
- Develop short-and long-term recommendations to address potential gaps; and
- Develop a roadmap to implement prioritized recommendations.

The document "HOC S trategic F indings" maintains the details of this year-long process.

Overall, we connected with HOC leadership across every division and engaged with more than 100 staff as we compiled feedback and suggestions during a comprehensive listening tour.

IT MISSION AND VALUES

The Information Technology Division empowers staff to effectively and equitably use information technology to teach, learn, innovate, collaborate, and achieve HOC's mission. As a division that has knowledgeable and diverse staff, we strive to build and maintain sound, advanced, secure information technology systems that serve the Montgomery County, Maryland community as well as financial and real estate partners.

Over the coming years, the Information Technology Division will build on our unique strengths and transform our systems and services to be secure, scalable and sustainable in order to meet the needs of an evolving community. In addition, we must use information and communication technology to modernize our administrative work-flows and streamline the flow of information between HOC's business functions and departments.

Through its mission, the Information Technology Division is committed to:

- Innovating HOC's technology systems and service delivery;
- Leading research computing, data analytics, high performance computing, and network technology;
- Partnering in a way that effectively and ethically guides people to be creative in a digitally connected world;
- Fostering a culture of engagement and service, making the Information Technology Division a place staff can grow and add value; and
- Supporting HOC's staff leadership, commissioners, and residents as they use technology to accomplish their goals.

The Information Technology Division's core values are:

- **Excellence in people, systems, and services**
  We are talented staff who work to ensure that our systems and services are reliable, useful, automated when feasible, and systematically evaluated.

- **Diversity and inclusion of people and ideas**

We are an inclusive team that encourages the free exchange of ideas with mutual regard and consideration for our differences.

- **Collaboration**
  We are a holistic team that works collaboratively to achieve our mission by respectfully listening to our clients and our colleagues.

- **Discovery and innovations**
  We are explorers who value new ideas and are willing to take risks and embrace failure as we build and solve for the future.

- **Integrity, transparency, and trust**
  We are transparent about our decisions, accept full responsibility for our plans and actions and believe that we will get the right results if we do the right things.

STRENGTHS

The following strengths represent the critical attributes that will enable the achievement of our mission. The Information Technology Division is committed to maintaining excellence in these areas:

We safeguard IT systems and HOC data
Facilitate secure and safe information technology systems and services by utilizing technology, compliance, and community engagement to reduce the risk of inappropriate disclosure, modification, or loss of information assets.

We enable innovative thinking and empowering technologies
Facilitate accessible, educational experiences providing opportunities for staff to learn and better leverage the technologies supplied by HOC.

We provide front-line support for our customers
Provide a quality, customer-focused “single point of contact” service desk for both general questions and information technology systems at HOC.

We make technology systems accessible and usable

We maintain and enhance infrastructure to enable communication
Provide a reliable and responsive telecommunication and network experience to anyone who utilizes voice and data communication systems across the entire HOC environment.

We have high-quality staff members
Develop a talented and motivated workforce that takes a customer-centric approach to their daily activities and works behind the scenes to ensure customers get a timely, quality, and consistent experience.

THE CHANGING LANDSCAPE

The changing landscape in information technology and society drives our institutional decisions and impacts our work at HOC. This plan accounts for the following trends:

- The need to anticipate and adjust to ever-changing social and political priorities as well as funding availability at the local, state, and national levels.
- The increasing demand for innovative housing solutions, practices, and means of delivery designed to foster collaboration, critical thinking, and creativity.
- The changes in demographics, which highlight the importance of promoting a context of cultural diversity and pluralism.
- The power of data and analytics that can drive proactive institutional decisions rather than just reflecting them.
- The truly mobile experience: The increased expectation for safe and reliable access anywhere and everywhere.
- The importance of successfully implementing hosted software solutions and adopting a cloud-first strategy for new systems and the struggle to achieve the full value of moving enterprise systems to the cloud.
- The juxtaposition of the increasingly pervasive and indispensable use of mobile devices and the digital divide faced by those who have restricted access and/or fluency to equally embrace the full potential of mobile technology.
- The intensifying requirements for data security, privacy, and access.
- The relentless need to retain qualified and motivated employees as a critical factor in our organization's success.

INFORMATION TECHNOLOGY DIVISION FIVE STRATEGIC INITIATIVES

We endeavor to leverage and build on our organization strengths and capabilities to create the best future for the HOC community, as well as our partners. To achieve this, we will focus and invest in five initiatives:

1. **INNOVATE AND INTEGRATE ADMINISTRATIVE SYSTEMS**
   The Information Technology Division will partner with HOC stakeholders to transform administrative systems and services in a way that provides timely, comprehensive, and accurate information to our business partners, eases administrative burdens, integrates institutional data, and streamlines the flow of information to maintain consistency between business functions and departments.

2. **ENHANCE TECHNOLOGY SYSTEMS AND SERVICES**
   The Information Technology Division will lead HOC-wide efforts to design, build, and support state-of-the-art technology that encourages collaborations, data driven decision making, and exploration of innovative ideas.

3. **PROMOTE EXCELLENT, SECURE, AND COMPLIANT SERVICES**
   The Information Technology Division will be recognized for its level of service efficient systems, quality of services, streamlined operations, and resource stewardship.

4. **FOSTER PARTNERSHIPS AND COLLABORATION**
   The Information Technology Division will partner with HOC stakeholders to collaboratively shape the vision, pace, and priorities of IT systems and services and to create policies that balance institutional interests and support the HOC mission.

5. **DEVELOP AND EMPOWER OUR TALENT**
   Within the Information Technology Division, we have careers, not just jobs. Our workforce will be well-trained, knowledgeable, and recognized for its strong commitment to our mission. The Information Technology Division will maintain a diverse workforce that is committed to increasing inclusiveness and collaboration as the standard, not the exception.

1. INNOVATE AND INTEGRATE ADMINISTRATIVE SYSTEMS

What is our objective?

The Information Technology Division will partner with HOC stakeholders to transform administrative systems and services in a way that provides timely, comprehensive, and accurate information to our HOC community, eases administrative burdens, integrates institutional data and streamlines the flow of information to maintain consistency between HOC business functions and departments.

Why is this relevant?

To meet our mission, HOC, more than ever, needs to take a holistic approach with people, processes and technology. By modernizing our administrative processes and systems, HOC will be able to serve our community more efficiently with improved experience.

What are our specific planned actions?

- The Information Technology Division will partner with stakeholders to provide support with technology solutions that improve the administrative systems.
- The Information Technology Division will collaborate with stakeholders to identify ways to improve data management across the institution (including access, consistency, and accuracy) for partners, staff, and constituents.
- The Information Technology Division will work with stakeholders to ensure new systems create a unified and easy-to-use experience for constituents and staff.
- The Information Technology Division will be a critical member of the institutional team that is developing Yardi for enterprise resource planning (ERP) resources.

How will we know if we have succeeded?

- The Information Technology Division is recognized by HOC stakeholders as the partner of choice that helps enable new business processes and systems.
- There is a reduction of duplications, mistakes and missing records in the administrative systems.
- By July 1, 2023, Yardi will be upgraded to the most current version and modules.
- By July 1, 2023, consistent collaboration is taking place between the Information Technology Division and all other divisions.
- In collaboration with stakeholders, we will monitor staff satisfaction to ensure that our approach is easy to engage, responsive and provides information relevant to HOC's success.

2. ENHANCE TECHNOLOGY SYSTEMS & SERVICES

What is our objective?

The Information Technology Division will lead HOC-wide efforts to design, build, and support state-of-the-art technology that encourages collaborations, data driven decision making, and exploration of innovative ideas.

Why is this relevant?

State-of-the-art technology is an essential foundation for effective work. For HOC staff to drive innovation and achieve efficiency, they must have easy access to modern technology relevant to their business processes and goals.

What are our specific planned actions?

- Identify a team of talented staff able to redesign, promote, and support technology services that meet the diverse needs of our HOC divisions and their collaborators.
- Provide a dedicated, advanced, compliant, cost-effective, and easy-to-use computing environment (both on-premises and in the cloud) that meets the growing needs of our community, including sensitive and protected information.
- Update documentation, design training, and expand our technology consultation for staff.
- Collaborate with the other division to develop a sustainable technology plan that aims at optimizing investments and minimizing administrative overhead and redundancy.

How will we know if we have succeeded?

- By July 2023, we have an expanded team of talented staff to lead our efforts to redesign the existing services and innovate new ones.
- Where appropriate we have reviewed and restructured our existing technology services to ensure compliance and cost-effectiveness and to reduce redundancies.

3. PROMOTE EXCELLENT, SECURE, AND COMPLIANT IT AND SERVICES

What is our objective?

The Information Technology Division will be recognized for its efficient system, quality of services, streamlined operations, and resource stewardship.

Why is this relevant?

Improving the quality and efficiency of our services allows the HOC community to perform their work functions effectively and without impediment.

What are our specific planned actions?

- The Information Technology Division will create a portfolio of projects specifically aimed at improving service delivery at HOC.
- The Information Technology Division will develop and execute a strategic communications plan to educate the HOC community about available Information Technology Division services and how they can improve productivity.
- The Information Technology Division will build and lead a culture of secure and compliant IT services.

How will we know if we have succeeded?

- By May 2024, new services enter their operation phase with clearly defined objectives, fiscally responsible cost considerations, assessment criteria, and thresholds for decommissioning.
- By July 2024, we have formally assessed and inventoried services and determined their level of value, cost and utilization.
- By September 2024, partners and customers have increased confidence in the Information Technology Division by understanding the value they receive.
- We receive positive feedback on our customer support survey feedback scores.

4. FOSTER PARTNERSHIPS AND COLLABORATION

What is our objective?

The Information Technology Division will partner with HOC stakeholders to collaboratively shape the vision, pace, and priorities of IT systems and services to create policies that balance institutional interests and support the HOC mission.

Why is this relevant?

To become recognized for fostering innovation in technology and service delivery, we have to be up to speed with (and ultimately ahead of) trends. We must cultivate partnerships within the division and throughout HOC to guide critical IT decisions and to proactively identify additional opportunities.

What are our specific planned actions?

- The Information Technology Division will identify a strategy to proactively collaborate and communicate with HOC stakeholders, as a trusted partner, on decisions pertaining to the IT systems and services used at HOC.
- The Information Technology Division will actively engage with its staff when making technical decisions.
- The Information Technology Division will make its priorities transparent to the HOC community.

How will we know if we have succeeded?

- We have collaborated to develop and implement a communication plan to inform strategic decisions about HOC IT systems and services.
- We have hosted at least two HOC employee engagements to collaboratively share data, provide updates and gather feedback by November 2023.
- Information Technology Division managers have participated in governance group meetings to listen to, receive, and synthesize feedback.

5. DEVELOP AND EMPOWER OUR TALENT

What is our objective?

Within the Information Technology Division, we have careers, not just jobs. Our workforce will be well-trained, knowledgeable, and recognized for its strong commitment to our mission. The Information Technology Division will maintain a diverse workforce that Is committed to increasing inclusiveness and collaboration as the standards, not the exception.

Why is this relevant?

In order for innovation to occur, the division must foster an environment where each employee is valued, heard, and encouraged to think outside of the box. In every aspect of a business, diverse backgrounds and skills are needed for achieving success and are key to attaining growth. While striving toward a more collaborative environment, Information Technology team members must feel empowered to perform as individuals and to work together toward a common task and project goal.

What are our specific planned actions?

- We will build resiliency into our team so that we have prepared for staff unavailability and free up time for our staff to test new ideas and work on innovative projects.
- We will identify a variety of ways to recognize staff members who consistently exemplify Information Technology Division values and support the mission of HOC with innovative solutions to IT challenges.

How we will know if we have succeeded?

- We have conducted analysis focusing on single points of failure and gaps in knowledge and identified paths for resilience and succession by July 2023.
- Thirty-five (35%) of Information Technology Division staff have participated in professional development opportunities.

Housing Opportunities Commission OF MONTGOMERY COUNTY

10400 Detrick Avenue
Kensington, MD 20895-2484
(240) 627-9400

HOUSING OPPORTUNITIES COMMISSION OF MONTGOMERY COUNTY DATA CLASSIFICATION GUIDELINES

PURPOSE

The purpose of this document is to explain that members of the HOC community who extract, post, or use **Sensitive Information** outside HOC's secured infrastructure applications are required to know the security of the application or service before storing **Sensitive Information** in such locations. In addition to HOC workstations, Active Directory shared locations, and mobile devices, this includes HOC supported web applications, Internet based cloud services, and departmental websites hosted on HOC servers. Web based cloud services include, but are not limited to, Google Suite and AODOCS, that are available to the entire HOC staff, or any other cloud based service or application used by specific administrative departments.

BACKGROUND

The Information Technology Division ("IT") protects HOC's sensitive data from unauthorized access or inappropriate use by enforcing technical and procedural security controls for infrastructure based systems and applications (e.g., Yardi) that store and/or process sensitive information. However, the availability of local workstations, shared drives, and HOC-hosted and Internet-based applications and services provides the opportunity for otherwise secure data to be extracted from infrastructure based systems and applications and used outside IT security control. Before **Sensitive Information** may be extracted from, posted, or used outside of HOC's protected infrastructure systems, including for use in any HOC web or cloud based application, users must ensure that the security of the storage location, web application or service equals the level of security protection applied to the data within HOC's infrastructure based systems.

SYSTEM RISK LEVEL DESIGNATIONS

HOC-maintained infrastructure systems and applications (including hardware, software and associated devices) store, process and protect various types of sensitive information under HOC control. IT uses a security risk assessment process to assign a security risk level to **Sensitive Information**, and to the systems and applications that maintain and process **Sensitive Information** in HOC's physical computing infrastructure. Risk level designations for IT maintained systems are based on the sensitivity of the data maintained or processed by each system or application. HOC systems or applications containing any Information designated as sensitive by laws or regulations, for example, have the highest level security designation (Level 3) and are the most securely protected. Systems or applications containing any personally identifiable information collected and retained by HOC about any member or affiliate of the HOC community, or any sensitive HOC proprietary institutional information, have a slightly lower (Level

2), although still significant, level of protection. Systems with the lowest level security designations (Level 1 and Level 0) do not collect, process, or store any sensitive information.

APPROPRIATE DATA USE

Members of the HOC community, who use any of the services listed in TABLE 1 below, must do so in accordance with the policies and guidelines that govern general computer use on premises. Users who have access privileges to any of HOC's infrastructure systems also must be aware of the sensitivity level of any data extracted from an infrastructure system that they may store in one of these applications. Before doing so, users must ensure the security risk level of the application is consistent with the level of protection required for the extracted data to be stored or processed and have obtained approval from your supervisor or manager (Contact IT if there are questions about the use of sensitive information in any HOC infrastructure system). The security risk level of the services listed in TABLE 1 have been evaluated based on the system risk level designations described above for HOC's infrastructure based systems and applications. **Sensitive Information** belonging to multiple sensitivity levels must be treated according to the highest level of sensitivity.

HOC considers information (i.e., data) to be sensitive if it is, or has been, determined to be confidential because of laws, regulations, HOC policy, or by agreement, whether the information is in physical or electronic format. Sensitive information includes the following types of information:

- **Level 3**. Information designated as sensitive by laws or regulations, such as:
    - Medical records covered by the Health Information Portability and Accountability Act (HIPAA);
    - Banking and credit card records covered by the Payment Card Industry (PCI) data security standards.

  Information of this type is <u>always sensitive</u> if personal identifiers (e.g. name, SSN, HOC ID, etc.) are, or can be, associated with the medical or banking records. This type of sensitive information receives the highest level of security protection within HOC's infrastructure systems and must never be extracted from those systems without express written permission.

- **Level 2**. Personally identifiable information collected and retained by HOC about any member or affiliate of the HOC community on behalf of HOC. This includes:
    - An individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:
        - Social Security Number (SSN);
        - Driver's license number, state identification card number, or other individual identification number issued by a unit;
        - Passport number or other identification number issued by the United States government;
        - Individual Taxpayer Identification Number;
        - Financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, which would permit access to an individual's account.

- Any individual or combination of data elements that, if disclosed without authorization, identifies a specific individual and could place the individual's privacy, or HOC, at risk.

This type of sensitive information also is protected securely within HOC's infrastructure systems and must be secured with the same level of protection if extracted from those systems. HOC leverages perimeter firewall security as well as endpoint detection and response security controls.

- **Level 1**. HOC proprietary institutional information, including:
  - Housing related records covered by a Privacy Act;
  - Sensitive institutional information such as intellectual property, project proposals, or patent applications; and
  - Administrative Correspondence containing personally identifiable information or otherwise marked confidential due to its content.

This type of sensitive information also is protected securely within HOC's infrastructure systems and must be secured with the same level of protection if extracted from those systems. HOC leverages perimeter firewall security as well as endpoint detection and response security controls.

- **Level 0**. Public Information not classified as level 1-3.

Table 1 Approved Risk Level by Storage Category or Device

	Approved Risk Level				
Service	**0**	**1**	**2**	**3**	**Comments**
HOC Owned Workstations	✓	✓			Level 0 and 1 data can be stored locally on your workstation. If you have level 2 data, this must be stored on the active directory, box.com, or encrypted portable electronic storage obtained from IT.
Personally Owned Workstations	✓				Personally owned workstations can only be used to store HOC **public** information.
Active Directory Centralized File Share	✓	✓	✓		
Mobile Devices	✓				Mobile devices, whether HOC or personally-owned, should be used only with **public** HOC information.
Google Apps	✓	✓			
Email	✓	✓			Never send level 2 or higher data through email regardless of the email provider. Send a link to data (e.g., link to **Google)**
Microsoft OneDrive	✓	✓			

Service	0	1	2	3	Comments
Public Cloud Storage Sites (e.g. Dropbox)	✓				Some publicly available cloud servers are located outside U.S. territory.
Portable Electronic Storage Media	✓	✓			Never store level 2 or 3 data on portable electronic storage media such as USB devices, CD/DVD ROM, or external hard drives.
Encrypted Portable Electronic Storage Media	✓	✓	✓	✓	If you need to store Level 2 or 3 data, work through IT to get an approved encrypted device. Level 3 data must be explicitly approved by IT.

Users must assess the security level of any service or application not listed in Table 1 before posting or storing Sensitive Information in such locations. If you have questions, please contact the IT Division.

Violation of these Data Classifications Guidelines or other HOC policies may result in temporary or permanent restriction of access privileges to services, or other measures detailed in the Information Technology and Acceptable Use of Information Technology Infrastructure and Resources Policy ("IT Policy"), HOC Personnel Policy, and the Collective Bargaining Agreement.

PLAN REVISION

Revision	*Date*	*Summary of Changes*	*Approved by*
1.0	3-2-2022	Document Creation	
1.1	5-6-2022	Addressed CLA requested revisions as of 5/4/2022	

M E M O R A N D U M

TO: Housing Opportunities Commission of Montgomery County
Administrative and Regulatory Committee

VIA: Kayrine V. Brown, Acting Executive Director

FROM:

Staff: David Brody	Division: Information Technology	Ext. 9449
Irma Rodriguez	Division: Information Technology	Ext. 9415
Karlos Taylor	Division: Information Technology	Ext. 9454

RE: **Technology Policy and Acceptable Use Policy:** Approval of Information Technology and Acceptable Use of Information Technology Infrastructure and Resources Policy to Reflect Current Processes and Risks

DATE: May 16, 2022

STATUS: **Consent _____ Deliberation ___X___ Status Report____ Future Action_____**

OVERALL GOAL & OBJECTIVE:

To request that the Administrative and Regulatory Committee recommend to the Housing Opportunities Commission ("HOC") of Montgomery County the adoption of the Information Technology and Acceptable Use of Information Technology Infrastructure and Resources Policy ("IT Policy") to reflect current processes and risks. In addition, to authorize the Acting Executive Director, or her designee, to implement the IT Policy.

BACKGROUND:

The Information Technology and Acceptable Use of Information Technology Infrastructure and Resources Policy ("IT Policy") will supersede the Technology Policy, last revised in April 2006.

Information Technology ("IT") policies are designed to help organizations and businesses use, operate, and manage IT infrastructure and systems effectively and efficiently. In so doing, IT resources and services are available to support business activities and operations as well as ensure continuity and meet regulatory, legal, and statutory requirements. Given the continually evolving environment in IT, outdated policies and procedures can create conflict between processes actually occurring and documented procedures.

The IT Policy will provide expectations and guidelines for those who use and manage IT resources and services, in alignment with current IT practices regarding user responsibilities and prohibited uses, intellectual property, privacy, monitoring, reporting, violation and disciplinary action, and user policy acknowledgement.

ISSUES FOR CONSIDERATION:

Does the Administrative and Regulatory Committee wish to join staff's recommendation to the Housing Opportunities Commission of Montgomery County to adopt the proposed IT Policy?

TIME FRAME:

For discussion by the Administrative and Regulatory Committee at its meeting on May 16, 2022. For formal Commission action on June 8, 2022

STAFF RECOMMENDATION & COMMISSION ACTION NEEDED:

Staff recommends that the Administrative and Regulatory Committee join staff's recommendation that the Commission adopt the proposed IT Policy.

Housing Opportunities Commission OF MONTGOMERY COUNTY

10400 Detrick Avenue
Kensington, MD 20895-2484
(240) 627-9400

HOUSING OPPORTUNITIES COMMISSION OF MONTGOMERY COUNTY INFORMATION TECHNOLOGY AND ACCEPTABLE USE OF INFORMATION TECHNOLOGY INFRASTRUCTURE AND RESOURCES POLICY

STATEMENT OF POLICY

Purpose

This Information Technology and Acceptable Use of Information Technology Infrastructure and Resources Policy ("IT Policy") provides the Housing Opportunities Commission of Montgomery County's ("HOC") expectations and guidelines to those who use and manage its Information Technology ("IT") resources and services. This policy is current as of July 2022, and supersedes the Technology Policy of April 2006. It will remain in effect until such times that revisions are necessary.

HOC's IT Division provides resources to the agency to enable it to provide affordable housing and supportive services that enhance the lives of low- and moderate-income families and individuals throughout Montgomery County, Maryland so that:

- No one in Montgomery County is living in substandard housing;
- HOC can strengthen families and communities as a good neighbor;
- HOC can establish an efficient and productive environment that fosters trust, open communication and mutual respect; and
- HOC can work with advocates and providers to enhance support for residents of Montgomery County.

Access or use of IT resources that interferes, interrupts, or conflicts with these purposes is not acceptable and will be considered a violation of this IT Policy.

Scope

This IT Policy, and all policies referenced herein, apply to the entire HOC community including staff, residents, volunteers, administrative officials, authorized guests, commissioners, delegates, and independent contractors (the "User(s)") who use, access, or otherwise employ, locally or remotely, HOC IT resources, whether individually controlled, shared, stand-alone, or networked.

This IT Policy specifically incorporates by reference the Information Security Assurance Policy ("ISA Policy"), Data Classification Guidelines and the Cyber Incident Response Plan. All Users are responsible for reviewing these documents in conjunction with this IT Policy.

Definitions
IT resources include computing, networking, communications, application, telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, cloud-based vendors, Software as a Service (SaaS) vendors, and any related materials and services.

USER RESPONSIBILITIES AND STATEMENT OF PROHIBITED USES

A. Intent of Use

Only authorized Users have the privilege to access and use IT resources. Access and use is limited to the purposes that are consistent with the mission and administrative goals of HOC.

Users are expected to uphold the standards and principles of HOC while using IT resources and are required to respect the rights of others at all times. Users are prohibited from using any portion of IT resources to post or transmit any information, including data, text, files, links, software, chat, collaboration, communication, or other content ("Content") that is abusive, disparaging, discriminatory, hostile, combative, threatening, harassing, intimidating, defamatory, pornographic, or obscene. Users who do not respect the Intent of Use of IT resources may be held in violation of this IT Policy.

B. Username

HOC recognizes that common practice in computing, online or otherwise, involves use of a "username", "login", "AccessIT ID", or "screen name" (collectively, "Username") that may be different from the User's legal name. Using someone else's name or assuming someone else's identity without appropriate authorization, however, is a violation of HOC's principles and this IT Policy.

Users may not use IT resources under false name, identification, email address, signature, or other medium of any person or entity without proper authorization. HOC prohibits such use of a Username for the purposes of misrepresentation or an attempt to avoid legal or other obligations. Any such unethical use may constitute a violation of this IT Policy.

C. Passwords

When choosing a password for access to IT resources, or portions thereof, Users must adhere to the following rules so as to prevent unauthorized access through any User's password.

1. Use a different password for each account.
2. Do not write down password(s) on a piece of paper or record them in a file.
3. Do not use the following items to formulate passwords:
    1. Birth dates;
    2. Names (First, Last, or any combination);
    3. Unaltered words that could be found in a dictionary, including non-English words, and words spelled backwards;
    4. Telephone numbers;
    5. Social Security numbers;
    6. Famous or other proper names; or
    7. Alphabet or keyboard sequences (e.g., "QWERTY").

4. Passwords must meet the following criteria:
    1. Consist of eight (8) characters or more;
    2. Contain at least one (1) numeric;
    3. Contain at least one (1) uppercase and one (1) lowercase character; and
    4. Does not contain any of the following special characters: @& /

Passwords must not be reused; Users are required to change their password every (90) days.

Users should not have an expectation of privacy regarding Content located in HOC's IT resources, whether that Content is protected by a Username and password, or otherwise.

D. Additional Responsibilities

All Users must fully comply with the standards and responsibilities of acceptable use as outlined in:

1. All applicable provisions of HOC's employee handbooks, agreements, and any and all other policies, standards, and procedures established by HOC;
2. This IT Policy in its entirety including the related policies as defined in the Related Policies and Procedures section;
3. All local, state, federal, and international laws;
4. All application and/or software license agreements acquired by HOC and its authorized units; and
5. All applicable HOC policies and procedures including sexual harassment and non-discrimination.

Users must adhere to the following responsibilities:

1. Self-policing of passwords and access codes as set forth above;
2. Respecting and protecting the confidentiality, integrity, and availability of all HOC IT resources;
3. Ensuring that all data and files that the User accesses, transmits, and/or downloads are free from any computer code, file, or program which could damage, disrupt, expose to unauthorized access, or place excessive load on any computer system, network, or other IT resources;
4. Reporting any security risk or code, file, or program, including computer viruses, Trojan horses, worms, or any other malware that affects any IT resources, including any owned or operated by the User; and
5. Properly backing up appropriate User systems, software, and data.

E. Additional Prohibited Uses

Users are prohibited from accessing or using IT resources in the following manners:

1. Initiating or participating in unauthorized mass mailings to news groups, mailing lists, or individuals, including, but not limited to, chain letters, unsolicited commercial email (commonly known as "spam"), floods, and bombs;
2. Giving others, by password or other means, unauthorized access to any User account or IT resources;
3. Seeking to, without authorization, wrongly access, improperly use, interfere with, dismantle, disrupt, destroy, or prevent access to, any portion of IT resources including User or network accounts;

4. Violating or otherwise compromising the privacy, or any other personal or property right, of other Users or third parties through use of IT resources;
5. Disguising or attempting to disguise the identity of the account or other IT resources being used including "spoofing" resource addresses, impersonating any other person or entity, or misrepresenting affiliation with any other person or entity;
6. Using IT resources to gain or attempt to gain unauthorized access to networks and/or computer systems;
7. Engaging in conduct constituting wasteful use of IT resources or which unfairly monopolizes them to the exclusion of others;
8. Engaging in conduct that results in interference or degradation of controls and security of IT resources;
9. Exploiting or otherwise using IT resources for any commercial purpose, unless expressly authorized by HOC in writing;
10. Engaging in computer crimes or other prohibited acts;
11. Intentionally or unintentionally violating any applicable local, state, federal, or international law;
12. Knowingly or negligently running, installing, uploading, posting, emailing, or otherwise transmitting any computer code, file, or program, including, but not limited to, computer viruses, Trojan horses, worms, or any other malware, which damages, exposes to unauthorized access, disrupts, or places excessive load on any computer system, network, or other IT resource; and
13. Using any IT resource, including email or other communication system to intimidate, insult, embarrass, or harass others, or to interfere unreasonably with an individual's work or to create a hostile or offensive environment.

INTELLECTUAL PROPERTY

As each User should have an expectation that others will not abuse his or her intellectual property rights, every User must also respect the intellectual property rights of others, including those of other Users, all members of the HOC community, and all third parties.

Potential violation of intellectual property laws and rights is not merely limited to unauthorized downloading of copyrighted movies, television shows, music, and software through file-sharing software. Rather, the concept of intellectual property broadly covers all copyrighted works, trademarks, patents, and other proprietary and confidential information.

HOC requires every User to adhere to a strict policy of respecting intellectual property rights. Infringing and illegal uses may involve:

- Unauthorized copying, sharing, and use of digital videos or images, digital music as well as logos and other marks;
- Unauthorized copying, sharing, or installation of software, including commercially licensed software as well as "shareware"; and
- Unauthorized copying, sharing, or use of copyrighted, or otherwise proprietary, data or collections of data.

PRIVACY

A. Standard Use Privacy

HOC reserves the right to access, inspect, examine, monitor, intercept, remove, restrict, and take possession of all HOC owned and operated IT resources, including but not limited to, electronic mail, network connectivity, hard disks, printed media, devices, data, software, printers, voice mail, removable media, fax machines, scanners, computers, mobile devices, telephony equipment, connected devices, laptops, documents, and other files.

HOC also reserves the right to access, inspect, examine, monitor, intercept, remove and restrict use and access to the IT resources indicated above.

HOC may exercise these rights for various reasons, including but not limited to:

- Ascertaining whether Users are using the systems in accordance with this IT Policy and other HOC guidelines;
- Preventing, investigating, or detecting unauthorized use of HOC's systems;
- Ensuring compliance with third party agreements and guidelines; and
- Ensuring compliance with applicable laws and regulations.

Users are expected and obligated to use such IT resources in a manner consistent with the purposes, objectives, and mission of HOC and this IT Policy.

Except where applicable law provides otherwise, Users should have no expectation of a reasonable level of privacy while accessing or using HOC IT resources. For example, issuance of a password or other means of access is to assure appropriate confidentiality of HOC-related information and files. However, it does not guarantee privacy, especially for personal or unlawful use of IT resources.

Users should note that HOC may also require back-up and caching of various portions of IT resources; logging of activity; monitoring of general usage; and other activities that are not directed against any individual User or User account, for protecting HOC's IT resources and systems, maintaining security and maintenance, or restoring normal operations of IT resources.

HOC reserves the right to examine, use, and disclose any data or content found on HOC's IT resources for the purposes of furthering the health, safety, discipline, legal rights, security, or intellectual or other property of any User or other person or entity. Information that HOC gathers from such permissible monitoring or examinations may also be used in disciplinary actions. Such information may be disclosed to law enforcement officials when necessary.

Users are responsible for the security of their own User IDs and passwords. Passwords must not be shared with other persons.

B. Website Privacy

HOC uses the following practices and procedures for its website. HOC reserves the right to change these practices and procedures at any time without prior notice. The following is not intended and should not be interpreted as a contract of any nature, either stated or implied. The Privacy Policy may be found here:

https://www.hocmc.org/extra/91-privacy-policy.html

MONITORING, REPORTING, VIOLATION, AND DISCIPLINARY ACTION

A. Monitoring

As noted above, HOC may, but is not required to, monitor, block, or otherwise prevent inappropriate use of IT resources. Nonetheless, in the event of a violation or failure to comply with this IT Policy, HOC may monitor any User's access and use of IT resources in order to determine whether violations are taking place. If violations are found, HOC may initiate charges and impose appropriate sanctions by following the various processes and procedural safeguards that are applicable to the User's employment or program status.

B. Reporting

Users have an obligation to report violations of this IT Policy as well as any potential security or other breach of any portion of IT resources. Reporting of any such violations or other issues involving the inappropriate use of IT resources should be referred to:

- The Chief Technology Officer (or delegate); and
- The Division Director of the person making the report.

C. Violations

A violation of this IT Policy is considered a violation of HOC's principles, objectives, and standards. Depending on the severity of the violation, it may also violate HOC's other policies or even local, state, federal, or international law. HOC may impose penalties ranging from the termination of the User's access to IT resources to disciplinary review and further action including non-reappointment, discharge, or dismissal. In cases involving egregious violations, HOC may initiate legal action or cooperate with an action brought by applicable authorities or third parties.

D. Disciplinary Action

Users who fail to fulfill their responsibilities and engage in prohibited conduct are subject to disciplinary action imposed by HOC. Staff are subject to disciplinary action including reprimand, suspension, and dismissal under their respective handbook and collective bargaining agreements. Depending on the nature and severity of the violation, sanctions can range from various levels of warnings to immediate termination of employment or program participation.

HOC will exercise good faith and proper discernment in its enforcement of this IT Policy. HOC will respect the freedom to which Users are entitled, insofar as legally required. Under no circumstances shall HOC be liable to any User or third party for any violation, including illegal or improper acts that any User commits through the use of IT resources.

USER OBLIGATION TO REVIEW AND ACCEPT

HOC will periodically update this IT Policy. Prior to accessing and using IT resources, each User represents and acknowledges that the User has checked and read this IT Policy as well as the ISA Policy on a regular basis so as to be informed of any changes hereto. If any User does not agree to check this IT Policy for revisions on a regular basis, said User may not use IT resources. As such, Users will be required to sign an acknowledgement of this IT Policy, ISA Policy and Data Classification Guidelines as part of their onboarding process. Additionally, Users will be required annually to review and sign an acknowledgment of both policies and guidelines, following their mandatory cybersecurity training.

PLAN REVISION

Revision	*Date*	*Summary of Changes*	*Approved by*
1.0	3-2-2022	Document Creation	
1.1	5-6-2022	Addressed CLA requested revisions as of 5/4/2022	

M E M O R A N D U M

TO: Housing Opportunities Commission of Montgomery County
Administrative and Regulatory Committee

VIA: Kayrine V. Brown, Acting Executive Director

FROM:

Staff: David Brody	Division: Information Technology	Ext. 9449
Irma Rodriguez	Division: Information Technology	Ext. 9415
Karlos Taylor	Division: Information Technology	Ext. 9454

RE: **Information Security Assurance Policy and Telework Policy:** Approval of Information Technology Security Assurance Policy to Incorporate Changes in Systems Infrastructure, New Technologies, and User Environment to Reflect Current Processes and Risks and Approval of the HOC Telework Policy

DATE: May 16, 2022

STATUS: **Consent _____ Deliberation ___X___ Status Report____ Future Action_____**

OVERALL GOAL & OBJECTIVE:

To request that the Administrative and Regulatory Committee recommend to the Housing Opportunities Commission ("HOC") of Montgomery County the adoption of the Information Security Assurance Policy ("ISA Policy") and the HOC Telework Policy, which is referenced in the ISA Policy and resulted from the CliftonLarsonAllen LLP's ("CLA"s) Management Letter recommendations. In addition, to authorize the Acting Executive Director, or her designee, to implement the ISA Policy and the HOC Telework Policy.

BACKGROUND:

The **Information Security Assurance Policy ("ISA Policy")** will serve in conjunction with the Information Technology and Acceptable Use of Information Technology Infrastructure and Resources Policy ("IT Policy") to supersede the Technology Policy, last revised in April 2006.

Information Technology ("IT") security policies are essential to secure sensitive corporate information for organizations and businesses. By adhering to requirements within these policies and procedures therein, the risks of security threats (i.e., unauthorized access, disclosure, corruption, loss, and disruption in both physical and electronic formats) are mitigated. These policies also set forth measures for corrective action and audit. Outdated policies and procedures can create conflict between processes actually occurring and documented procedures, which may in turn, affect practices implemented to guard against the ever widening security threat landscape in IT

The ISA Policy defines required technical controls and security configurations; user action and prohibitions; and acceptable use of IT resources and services; in order to ensure integrity and availability of the HOC data environment in accordance with current industry practices.

The ISA Policy incorporates and addresses the following processes:

1. Statement of policy and management responsibilities;
2. Employee responsibilities;
3. Identification and authentication;
4. Network resource connectivity;
5. Antivirus/Anti-Malware/Software;
6. Encryption;
7. Building and physical access;
8. Telework;
9. Mobile device management;
10. Disposal of hardware;
11. Change management;
12. Data integrity;
13. Security and awareness training;
14. Security management process;
15. Employee background checks;
16. Discovery policy - procedures and disclosure;
17. eDiscovery policy – retention; and
18. Cyber breach and notification procedures

The HOC Telework Policy is referenced in *Chapter 8, "Telework"* of the ISA Policy and presented separately as an attachment to this memorandum for review and discussion.

The key terms of the Telework Policy are incorporated in the Telework Program of the Collective Bargaining Agreement ("CBA"), which were presented and approved by the Commission on May 4, 2022, and summarized below:

- The Telework Policy outlines the General Roles and Responsibilities of multiple parts of the organization for coordinating and managing the telework program, including 1) **Human Resources to** Administers of HOC's Telework Program, 2) **HOC Departments/Divisions for its** Implementation, 3) **Supervisors to facilitate Employee and Team Telework Success, and 4) Teleworkers** to maintain or enhance services and outcomes for HOC customers.
- Participation in Telework is voluntary. The employee participation in Telework may fall in one of the following categories: 1) Recurring telework with employees working from a remote location on a regular, recurring basis up to five days per week; or 2) Intermittent/Situational telework with employees generally working on-site, but would telework for limited periods of time based on either circumstances impacting the availability of the HOC worksite, or job responsibilities that could best be accommodated by working remotely.

- Eligible Positions: For the purposes of the Telework Program, HOC has developed a list of standards for the determination of position eligibility.
- Employee Requests to Telework: Employees may request to participate in the Telework Program by completing a Telework Application. The application is evaluated to ensure that the duties and responsibilities within the position can be accomplished through telework, provided it does not negatively affect service delivery or performance.
- Other components of the Telework Program cover:
    - Continued Participation in Telework;
    - Computer Requirements – Mandatory HOC-issued laptop;
    - Employee Workspace, Work Schedule/Time and Attendance;
    - Customer Service, Performance & Telework;
    - Security and Data sharing;
    - Terms and Conditions of Telework Agreements; and
    - Discontinuation of Telework and the appeals process.

ISSUES FOR CONSIDERATION:

Does the Administrative and Regulatory Committee wish to join staff's recommendation to the Housing Opportunities Commission of Montgomery County to adopt the proposed ISA Policy?

Does the Administrative and Regulatory Committee wish to join staff's recommendation to the Housing Opportunities Commission of Montgomery County to adopt the proposed HOC Telework Policy?

TIME FRAME:

For discussion by the Administrative and Regulatory Committee at its meeting on May 16, 2022. For formal Commission action on June 8, 2022.

STAFF RECOMMENDATION & COMMISSION ACTION NEEDED:

Staff recommends that the Administrative and Regulatory Committee join staff's recommendation that the Commission adopt the proposed ISA Policy.

Staff also recommends that the Administrative and Regulatory Committee join staff's recommendation that the Commission adopt the proposed HOC Telework Policy.

Housing Opportunities Commission OF MONTGOMERY COUNTY

10400 Detrick Avenue
Kensington, MD 20895-2484
(240) 627-9400

HOUSING OPPORTUNITIES COMMISSION OF MONTGOMERY COUNTY
INFORMATION SECURITY ASSURANCE POLICY

1. INTRODUCTION

1.1 Purpose

This Information Security Assurance Policy ("ISA Policy") defines the technical controls and security configurations which Users and Information Technology ("IT") administrators are required to implement in order to ensure the integrity and availability of the data environment at the Housing Opportunities Commission of Montgomery County ("HOC"). It serves as a central policy document with which all employees, contractors, volunteers and temporary staff must be familiar and defines actions and prohibitions that all Users must follow. The ISA Policy provides IT managers within HOC with policies and guidelines concerning the acceptable use of HOC technology equipment, email, internet connections, voicemail, facsimile, future technology resources and information processing.

The requirements and restrictions defined in this document shall apply to network infrastructures, databases, External Media, Encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. All HOC employees, temporary workers, contractors, and subcontractors working at all locations must adhere to this ISA Policy.

Security Policy Statement

- HOC must integrate information security principles into all aspects of HOC's activities.
- HOC must ensure that reasonable security policies, standards, controls, processes, practices, and procedures are established and maintained to safeguard IT resources.
- HOC must follow a risk-based approach to protect the confidentiality, integrity, and availability of assets as business needs and IT resources change.
- HOC must operate IT security activities effectively, responsibly, and ethically, complying with all local, state and federal laws, and regulations.
- With oversight from the Board of Commissioners and HOC's strategic plan, the Chief Technology Officer ("CTO") and Chief Compliance Officer ("CCO") must be responsible for the approval of and ensuring ongoing compliance with this policy.
- The CTO and CCO together are responsible for ensuring IT resources are secure from unauthorized access (to maintain appropriate confidentiality) and unauthorized alterations (to maintain integrity), and are available to authorized Users (to maintain availability), to enable HOC to meet its mission in an effective and timely manner.
- The CTO and CCO together are responsible for establishing and maintaining an information security program aligned to HOC's IT risk that includes developing, deploying, and maintaining

reasonable security policies, processes, practices, procedures, guidelines, and technologies to protect IT resources.

- The CTO and CCO together ensure that the information security program includes training to support this ISA Policy.
- The CTO and CCO are to be members of and coordinate with the Cybersecurity Incident Response Team ("CSIRT") in response to information security incidents, violations, or crimes arising from or relating to the use of IT resources.
- Users are responsible for safeguarding IT resources, which Users utilize, access, and interact with, even if Users do not have the responsibility of managing them.
- HOC Legal provides legal guidance to this ISA policy.

1.2 Scope

This ISA Policy document defines common security requirements for all HOC personnel and systems that create, maintain, store, access, process or transmit information. This ISA Policy also applies to information resources owned by others, such as contractors of HOC, entities in the private sector, in cases where HOC has a legal, contractual or fiduciary duty to protect said resources while in HOC custody. In the event of a conflict, the more restrictive measures apply. This ISA Policy covers the HOC network system, which comprises various hardware, software, communication equipment and other devices designed to assist HOC in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment at its office locations, remote locations, and other cloud and third party environments.

Third-Party IT Resources

HOC may contract with software application vendors or providers of other IT resources. Such third-party providers may have their own policies applicable to Users. This ISA Policy requires that you must comply with any such third-party policies if it is more restrictive than this policy.

1.3 Acronyms / Definitions

Common terms and acronyms that may be used throughout this document.

CCO	The Chief Compliance Officer is responsible for annual security training of all staff on confidentiality issues and administering HIPAA privacy compliance issues.
CSIRT	Cybersecurity Incident Response Team – a cross-divisional team of technical and business leaders organized by their role in the incident response process.
CST	Confidentiality and Security Team
CTO	The Chief Technology Officer
Cyber Security Breach	Any incident that results in unauthorized access to computer data, applications, networks, or devices.
Data Breach	A security violation (e.g., unintentional information disclosure, data leak, information leakage, data spill), in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Data Owners	Each department or unit that maintains HOC data, either in electronic or paper form, is required to designate a records management coordinator who will ensure that records in their area are preserved, maintained, and retained in compliance with records management policies and retention schedules established by the Compliance Division [or other designated authority].
ED	The Executive Director is responsible for the overall privacy and security practices of the organization.
Encryption	The process of transforming Information, using an algorithm, to make it unreadable to anyone other than those who have a specific "need to know".
External Media	i.e., CD-ROMs, DVDs, flash drives, USB keys, thumb drives.
Firewall	A dedicated piece of hardware of software running on a computer which allows or denies traffic passing through it, based on a set of rules.
HIPAA	Health Insurance Portability and Accountability Act
HOC	Housing Opportunities Commission of Montgomery County
IIHI	Individually Identifiable Health Information (IIHI), which includes information related to the past, present or future condition, treatment, payment or provision of health care to the identified individual.
IT	Information Technology
Legal Services	May consist of internal HOC Legal Counsel and/or outside Counsel.
PHI	Personal Health Information. Individually identifiable health information except for education records covered by FERPA and employment records.
PII	Personally Identifiable Information - any form that consists of a combination of an individual's name and one or more of the following: Social Security Number, driver's license or state ID, account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or other information which could be used to identify an individual.
Security Breach Group	Responds to initial privacy/security breach reports. Members include Chief Compliance Officer, Chief Technology Officer, Manager of Technical Operations, Help Desk Supervisor and General Counsel Contact: securitybreach@hocmc.org
User	Any staff, residents, volunteers, administrative officials, authorized guests, commissioners, delegates, and contractors who use, access, or otherwise employ, locally or remotely, HOC IT resources, whether individually controlled, shared, stand-alone, or networked.
Virus	A software program capable of reproducing itself and usually capable of causing great harm to files or programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

1.4 Management Responsibilities

Human Resources/Compliance must:

- Ensure that all personnel are aware of and comply with this ISA Policy;

- Create performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this ISA Policy; and
- Request all technology related services through the Information Technology Division.

HOC has established a Compliance Officer as required by federal law. This Privacy/Compliance Officer (P/CO) will oversee all ongoing activities related to the development, implementation, and maintenance of HOC privacy policies in accordance with applicable federal and state laws.

The current Privacy/Compliance Officer for HOC is: Darcel Cox, CCO

1.5 Confidentiality / Security Team (CST)

HOC has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within HOC, and act as the first line of defense in enhancing the appropriate security posture.

All members identified within this ISA Policy are assigned to their positions by the Executive Director. This team will consist of the positions within HOC most responsible for the overall security policy planning of the organization - the ED, P/CO, and CTO (where applicable). The members of the CST are:

1. Executive Director
2. Chief Compliance Officer
3. Chief Technology Officer
4. Manager of Technical Operations, IT Division

The CST will meet as needed to discuss security issues and to review concerns that arise. The CST will identify areas that should be addressed during annual training and review/update security policies as necessary.

The CST will address security issues as they arise, recommend, and approve immediate security actions to be undertaken. It is the responsibility of the CST to identify areas of concern within HOC and act as the first line of defense in enhancing the security posture of HOC.

The CST is responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during meetings as needed.

2. EMPLOYEE RESPONSIBILITIES

2.1 Employee Requirements

The first line of defense in data security is the individual User. A user is defined as any staff, residents, volunteers, administrative officials, authorized guests, commissioners, delegates, and contractors who use, access, or otherwise employ, locally or remotely, HOC IT resources, whether individually controlled, shared, stand-alone, or networked. HOC Users are responsible for the security of all data, which may come to them in whatever format. HOC is responsible for maintaining ongoing training programs to inform all Users of these requirements.

Wear Identifying Badge - In order to help maintain building security, all employees should prominently display their employee identification badge. Contractors who may be in HOC facilities are provided with different colored identification badges. Other people who may be within HOC facilities should be wearing visitor badges and should be chaperoned.

Challenge Unrecognized Personnel - It is the responsibility of all HOC personnel to take positive action to provide physical security. If an employee notices an unrecognized person in a restricted HOC office location, the employee should immediately report the unrecognized person to any security personnel on duty and/or Facilities. All visitors to HOC offices must sign in at the front desk. In addition, all visitors must wear a visitor/contractor badge. All other personnel must be employees of HOC. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Secure Laptop - When out of the office, all laptop computers must be secured. HOC computers will contain sensitive data; the utmost care should be taken to ensure that data is not compromised. Laptop computers are easy to steal, particularly during periods of mobility.

Unattended Computers - Unattended computers should be locked by the User when leaving the work area. This feature is discussed with all employees during yearly security training. HOC policy states that all computers will have automatic screen locking functionality set to activate upon fifteen (15) minutes of inactivity. Employees are not permitted to take any action, which would override this setting.

Home Use of HOC Corporate Assets - Only computer hardware and software owned by and installed by HOC is permitted to be connected to or installed on HOC equipment. Only software that has been approved for corporate use by HOC may be installed on HOC equipment. All employees and contractors must read and understand the list of prohibited activities that are outlined in the Information Technology & Acceptable Use of Information Technology Infrastructure and Resources Policy and herein.

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the HOC are the property of HOC unless covered by a contractual agreement. Nothing contained herein applies to software purchased by HOC employees at their own expense.

2.2 Prohibited Activities

Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document and within the Information Technology & Acceptable Use of Information Technology Infrastructure and Resources Policy.

- Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of User action, a repetition of the action by that User may be viewed as a deliberate act.
- Attempting to break (i.e., hack) into an IT resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs and attempting to circumvent file or other resource permissions.
- Introducing, or attempting to introduce, computer Viruses, malware, Trojan horses, peer-to-peer (i.e. P2P) or other malicious code into an information system.
    - Exception: Authorized information system support personnel, or others authorized by the CTO or HOC Privacy/Compliance Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
- The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. HOC has access to private information which is protected by a variety of federal, state and local laws including but not limited to HIPAA regulations which stipulate a "need to know" basis before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
- Use of personal software is prohibited. All software installed on HOC computers must be approved by HOC.
- Violating or attempting to violate the terms of use or license agreement of any software product used by HOC is strictly prohibited.
- Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of HOC is strictly prohibited.

Guidelines Statement

Personnel should follow the following guidelines:

- Approved anti-malware software must be installed on HOC-owned and managed devices.
- Users should report suspicious activity to the HOC Helpdesk.
- Do not allow downloads from unknown or untrusted sites.
- Be aware of browser warnings when a website asks for additional access to your computer.
- Be aware of spyware or adware on your computer. These types of software often have adverse effects on a computer, including, but not limited to: pop-ups or unsolicited tabs in a web browser, sluggish computer performance, or multiple unrequested browser windows.

2.3 Electronic Communications, Internet, and Web Usage

As a productivity enhancement tool, HOC encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by HOC owned

equipment are considered the property of HOC– not the property of individual Users. This applies to all HOC employees and contractors, and covers all electronic communications including, but not limited to, telephones, mobile phones, email, voice mail, instant messaging platforms, Internet, fax, computers, servers, Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

HOC-provided IT resources are intended for business purposes. However, incidental personal use is permissible as long as:

1. It does not consume more than a trivial amount of employee time or resources;
2. It does not interfere with staff productivity;
3. It does not preempt any business activity; and
4. It does not violate the acceptable use policy or any of the following:
    a. Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
    b. Illegal activities – Use of HOC information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
    c. Commercial use – Use of HOC information resources for personal or commercial profit is strictly prohibited.
    d. Political Activities – All political activities are strictly prohibited on HOC premises. HOC encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using HOC assets or resources.
    e. Harassment – HOC strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, HOC prohibits the use of computers, email, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse include, but are not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

Email is typically not considered a secure data transfer method, especially when sending it externally (i.e., not HOC domain). Secure information may be sent through email, provided an HOC approved email Encryption solution is used.

> Junk/SPAM Email - All communications using IT resources shall be purposeful and appropriate. Distributing “junk” mail, such as advertisements or unauthorized solicitations, is prohibited. Advertisement offers services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the email message immediately. Do not forward the email message to anyone.

Generally, while it is NOT the policy of the HOC to monitor the content of any electronic communication, HOC is responsible for servicing and protecting the HOC equipment, networks, data, and resource availability and therefore, may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals and are conducted at the discretion of designated HOC staff. HOC’s Information Technology & Acceptable Use of Information Technology Infrastructure and Resources Policy define the rights of the User.

HOC reserves the right, at its discretion, to review any employee's files or electronic communications to the extent necessary to ensure all electronic media, data, and services are used in compliance with all applicable laws and regulations as well as HOC policies.

Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

2.4 Social Media Participation

These guidelines apply to HOC employees or contractors who create or contribute to blogs, wikis, social networks, virtual worlds, or any other kind of social media. Whether a User logs into Twitter, Instagram, LinkedIn, Yelp, Wikipedia, or Facebook pages, or comment on online media stories — these guidelines apply.

While all HOC employees are welcome to participate in social media, we expect everyone who participates in online commentary to understand and to follow these simple but important guidelines. The overall goal is simple: to participate online in a respectful, relevant way that protects our reputation and follows the letter and spirit of the law.

1. Be transparent and state that you work at HOC. If you are writing about HOC or a competitor, use your real name, identify that you work for HOC, and be clear about your role.
2. Never represent yourself or HOC in a false or misleading way. All statements must be true and not misleading; all claims must be substantiated.
3. Post meaningful, respectful comments — in other words, please, no spam and no remarks that are off- topic or offensive.
4. Use common sense and common courtesy: for example, it is best to ask permission to publish or report on conversations that are meant to be private or internal to HOC. Make sure your efforts to be transparent do not violate HOC's privacy, confidentiality, and legal guidelines for external commercial speech.
5. Stick to your area of expertise and do feel free to provide unique, individual perspectives on non-confidential activities at HOC.
6. When disagreeing with others' opinions, keep it appropriate and polite. If you find yourself in a situation online that looks as if it's becoming antagonistic, do not get overly defensive and do not disengage from the conversation abruptly: feel free to ask the Director of Legislative and Public Affairs for advice and/or to disengage from the dialogue in a polite manner that reflects well on HOC.
7. If you want to write about the competition, make sure you behave diplomatically, have the facts straight and that you have the appropriate permissions.
8. Never comment on anything related to legal matters, litigation, or any parties with whom HOC may be in litigation.
9. Never participate in Social Media when the topic being discussed may be considered a crisis. Even anonymous comments may be traced back to your or HOC's IP address. Refer all Social Media activity around crisis topics to Legislative and Public Affairs and/or Legal.
10. Be smart about protecting yourself, your privacy, and HOC's confidential information. What you publish is widely accessible and will be around for a long time, so consider the

content carefully. Google has a long memory.

NOTE: Mainstream media inquiries must be referred to the Director of Legislative and Public Affairs.

2.5 Internet Access

Internet access is provided for HOC Users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. Internet access provided by HOC should be used in accordance with the Information Technology & Acceptable Use of Information Technology Infrastructure and Resources Policy.

Users must understand that individual Internet usage is monitored, and if an employee is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, and online music sharing applications, may be blocked by HOC's routers and Firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

2.6 Reporting Software Malfunctions and Potential Compromises

Users should inform the HOC Helpdesk when the User's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the User, or the User's manager or supervisor, suspects a computer Virus infection, HOC computer Virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer.
- Do not carry out any commands, including commands to Save data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel or IT as soon as possible.
- Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected Virus!

If the issue is found to have the potential of spreading, the IT response team must escalate the issue to the CSIRT and appropriate communications to all HOC staff should be sent to mitigate any additional risk and exposure.

2.7 Report Security Incidents

It is the responsibility of each HOC employee, contractor, volunteer, or intern to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person who has access to an information resource as referenced in *Section 2.1 Employee Requirements*. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security

incidents or violations of the security policy immediately to the CTO or CCO. Users should report any perceived security incident to either their immediate supervisor, or to their division director.

Reports of security incidents shall be escalated as quickly as possible. Each member of the CSIRT must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. It is the responsibility of the CSIRT to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, IT and the Chief Compliance Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to, the police or the FBI.

2.8 Transfer of Sensitive / Confidential Information

When confidential or sensitive information from one individual is received by another while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with HOC privacy policies as well as all applicable laws. All employees must recognize the sensitive nature of data maintained by HOC and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of HOC policy and will result in personnel action, and may result in legal action.

Personal software shall not be used on HOC computers or networks. If a need for specific software exists, Users must submit a request to their supervisor or division head. Users shall not use HOC purchased software on systems unless licensed to do so. Leveraging HOC supplied SaaS solutions from non-HOC equipment may be allowed so long as the appropriate security protocols are being followed.

HOC proprietary data, including but not limited to employee information, IT Systems information, financial information or human resource data, shall not be placed on any system (computer or service) that is not the property (or licensed) of HOC without written consent of the respective supervisor or division director. SaaS solutions such as G-Suite and AODOCS are supplied to enable data access with mobility while maintaining security. It is crucial to HOC to protect all data and, in order to do that effectively, we must control the systems in which it is contained. In the event that a supervisor or division director receives a request to transfer HOC data to a non- HOC computer system or service, the supervisor or division director should notify the CTO and CCO or appropriate personnel of the intentions and the need for such a transfer of data.

2.9 Handling Sensitive Information

“Sensitive Information” is information that must be protected from unauthorized access or disclosure because of laws, regulations, HOC policy, or by agreement, whether the information is in physical or electronic format.

Members of the HOC community, who access information, in physical or electronic format, obtained by or from HOC staff, vendors, customers, volunteers, contractors, or visitors using HOC facilities, services or IT systems, are responsible for properly using and, when appropriate, protecting and safeguarding the privacy of Sensitive Information that has been collected, produced or maintained by HOC in connection with its mission and/or operation as a public entity.

Members of the HOC Community must know the difference between Public Information and Sensitive Information and how to classify and protect Sensitive Information.

Every member of the HOC community is obligated to protect Sensitive Information from unauthorized access or disclosure and should be aware of the four (4) Data Classification levels used to identify and secure Sensitive Information per the Data Classification Guidelines. The goal is to assure that every member of our community can readily define Sensitive Information, such as Social Security numbers (SSN), or financial numbers in conjunction with a person's name, so they can appropriately classify the information, follow appropriate security precautions to protect the information, and not jeopardize the privacy rights of others or HOC's institutional rights or obligations.

Assigning the appropriate level of protection to Sensitive Information is called Data Classification. Much of the information under HOC's control is classified as public information, in physical and/or electronic format, and can be shared without constraint. However, some information is classified as non-public because it is personally identifiable information ("PII"), HOC proprietary information, sensitive research data, or information that is controlled by laws or regulations. Whether in physical and/or electronic format, Data Owners and Custodians must identify and appropriately classify Sensitive Information so it is protected appropriately.

2.10 Transferring Software and Files between Systems

Special precautions are required to block Internet (public) access to HOC information resources not intended for public access, and to protect confidential HOC information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage.

Prior approval of the CTO, CCO, or appropriate personnel authorized by HOC shall be obtained before:

- An Internet, or other external network connection, is established.
- HOC information (including notices, memoranda, documentation and files, software, and other forms of content) is made available on any Internet-accessible computer (e.g. web, SaaS, PaaS, and IaaS) or device.
- Users may not install or download any software (applications). If Users have a need for additional software, the User is to contact their supervisor.
- Use shall be consistent with the goals of HOC. The network can be used to market services related to HOC, however use of the network for personal profit or gain is prohibited.
- Confidential or sensitive data - including all Personal Identifiable Information (PII), credit card numbers, social security numbers, passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.

3. IDENTIFICATION AND AUTHENTICATION

3.1 User IDs

Individual Users shall have a unique login ID and password. An access control system shall identify each User and prevent unauthorized Users from entering or using information resources. Security requirements for User identification include:

- Each User shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.

All User login IDs are audited at least twice yearly. HOC must be notified upon the departure of all employees and contractors, at which time login IDs are revoked.

The logon ID is locked or revoked after a maximum of three (3) unsuccessful login attempts, which then require the passwords to be reset by the appropriate Administrator.

Users who desire to obtain access to HOC systems or network resources must be authorized to do so by their supervisor and IT.

3.2 Passwords

User Account Passwords

User IDs and passwords are required in order to gain access to all HOC computers, network services and technology resources. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to compromise. Users are required to select a password in order to obtain access to any electronic information at the system, network and computer level. When passwords are reset, the User will be automatically prompted to manually change that assigned password.

3.3 Multi-Factor Authentication

Users must utilize Multi-Factor Authentication (MFA) to access all IT resources (e.g., Yardi, portal, Housing Path, email, Google Drive™, Zoom®).

Users must not share individual account access methods (e.g., DUO passcodes, passwords) with others. Users may authenticate via push notifications to smartphones and tablets, mobile passcode, SMS passcode, telephone callbacks, or hardware tokens. Should these methods not be available to the User, they should contact the HOC Helpdesk for support.

The CTO and/or CCO must approve access to IT resources that cannot support MFA.

3.4 Confidentiality and Secure Handling

Users of IT resources shall sign, as a condition for employment, an appropriate confidentiality agreement. The agreement shall include the following statement, or a paraphrase of it:

"I understand that any unauthorized use or disclosure of information residing on HOC information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies."

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing HOC information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

HOC protected data, HOC sensitive data, or public data must be stored or transmitted per the Data Classification Guidelines.

Protection measures must be taken and maintained to prevent unauthorized or unlawful disclosure of HOC data. Protection measures are based on data classification and include, but are not limited to, the following:

3.5 Access Control

Forms of access control include:

- Physical access control (e.g., controlled access to buildings, rooms, data centers, appropriate handling, storage, and disposal of media).
- Administrative access control (e.g., restrict access based on role or authority).
- Technical access control (e.g., information stored on a secure server and use of privacy configurations, appropriate handling, storage, and disposal of media).

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e., directory data, passwords, Encryption, access control lists, constrained User interfaces, etc.) and external (i.e., intrusion detection and preventions systems, Firewalls, antivirus and malicious content prevention, authentication systems, etc.).

Rules for access to resources (including internal and external telecommunications and networks), have been established by the information/application owner or manager with responsibility for the resources. Access is granted only by the approval of a division supervisor, system owner and CTO. This guideline satisfies the "need to know" requirement of federal regulations, since the supervisor or division director is the person who most closely recognizes an employee's need to access data.

System Based Identification and Authentication Requirements: The systems maintaining sensitive data shall maintain logs, including current User activity authorizations and data access.

3.6 User Login Entitlement Reviews

If an employee changes positions at HOC, the employee's new supervisor or division director shall promptly notify the Information Technology Division of the change in roles, by indicating through the employee onboarding system, both the roles or access to be added and the roles or access to be removed. This ensures that the employee has access to the minimum necessary data to effectively perform their new job functions. The effective date of the position change should also be noted during the employee

onboarding process so that the IT Division can ensure that the employee will have appropriate roles, access, and applications for their new job responsibilities. For a limited training period, it may be necessary for the employee who is changing positions to maintain their previous access as well as adding the roles and access necessary for their new job responsibilities.

3.7 Termination of User Login Account

Upon termination of an employee, whether voluntary or involuntary, the employee's supervisor or division head shall promptly notify the IT Division by indicating “Remove Access” through the employee off boarding process. If the employee’s termination is voluntary and the employee provides notice, the employee's supervisor or division director shall promptly notify the IT Division of the employee's last scheduled work day so that their User account(s) can be configured to expire. The employee’s division director shall be responsible for ensuring that all keys, ID badges, and other access devices as well as HOC equipment and property is returned to HOC prior to the employee leaving HOC on their final day of employment.

No less than quarterly, the IT Manager(s) or their designee(s) shall provide a list of active User accounts for both network and application access to Human Resources for review. Human Resources shall review the employee access lists within five (5) business days of receipt. If any of the employees on the list are no longer employed by HOC, Human Resources will immediately notify the IT Division of the employee’s termination status and submit the updated off boarding information.

4. NETWORK RESOURCE CONNECTIVITY

4.1 Firewalls

Authorization from the CTO or appropriate personnel must be received before any employee or contractor is granted access to an HOC router or Firewall.

The following requirements must be met:

- Users who have the ability to grant access to restricted network devices including but not limited to routers, switches, and Firewalls must abide by the rules in this ISA Policy.
- All IT resources that allow access to data, systems, and networks must contain a default "deny all" inbound access rule.
- All sensitive IT resources on networks and systems must be secured from direct public access.

4.2 Wireless

User authentication is required before accessing the HOC wireless networks.

HOC monitors the wireless network for interfering devices to ensure reliable access.

HOC reserves the right to restrict/remove device access to the wireless network to prevent Users from infecting, degrading, or otherwise negatively affecting IT resources.

Users must not install a personal wireless access point or any device that interferes with wireless IT resources. Should any such device be detected, HOC notifies the User, the User is then required to disable and remove the device from the network. If the User does not promptly disable the device, HOC reserves the right to disconnect the device from the network.

5. ANTIVIRUS/ANTI-MALWARE/SOFTWARE

5.1 Antivirus

Antivirus software is installed on all HOC computers and servers. Virus definitions update patterns are updated daily on HOC servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff who are responsible for keeping all Virus patterns up to date.

All HOC IT resources must maintain up-to-date antivirus software.

HOC provides antivirus software and maintains it on all HOC-owned IT resources.

Updates and Virus patches may be pushed out to individual devices through automated procedures on an as needed basis, which is known as Remote Deployment Configuration.

Uninstalling or disabling the antivirus product for any reason is prohibited.

Individuals who use non-HOC devices and choose to use other solutions should refer to the documentation provided with the software.

Users are responsible for updating the software to the most current version when prompted by their systems; IT will configure to update Virus definitions daily automatically.

5.2 Anti-Malware

All capable HOC-owned and managed devices must have installed approved anti-malware software.

Users should report suspicious activity to the HOC Helpdesk.

Users shall not allow downloads from unknown or untrusted sites.

Users should be aware of browser warnings when a website asks for additional access to your computer.

Users should be aware of spyware or adware on their computer. These types of software often have adverse effects on a computer, including, but not limited to: pop-ups or unsolicited tabs in a web browser, sluggish computer performance, or multiple unrequested browser windows.

5.3 Retention of Ownership: Software

All software programs and documentation generated or provided by employees, consultants or contractors for the benefit of HOC are the property of HOC unless covered by a contractual agreement. Nothing contained herein applies to software purchased by HOC employees at their own expense.

6. ENCRYPTION

Encryption involves the process of transforming data so that it is unreadable by anyone who does not have a decryption key. Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is called cipher text.

Full disk Encryption ("FDE"), also known as whole disk Encryption, is the process of encrypting all the data on the hard drive(s) on a computer, including the computer's operating system, and permitting access to the data only after successful authentication.

- The Encryption software used and the specific Encryption methods shall be chosen and maintained by designated IT personnel only. Staff are not to encrypt HOC data or personal data stored with an HOC system without the clear direction and approval of the HOC IT Division.
- Laptops, desktops, and servers are required to employ full disk Encryption regardless of their intended use or the data stored on them.
- Users are required to employ Encryption for all HOC Sensitive and Protected data regardless of the medium (e.g., USB, external hard drive, cloud storage).
- Users must not attempt to disable, remove, or otherwise tamper with the Encryption software.

7. BUILDING AND PHYSICAL ACCESS

It is the policy of HOC to provide building access in a secure manner. Each site is unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and room control. However, HOC strives to continuously upgrade and expand its security and to enhance protection of its assets and sensitive information that has been entrusted to it.

The following list identifies measures that are in effect at HOC. All other facilities, as applicable, have similar security appropriate for that location.

- Description of building, location, square footage, and the use of any generator.
- Entrance to the building during non-working hours is controlled by a security code system. Attempted entrance without this code results in immediate notification to the police department.
- Only specific HOC employees are given the security code or badge access rights for entrance. Disclosure of the security code to non-employees is strictly prohibited.
- The security code is changed on a periodic basis and eligible employees are notified by company email or voice mail. Security codes are changed upon termination of employees that had access.
- The reception area is staffed at all times during the working hours of 8:00 AM to 5:00 PM.
- Any unrecognized person in a restricted office location should be reported to any security personnel on duty and/or Facilities. All visitors must sign in at the front desk, wear a visitor badge, and be accompanied by an HOC staff member. In some situations, non-HOC personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times.
- Swipe cards control access to all other doors. Each card is coded to allow admission to specific areas based on each individual's job function or need to know.
- The first floor of the building has motion detection sensors that are activated after hours. Any movement within the building will result in immediate notification to the police department. All outside windows have glass breakage sensors, which if tripped, will result in immediate notification to the police department.
- The building is equipped with security cameras to record activities in the parking lot and within the area encompassing the front entrance. All activities in these areas are recorded on a 24-hour a day, 365 days per year basis.
- Fire Protection: Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

8. TELEWORK

All Users who participate in the HOC Telework program shall adhere to and act in accordance with guidelines set forth within the HOC Telework Policy.

9. MOBILE DEVICE MANAGEMENT

9.1 HOC-Owned Mobile Devices

Mobile devices issued to employees of HOC are to be used for business purposes only and remain the property of HOC.

All requests for mobile devices must be made using a service request and approved by the supervisor and division director.

HOC-owned mobile devices must be returned to the approving HOC division director, upon leaving the department, or when the device is no longer needed to conduct HOC business.

9.2 Bring Your Own Devices (BYOD)

When accessing HOC IT resources with a personal mobile device, the User must follow the data classification policies per the Data Classification Guidelines and is subject to the rules governing data.

HOC does not accept liability for the maintenance, backup, or loss of data stored on Users' personal mobile devices.

Users are responsible for backing up all software and data to appropriate backup storage systems.

HOC is not liable for the loss, theft, or damage of any User's personal mobile devices, including, but not limited to when the device is being used for HOC business or during business travel.

The User's personal mobile device may be subject to disclosure in the event of litigation, and the User will be required to cooperate with HOC in providing access to the device for that purpose.

9.3 Terms and Conditions

Users of mobile devices that access IT resources, which include non-HOC owned devices, must comply with the following security and risk management measures:

1. If your device is lost, stolen, or compromised, you must report it immediately to the IT Helpdesk.
2. HOC IT provides security and risk management software for accessing IT resources.
3. HOC does not accept liability for any damages due to the installation of the software mentioned above on non-HOC-owned devices.
4. All devices must be secured using a PIN (4-digit minimum) or other password protection.
5. All devices must enable automatic lockout for idle devices for (5) five or fewer minutes, where possible.
6. All devices must have remote wipe capability installed and enabled, where possible.
7. Users of mobile devices that access IT resources will be subject to remote locking or data wiping of lost, stolen, or otherwise compromised devices. To implement these security requirements, Users may contact the HOC Helpdesk.

User Code of Conduct

Users of mobile devices that access IT resources, which include non-HOC owned devices, are expected to take reasonable measures to protect the security and integrity of that data, including:

- Following the rules outlined in Section 4.2, "Wireless" of this ISA Policy;
- Protecting the physical security of the device;
- Maintaining the software configuration of the device (i.e., operating system or installed applications);
- Installing an up-to-date and secure operating system and application software as they become available;
- Following rules of HOC Protected or HOC Sensitive data per the Data Classification Guidelines; and
- Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes, or security setting changes and working with the IT Helpdesk to test and validate any configuration, application, or settings.

10. DISPOSAL OF HARDWARE

10.1 External Media

It must be assumed that External Media possesses sensitive data that should be protected and disposed of accordingly. External Media should be disposed of in a method that ensures that there will be no data leakage and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

- It is the responsibility of each employee to identify media, which should be shredded and to utilize this ISA Policy in its destruction.
- External Media should never be placed in the trash.
- When no longer needed, all forms of External Media are to be sent to the appropriate personnel for proper disposal.
- The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.

10.2 Requirements Regarding Equipment

All equipment to be disposed of will be wiped of all data or destroyed, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

10.3 Disposition of Excess Equipment

As older HOC computers and equipment are replaced with new systems, older machines are held in inventory for a variety of uses:

- Older machines may be utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.

11. CHANGE MANAGEMENT

Statement of Policy

To ensure that HOC is tracking changes to network resources, systems, and devices including software releases and software vulnerability patching in information systems that contain protected data. Change tracking allows the IT Division to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system. Change tracking also allows for efficient communications to the business regarding notifications that may impact critical processes.

Procedure

1. The IT staff or other designated HOC employee who is updating, implementing, reconfiguring or otherwise changing any production infrastructure system (i.e., servers, network equipment or cloud infrastructure) will present a change plan and justification for the change to the CTO for approval.
    a. Changes to systems that may have an impact on the business must be communicated to the business prior to the change or immediately after if addressing an emergency.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change also shall be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

12. DATA INTEGRITY

Statement of Policy

HOC shall implement and maintain appropriate electronic mechanisms to corroborate that sensitive data has not been altered or destroyed in an unauthorized manner.

The purpose of this policy is to protect HOC data from improper alteration or destruction.

Procedure

To the fullest extent possible, HOC shall utilize automation, applications, integrations, and workflows with built-in intelligence that automatically checks for human errors.

HOC shall maintain intrusion detection systems. The Chief Technology Officer or delegate shall be responsible for installing, maintaining, and updating such systems.

To prevent transmission errors as data passes from one computer to another, HOC will use Encryption, as determined to be appropriate, to preserve the integrity of data.

HOC will check for possible duplication of data in its database repositories and systems to prevent poor data integration between different systems.

To prevent programming or software bugs, HOC will test its information systems for accuracy and functionality before it starts to use them. HOC will update its systems when IT vendors release fixes to address known bugs or problems.

HOC will install and regularly update antivirus software on monitoring all systems to detect and prevent malicious code from altering or destroying data.

13. SECURITY AND AWARENESS TRAINING

Statement of Policy

To establish a security awareness and training program for all members of HOC.

All workforce members shall receive appropriate training concerning HOC security policies and procedures. Such training shall be provided on an ongoing basis to all new and current employees.

1. Security Training Program
    a. The Chief Technology Officer and Chief Compliance Officer shall have joint responsibility for the development and delivery of the security training. All workforce members shall receive such training throughout the year. Training will be monitored and attendance and/or participation in such training will be mandatory for all.
    b. The CTO shall be responsible for maintaining appropriate documentation of all training activities and supporting the selection of training materials. This includes responsibility for the development and delivery of ongoing security training in response to environmental and operational changes affecting the security of data, e.g., threat landscape changes, new software, and new protocols.

2. Security Reminders
    a. The CTO shall generate and distribute routine security reminders to all workforce members on a regular basis. Periodic reminders may address credentials, malicious software, incident identification and response, and access control. The CTO may provide such reminders through formal training, e-mail messages, and discussions during staff meetings, newsletter/intranet articles, posters, promotional items such as coffee mugs, mouse pads, sticky notes, etc. The CTO shall be responsible for maintaining appropriate documentation of all periodic security reminders.
    b. The CTO shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

3. Protection from Malicious attacks and software
    a. As part of the aforementioned Security Training Program and Security Reminders, the CTO shall provide training concerning the prevention, detection, containment, and eradication of malicious software.
    b. In addition, the CTO will ensure the workforce is educated on ransomware threats, attacks, and responses. Every staff member may play a critical role in defending and mitigating such risks; therefore, each must be part of the solution.

14. SECURITY MANAGEMENT PROCESS

Purpose

To ensure HOC conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of IT resources held by HOC.

Annually, HOC shall conduct an accurate and thorough risk analysis. HOC shall re-assess the security risks to its business and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business practices and technological advancements.

The CTO (or designee) is authorized to perform periodic information security risk assessments to determine areas of vulnerability and to initiate appropriate remediation.

Risk assessments must identify, quantify, and prioritize risk acceptance and objectives relevant to HOC. The results are to guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls to protect against these risks.

Risk assessments are performed periodically to address changes in security requirements and the risk situation (e.g., threats, vulnerabilities, impacts, risk evaluation, and data classification).

Risk assessments are to be undertaken systematically, capable of producing comparable and reproducible results. The information security risk assessment should have a clearly defined scope to be effective and should include relationships with risk assessments in other areas, if appropriate.

All patches or configuration changes must be deployed to HOC-owned or managed IT resources in a timely manner.

All IT resources must be part of a patch management cycle.

Application and system owners are responsible for the assessment and remediation of IT resources under their management or supervision.

If a solution or remediation is not available to address a vulnerability, the CSIRT must approve any compensating or other mitigating controls.

Application and system owners must have a written and auditable procedure addressing remediation steps.

The CTO or their delegate shall evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.

The CTO shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The IT Division shall identify appropriate persons within the organization to assist with such evaluations. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the HIPAA Security Regulations; new federal, state, or local laws or regulations affecting the security of PHI; changes in technology, environmental processes, or business

processes that may affect HIPAA Security policies or procedures; or the occurrence of a serious security incident. Follow-up evaluations shall include the following:

- Inspections, reviews, interviews, and analysis to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews and tabletop exercises to assess employee compliance; review of latest security policies and procedures for correctness and completeness; and inspection and analysis of training, incident, and logs for compliance.
- Analysis to assess adequacy of controls within the network, operating systems and applications. As appropriate, HOC IT shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement.

15. EMPLOYEE BACKGROUND CHECKS

HOC will conduct employment reference checks, investigative consumer reports, and background investigations on all candidates for employment prior to making a final offer of employment and may use a third party to conduct these background checks. HOC will obtain written consent from applicants and employees prior to ordering reports from third-party providers and will provide a description of applicant and employee rights and all other documentation as required by law to each applicant or candidate in accordance with FCRA and applicable state and federal statutes. All background checks are subject to these notice and consent requirements.

An investigative consumer report compiles information on a candidate's general reputation, personal characteristics, or mode of living. This information may be gathered online including social networking sites, through public or educational records, or through interviews with employers, friends, neighbors, associates, or anyone else who may have information about the employee or potential employee. In the pre-employment process, investigative consumer reports typically include such things as criminal records checks, education verification checks, and employment verification checks.

The type of information that will be collected by HOC in background checks may include, but is not limited to, some or all of the following:

- Private and government agency reports related to any history of criminal, dishonest, or violent behavior, and other reports that relate to suitability for employment.
- Education (including degrees awarded and GPA).
- Employment history, abilities, and reasons for termination of employment.
- Professional licensing board reports.
- Address history.
- Credit reports.
- Social security number scans.
- Civil court filings.
- Motor vehicle and driving records.
- Professional or personal references.

This information may also be sought out at other times during employment, such as during reassignment or promotional periods, and following safety infractions or other incidents.

HOC will conduct background checks in compliance with the federal Fair Credit Reporting Act (FCRA), the Americans with Disabilities Act (ADA), and all other applicable local, state, and federal laws and regulations. Applicants and employees may request and receive a copy of requested "investigative consumer reports."

A reported criminal offense conviction will not necessarily disqualify a candidate from employment. The nature and seriousness of the offense, the date of the offense, the surrounding circumstances, rehabilitation, the relevance of the offense to the specific position(s), and whether hiring, transferring or promoting the applicant would pose an unreasonable risk to the business may be considered before a final decision is reached. HOC will follow FCRA requirements, other applicable statutes, and HOC procedures for providing information and reports, making decisions, and responding to applicants and employees regarding potentially adverse actions to an investigative report.

HOC reserves the right to withdraw any offer of employment or consideration for employment, or discharge an employee, upon finding falsification, misrepresentation, or omission of fact on an employment application, resume, or other attachments, as well as in verbal statements, regardless of when it is discovered.

Background check reports shall be maintained in separate, confidential files and retained in accordance with the HOC's document retention procedures.

16. DISCOVERY POLICY: PRODUCTION AND DISCLOSURE

Statement of Policy

It is the policy of this organization to produce and disclose relevant information and records in compliance with applicable laws, court procedures, and agreements made during the litigation process.

Purpose

The purpose of this policy is to outline the steps in the production and disclosure process for health information and records related to e-discovery for pending litigation.

Scope

This policy addresses e-discovery production and disclosure procedures related to the Federal Rules of Civil Procedures.

Procedure

Accurate Employee Identification

Responsible	Action
HOC	For litigation involving an individual's Computer Work, phone verify the employee's identity, including demographic information and identifiers, including the employee number. *[Note: When conducting searches, it is critical to identify the correct employee and relevant information.]*

Subpoena Receipt and Response

Responsible	Action
Legal Services	Upon receipt, subpoenas should be reviewed to determine that all elements are contained, the parties and the purpose are clearly identified, and the scope of information requested is clear. ● Validate the served subpoenas before official acceptance. The validation process includes at a minimum: ○ Verification of appropriate service of the subpoena and that the organization is under legal obligation to comply with it, and ○ Verification that the seal and clerk of the court signature are present and valid. Review of the venue and jurisdiction of the court for the case.
HOC	Notify Legal Services that a subpoena has been received and determine if a legal hold is in place. If not, Legal Services should determine whether a legal hold should be applied.
HOC	If the subpoena requests "any and all records," HOC and/or Legal Services should work with the judge and/or plaintiff's attorney to clarify the scope and type of information being requested. *[Note: The e-discovery process will identify vast volumes of data, which can overwhelm a case; the parties should identify information that is necessary and relevant rather than providing all information.]*

Responsible	Action
Legal Services	Provide direction to HOC in the processing of the subpoena, including the specific information to produce, agreed upon file formats and forms of production, whether an objection will be filed, timeframe to produce and disclose, and whether on-site testing/sampling will be conducted by the requesting party.
Legal Services	If an outside firm is retained, such as outside counsel or discovery/litigation consultants, perform an analysis to determine if the contracted firm will have access to PHI and will need to sign a contract with HOC.

Search and Retrieve Process

Responsible	Action
Legal Services	Identify the potential sources of information which may hold potentially relevant information, such as: ● Local area servers for the office ● Personal shares or personal folders on servers ● Dedicated servers for the organization ● Laptop and/or department computers ● Home computers, PDAs, smartphones ● Email, including archived email and sent email ● Email trash bin, desktop recycle bin ● Text/instant message archives ● Removable storage media (e.g., CDs, DVDs, memory sticks and thumb drives) ● Department/office files such as financial records ● Personal desk files ● Files of administrative personnel in department/office ● Files located in department/office staff home ● Web site archives
HOC, Data Owners	Based on direction from Legal Services on the potential locations of relevant information and the information agreed upon in the discovery plan and/or subpoena, establish search parameters (employee identifiers, search terms, key words, etc.) and conduct the search process. Maintain a record of the systems searched, search methodology, search parameters (terms), and search results.
IT	Assist HOC and Data Owners in the search and retrieval process for various systems and data sources.
HOC, Data Owners	Screen or filter the search results, eliminating inappropriate information (e.g., wrong employee, outside the timeframe, not relevant to the proceeding, etc.).
Legal Services	Review the content of the data/data sets found to determine relevance to the proceeding and identify information that is considered privileged.
Legal Services, HOC, Data Owners	Determine the final list of relevant data/data sets, location, and search methodology.

Production of Records/Data

Responsible	Action
HOC, Data Owners, IT	Determine the format the information will be disclosed, such as: paper, ASCII, PDF, TIF, screen shot, mirror copy of data file, or review of material on-line. The format will vary depending on data, source, and agreement made in the Discovery Plan/Form 35.

HOC, Data Owners, IT	Produce the information in the agreed-upon format as outlined in the discovery plan/Form 35.
Legal Services, HOC, Data Owners, IT	Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different employee) as appropriate.
Legal Services	Conduct final review of information before disclosing to requesting party
Legal Services	Retain a duplicate of information disclosed to the requesting party.

Charges for Copying and Disclosure

Responsible	Action
HOC, Data Owners, IT	For the information searched and disclosed, calculate the costs for search, retrieval, and disclosure methods using the organization's established formula and governmental formulas for reproduction charges.
HOC	Invoice requesting parties for allowable charges related to the reproduction of employee information and records
Legal Services	Determine whether other expenses may be charged in accordance with the discovery plan or negotiation with litigants and/or judge.

Testing and Sampling

Responsible	Action
Legal Services	A party to the legal proceeding may request to test and sample the search and retrieve methodology. Testing and sampling should be discussed and agreed upon during the pretrial conference and part of the discovery plan, including whether an external party will test and sample the search and retrieve methodologies. The costs and charges should also be determined and negotiated.
HOC, Data Owners	Retain information on all searches; including methodology, key words, and systems used in case the methodology has to be recreated for testing purposes and to determine if the sample was statistically valid.
Legal Services, HOC	Assign a monitor for the outside party during their testing protocols.

Responding to Interrogatories, Deposition, Court Procedures

Responsibility	Action
Legal Services	Legal Services manages the completion of the interrogatories, the taking of depositions, and giving of testimonies in court.
HOC (official record custodian)	HOC may provide information for an interrogatory, be deposed, or testify in court. HOC is the official custodian of the record and can testify whether the records were kept in the normal course of business and the authenticity of the records. In addition, HOC also addresses the good faith operations related to records management, retention/destruction, and the search and retrieval process/parameters.
IT (official system custodian)	IT may provide information for an interrogatory, be deposed, or testify in court. IT is the official custodian of the information system and may testify about the technical infrastructure, system architecture, security practices, source applications, and the good faith operations from a technical infrastructure perspective.

Data Owners	Data owners may provide information for an interrogatory, be deposed, or testify in court. The Data Owners may testify about the specific issues related to their department/business process area.
Primary/Direct Custodian	Primary/direct custodians may provide information for an interrogatory, be deposed, or testify in court. The primary/direct custodians are those person(s) who work with the data directly or have direct involvement/knowledge of the events of the litigation.
Business Associates/Third Parties	Business Associates/Third Parties may provide information for an interrogatory, be deposed, or testify in court. These include contractors and others who serve a variety of functions associated with a party's information but who themselves are not parties to the litigation. Examples include Internet service providers, application service providers such as a claims clearinghouse, and other providers who provide services ranging from off-site data storage to complete outsourcing of the IT Division.

17. e-DISCOVERY POLICY: RETENTION

Statement of Policy

It is the policy of HOC to maintain and retain enterprise health information and records in compliance with applicable governmental and regulatory requirements. HOC will adhere to retention schedules and destruction procedures in compliance with regulatory, business, and legal requirements, and act in accordance with guidelines set forth within the HOC Compliance Oversight Process for Document Retention. The processes outlined within this policy serve to complement, not to supersede, the guidelines within the HOC Compliance Oversight Process for Document Retention.

Purpose

The purpose of this policy is to achieve a complete and accurate accounting of all relevant records within the organization; to establish the conditions and time periods for which paper based and electronic health information and records will be stored, retained, and destroyed after they are no longer active for employee or business purposes; and to ensure appropriate availability of inactive records.

Scope

This policy applies to all enterprise information and records whether the information is paper based or electronic.

Definitions

Data Owners - Each department or unit that maintains HOC data, either in electronic or paper form, is required to ensure that records in their area are preserved, maintained, and retained in compliance with records management policies and retention schedules established by the Compliance Division [or other designated authority].

Property Rights - All enterprise information and records generated and received are the property of the organization. No employee, by virtue of their position, has any personal or property right to such data even though they may have developed or compiled them.

Workforce Responsibility - All employees and agents are responsible for ensuring that enterprise data and records are created, used, maintained, preserved, and destroyed in accordance with this ISA Policy.

Destruction of Enterprise Information and Records - At the end of the designated retention period for each type of data source, it will be destroyed in accordance with the procedures in this ISA Policy, unless a legal hold/preservation order exists or is anticipated.

Unauthorized Destruction - The unauthorized destruction, removal, alteration, or use of employee information and records is prohibited. Persons who destroy, remove, alter or use health information and records in an unauthorized manner will be disciplined in accordance with the HOC Personnel Policy and the Collective Bargaining Agreement.

Procedure

Responsibility	Action
HOC	HOC will be responsible for the following: ● Review, maintain, publish, and distribute retention schedules and records management policies and procedures. ● Develop control forms relating to business records. ● Audit compliance with records management (both electronic and paper) policies and retention schedules and report findings as needed. ● Provide training for records management. Training will be provided to any individual or department that needs assistance. ● Oversee operation of designated offsite record storage center(s) for archival storage of paper health information and records or serve as contract administrator for such services. ● Contract for destruction of paper and electronic records and certification thereof.
IT/HOC/Data Owners	IT/HOC/Data Owners will ensure that electronic storage of enterprise health information and records is carried out in conjunction with archiving and retention policies.
HOC	Departments are responsible for implementing and maintaining records management programs for their designated areas. They will organize and manage online records management control forms relating to enterprise records and information in their areas of responsibility to accomplish the following: ● Transfer records to storage ● Identify, control, and maintain records in storage ● Retrieve and/or return records from/to storage ● Document the destruction of records and the deletion of records from the records inventory ● Monitor the records management process
Legal Services	Legal Services serves as subject matter expert and provides counsel regarding records designations and legal and statutory requirements for records retention and pending legal matters. It ensures that access to or ownership of records is appropriately protected in all divestitures of property or lines of business or facility closures.

Guidelines for Retention of Records/Information and Schedules

Record Retention	Unless otherwise stipulated, retention schedules apply to all records. Records will only be discarded when the maximum specified retention period has expired, the record is approved for destruction by the record owner, and a Certificate of Destruction is executed.
Non-record Retention	Non-records are maintained for as long as administratively needed, and retention schedules do not apply. Non-records may and should be discarded when the business use has terminated. For example, when the non-record information, such as an employee's personal notes, is transferred to a record, such as an incident report, the notes are no

	longer useful and should be discarded. Preliminary working papers and superseded drafts should be discarded, particularly after subsequent versions are finalized. Instances where an author or recipient of a document is unsure whether a document is a record as covered or described in this policy should be referred to the Compliance Officer for determination of its status and retention period.
Email Communication Retention	Depending on content, email may be considered records and are subject to this policy. If an email message would be considered a record based on its content, the retention period for that email message would be the same for similar content in any other format. The IT Division maintains an archive that ingests and securely retains all email separately from the email system.
Development of Records Retention Schedules	Retention Schedule Determined by Law: All records will be maintained and retained in accordance with Federal and state laws and regulations. Electronic records must follow the same retention schedule as physical records, acknowledging the format and consolidated nature of records within an application or database. Retention of Related Computer Programs: Retention of records implies the inherent ability to retrieve and view a record within a reasonable time. Retained electronic data must have retained with it the programs required to view the data. Where it is not economically feasible to pay for maintenance costs on retired or obsolete hardware or software only for the purpose of reading archived or retained data, then data may be converted to a more supportable format, as long as it can be demonstrated that the integrity of the information is not degraded by the conversion. Data Owners should work closely with IT personnel in order to comply with this section. Retention of Records in Large Applications: Retention of data for large-scale applications, typically those that reside in the data center and are accessed by a larger audience, shall be the responsibility of the IT Division. Retention of Records on Individual Workstations: Primary responsibility for retention of data created at the desktop level—typically with email, Microsoft Office applications such as Word, Excel, PowerPoint, Access, or other specialized but locally run and saved computer applications—shall be with the User/author. The User/author will ensure that the documents are properly named and saved to be recognizable by the User in the future, and physically saved to a “shared drive.” By saving a copy in this manner, IT will create an archive version of the saved document for a specified number of years after the User deletes the copy from the shared drive. Records with retention periods in excess of this period will require an alternative means of retention. Users are responsible for the security of any confidential information and/or protected health information created or maintained on their workstations.

Storage and Destruction Guidelines

Records Destruction	General Rule: Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the Records Retention Schedules. Permanent Records: Records that cannot be destroyed include records of matters in litigation or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the record may be destroyed in accordance with the Records Retention Schedules, but in no case shall records used in evidence to litigation be destroyed earlier than a specified number of years from the date of the settlement of litigation. Destruction of Records Containing Confidential Information: Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information unrecognizable. Approved methods shall be employed to destroy records in accordance with local, state and federal rules; these methods may include but are not limited to recycling, shredding, burning, pulping, pulverizing and magnetizing. Destruction of Non-Records Containing Confidential Information: Destruction of Non-Records containing personal health information or other forms of confidential corporate, employee, member, information of any kind shall be rendered unrecognizable for both source and content by means of shredding, pulping, etc., regardless of media. This material shall be deposited in on-site, locked shred collection bins or boxed, sealed, and marked for destruction. Disposal of Electronic Storage Media: Electronic storage media must be assumed to contain confidential or other sensitive information and must not leave the possession of the organization until confirmation that the media is unreadable or until the media is physically destroyed. Disposal of Electronic Media: Electronic storage media, such as CD-ROMS, DVDs, tapes, tape reels or USB thumb drives containing confidential or sensitive information may only be disposed of by approved destruction methods. Approved methods shall be employed in accordance with local, state and federal rules. These methods may include but are not limited to: burning, shredding or other approaches to rendering the media unusable, i.e., degaussing, which uses electro-magnetic fields to erase data, or, preferred for magnetic media when media will not be physically destroyed, “zeroization” programs (a process of writing repeated sequences of ones and zeros over the information). CD-ROMs, DVDs, magneto-optical cartridges and other storage media that do not use traditional magnetic recording approaches must be physically destroyed. Disposal of IT Assets: Disposal of information system equipment, including the irreversible removal of information and software, must occur in accordance with approved procedures and will be coordinated by IT personnel.

18. CYBER BREACH AND NOTIFICATION PROCEDURES

Definition

Cyber Security Breach is any incident that results in unauthorized access to computer data, applications, networks, or devices. A Data Breach is a security violation (e.g., unintentional information disclosure, data leak, information leakage, data spill), in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Statement of Policy

Any individual who suspects that a theft, breach, or exposure of HOC Protected data or HOC Sensitive data has occurred must immediately provide a description of what happened to the HOC Compliance Division via email.

Purpose

To outline the process for notifying affected individuals of a breach of protected information under the Privacy Act, unsecured protected health information (PHI) for the purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act ("HITECH"), and/or state breach notification purposes.

Scope

This applies to all employees, volunteers, and other individuals working under contractual agreements with HOC.

Definitions

State Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of Personal Information that compromises the security, confidentiality, or integrity of the Personal Information.

Personal Information – Personal Information has many definitions including definitions by statute, which may vary from state to state. Most generally, Personal Information is a combination of data elements, which could uniquely identify an individual. Please review applicable state Data Breach statutes to determine what definition of Personal Information is applicable for purposes of the document.

HIPAA Breach – Unauthorized acquisition, access, use, or disclosure of unsecured PHI.

Personally Identifiable Information ("PII") – Information in any form that consists of a combination of an individual's name and one or more of the following: Social Security Number, driver's license or state ID, account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or other information which could be used to identify an individual.

Individually Identifiable Health Information ("IIHI") – PII which includes information related to the past, present or future condition, treatment, payment or provision of health care to the identified individual.

Privacy Act Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information protected by the Privacy Act. This information includes, but is not limited to Social Security Number, government issued ID numbers, financial account numbers or other information posing a risk of identity theft.

Private Information – Information protected by the Privacy Act, Personally Identifiable Information, Personal Information and Protected Health Information collectively.

Protected Health Information (PHI) – Individually identifiable health information except for education records covered by FERPA and employment records.

Procedure

Reporting a Possible Breach

1. Any employee who becomes aware of a possible breach of privacy involving Private Information in the custody or control of HOC will immediately inform their supervisor/manager.
    a. Notification should occur immediately upon discovery of a possible breach.
2. The supervisor/manager will verify the circumstances of the possible breach and inform the Chief Compliance Officer, Chief Technology Officer, the division Administrator/Director, Security Breach group and HOC Help Desk immediately.
    a. Email helpdesk@hocmc.org and securitybreach@hocmc.org.
    b. Provide as much detail as possible.
    c. Be responsive to requests for additional information.
    d. Be aware that the Chief Compliance Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.

Containing the Breach

1. Members of the Security Breach group will take the following steps to limit the scope and effect of the breach.
    a. Work with division(s) to immediately contain the breach. Examples include, but are not limited to:
        i. Stopping the unauthorized practice.
        ii. Recovering the records, if possible.
        iii. Shutting down the system that was breached.
        iv. Mitigating the breach, if possible.
        v. Correcting weaknesses in security practices.
        vi. Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity. Any notification to the authorities must be in conjunction with the Executive Director and legal counsel.

Investigating and Evaluating the Risks Associated with the Breach

1. To determine what other steps are immediately necessary, the Chief Compliance Officer in collaboration with the HOC's Legal Counsel and affected department(s) and administration, will investigate the circumstances of the breach.
    a. A team will review the results of the investigation to determine root cause(es), evaluate risks, and develop a resolution plan.
    b. The Chief Compliance Officer, in collaboration with HOC Legal Counsel, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:
        i. Contractual obligations.
        ii. Legal obligations – the HOC Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment to the Chief Compliance Officer and the rest of the breach response team.
        iii. Risk of identity theft or fraud because of the type of information lost such as social security number, banking information, identification numbers.
        iv. Risk of physical harm if the loss puts an individual at risk of stalking or harassment.
        v. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records.
        vi. Number of individuals affected.

Notification

1. The Chief Compliance Officer will work with the division(s) involved, HOC Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
2. If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach.
    a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
        i. Notices must be in plain language and include basic information, including:
            1. What happened;
            2. Types of data involved;
            3. Steps individuals should take;
            4. Steps covered entity is taking; and
            5. HOC Contact Information.
        ii. Notices should be sent by first-class mail or if an individual agrees, electronic mail or phone call. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.
    b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.
3. The required elements of notification vary depending on the type of breach and which law is implicated. As a result, the HOC Chief Compliance Officer and Legal Counsel should work closely to draft any notification that is distributed.

4. Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.
    a. If deemed appropriate with a mass breach consisting of five hundred (500) or more individuals and contact information is insufficient for direct communications, HOC may notify a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.
5. Using multiple methods of notification in certain cases may be the most effective approach.

Business associates must notify the HOC if they incur or discover a breach of unsecured PHI.

1. Notices must be provided without reasonable delay and in no case later than sixty (60) days after discovery of the breach.
2. Business associates must cooperate with the HOC in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If the HOC Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five hundred (500) or more individuals, regardless of location, must be submitted to HHS at the same time that notices to individuals are issued.
2. If a breach involves fewer than five hundred (500) individuals, the HOC will be required to keep track of all breaches and to notify HHS within sixty (60) days after the end of the calendar year.

Prevention

1. Once immediate steps are taken to mitigate the risks associated with the breach, the Compliance Officer will investigate the cause of the breach.
    a. If necessary, this will include a security audit of physical, organizational, and technological measures.
    b. This may also include a review of any mitigating steps taken.
2. The Compliance Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

Compliance and Enforcement

All division directors, managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to discipline up to and including termination in accordance with the Collective Bargaining Agreement and HOC Personnel Policy.

PLAN REVISION

Revision	*Date*	*Summary of Changes*	*Approved by*
1.0	3-2-2022	Document Creation	
1.1	5-6-2022	Addressed CLA requested revisions as of 5/4/2022	

Housing Opportunities Commission OF MONTGOMERY COUNTY

10400 Detrick Avenue
Kensington, MD 20895-2484
(240) 627-9400

HOUSING OPPORTUNITIES COMMISSION OF MONTGOMERY COUNTY
TELEWORK POLICY

PURPOSE AND SCOPE

Telework is the employee's performance of duties and responsibilities of their position from home. Telework is intended to be a transparent arrangement. Teleworkers and supervisors should maintain awareness of its effect on position responsibilities and proactively adapt to minimize any negative effect on the work.

While telework is a critical element of an employee-friendly and family-friendly workplace, other options are available to employees and managers to accomplish this goal. These options include the use of Compressed Work Schedules and Flex Time**.** HOC's goal is to utilize telework to establish a more efficient, responsive, and resilient approach to providing services to customers and businesses in the community**.** Other advantages of telework include:

- Providing healthy work environments to foster an engaged workforce better able to balance work and life commitments.
- Enhancing recruitment and retention of employees.
- Building a more resilient organization prepared for future crises where we limit barriers to getting work done when in-office work is not possible.
- Leading other organizations within the County and region towards achieving environmental and health goals through more limited commuting.
- Contributing to achieving the County's greenhouse gas reduction goals to help move our community and our nation toward a better future.
- Cost savings for reduced office space needs.

Telework

It is important that the home office be conducive to the work to be performed and free from unnecessary distractions. HOC provides standards for the telework location in the section on "Workspace." Anyone requesting to work from a location other than their home, even temporarily, must get approval from their Division Director. Employees must notify their immediate supervisor of any changes to their telework location. All regular telework locations must be within 90 miles of the employee's HOC worksite.

Not all positions and not all employees are good candidates for telework. Some positions require direct face-to-face contact with customers or direct service that can only be done in-person or at a specific work location. In some cases, a position's duties and responsibilities may be restructured so that duties and assignments that can be performed through a telework arrangement are done in that manner and duties not suited to telework are performed in the traditional work setting.

It is also important to recognize that the telework location is not intended to duplicate the flexibility of the traditional work setting. Under no circumstances are work related in-person meetings to be conducted at an employee's home.

The key to a successful telework arrangement is individual proficiency with the tools and equipment that enable the employee to be productive while teleworking, including the ability to manage and prioritize the work requirements independently.

A teleworker who participates in the Telework Program more than half the time may be required to relinquish their office space and utilize a hoteling station when they are at the Main Worksite. In the event a teleworker does not have a dedicated workspace at the Main Worksite, the teleworker will be provided with a locking cabinet or drawer in which personal items may be stored for safekeeping while they are at the Main Worksite.

GENERAL ROLES AND RESPONSIBILITIES

Telework relies on multiple parts of the organization coordinating action through defined roles and responsibilities.

Human Resources - Administers HOC'S Telework Program

- Appoint a Telework Manager, who provides HOC's oversight to the program and searches for solutions to continuously improve teleworking.
- Provides guidance on position suitability and employee eligibility criteria for the departments/ divisions to apply.
- Assists departments/divisions in achieving the goals set forth.
- Provides direction to departments/divisions in the areas of pay and leave; Agency closure; Performance Plan and Review process; recruitment and retention; and accommodations for persons with disabilities, **c**onsistent with the Collective Bargaining Agreement (for represented staff) and Agency practices.
- Coordinates with other departments that play a role in teleworking such as Information Technology and Facilities.
- Acts as an information resource for teleworkers, departments and supervisors.
- Supports departments, teams, and employees–by providing education and training on best practices in telework environment.
- Coordinates Telework Application and Termination processes **(**including the Union Appeals process for represented staff).

HOC Departments/Divisions - Implement HOC Telework Program

- Maintain telework agreements.
- Determine position suitability for participation in telework.
- Work with Human Resources (HR) to meet telework objectives consistent with operational needs.
- Report to HR on the progress of implementing the telework program to include the approved number of telework participants and the approved frequency of participation.

- Incorporate telework into departmental Continuity of Operations Plans consistent with existing HOC policies and procedures.
- Division Directors will agree or disagree with the supervisor's recommendation by approving or denying Telework Applications.
- Submit all Telework Applications, whether approved or denied, to the Human Resources Office.

Supervisors - Facilitate Employee and Team Telework Success

- Implement telework agreements with individual employees and establish clear expectations with the employees regarding performance.
- Recommend Telework Applications for approval or denial and submit to the Department Director with supporting documentation.
- Ensure the individual has the appropriate training and equipment for successful teleworking.
- Identify and remove barriers to telework by utilizing new and/or available technologies and updating work processes, consistent with operational need.

Teleworkers – Maintain or Enhance Services and Outcomes for HOC Customers

- Submit a Telework Application, collaborate with supervisor to execute a telework agreement, and attend telework training as required.
- Prepare and plan for unexpected teleworking situations to ensure organizational resilience in the face of emergencies.
- Teleworking employees are expected to be able to attend on-site events that are needed to fulfill the responsibilities of their position. Each employee's telework agreement will clarify expectations regarding on-site availability. Just as with on-site employees, commuting expenses are the responsibility of the employee.
- Telework employees agree to perform only official duties and not to conduct secondary employment or personal business during scheduled working hours. Personal business includes, but is not limited to, actively caring for dependents, making home repairs, running errands, etc. during working hours.
- Teleworkers are required to immediately notify management of any changes that may alter their telework agreement.

PARTICIPATION IN TELEWORK

Participation in the Telework Program is voluntary. The expectation is that any employee in a position eligible for telework will be prepared for telework should the occasion arise. Position duties and responsibilities may be restructured so that duties and assignments that can be performed through a telework arrangement are done in that manner and duties not suited to telework are performed at the HOC worksite.

Employee participation in telework may fall in one of the following categories:

- Recurring telework – employees work from a remote location on a regular, recurring basis up to five (5) days per week.

- Intermittent/Situational telework – employees would generally work on-site, but would telework for limited periods of time based on either circumstances impacting the availability of the HOC worksite, or job responsibilities that could best be accommodated by working remotely.
- On-site – employees do not telework.

Employees working remotely and employees working on-site have equal responsibility to provide seamless access to information and participate in work functions, as well as video conferencing and meetings to fully support a partially remote telework environment.

ELIGIBLE POSITIONS

For the purposes of the Telework Program, the Housing Opportunities Commission has developed the standards listed below for the determination of position eligibility.

- The essential functions of the position must be able to be performed off-site with access to Google Drive, email, and phone support.
- Telework employees must be able to troubleshoot routine problems independently or with only phone assistance from the Informational Technology Division.
- The employee must be able to work independently and plan and carry out assignments with little assistance or direction from others.
- Confidentiality of proprietary information of the Housing Opportunities Commission must be maintained.
- Service delivery to the customers of the position, internally and externally, must be maintained or improved.

Examples of duties typically suitable for remote work/telework

Many positions have duties which are "portable" and thus should be at least in part compatible with remote work. These tasks do not require employees to be physically present at the worksite. Examples include:

- Reading/reviewing documents, articles, or emails
- Data entry and analysis
- Receiving and making telephone calls
- Performing research
- Analyzing documents and studies
- Preparing written letters, memorandums, reports, and correspondence
- Preparing presentations
- Participating in virtual programs/events
- Setting up and participating in conference calls or online/virtual meetings
- Participating in and creating professional development and training
- Collaborating with team members and supervisors

Duties not typically suitable for remote work/telework

Functions which require on-site, physical interface or interaction in order to be fully effective typically do not lend themselves to being performed effectively remotely. In some cases, these interactions may

involve direct service to the public; in other cases, the duties require a physical presence for other reasons and may include the following:

- On-site Events – e.g., duties that must be performed in a building or other structure, a promotional event such as groundbreaking ceremonies, town hall meetings, snow removal etc.
- Job Duties – e.g., maintenance work for housing units and HOC facilities, performing on-site inspection activities, leasing activities, and other responsibilities such as picking up and delivering mail as well as functions which require use of equipment located at HOC facilities, large scale scanning and printing.
- Individuals – e.g., positions that work with people that require in-person interaction or oversight, etc.
- Outside organizations or entities – positions that require in-person interaction or oversight e.g., a senior living complex, etc.

EMPLOYEE REQUESTS TO TELEWORK

Employees may request to participate in the Telework Program by completing a Telework Application. The Application allows the employee to respond to several questions concerning the duties and responsibilities of their position. The questionnaire is designed to assist the employee, supervisor, and Division Director in studying the essential functions of the job in order to determine whether and how, all or some of the duties and responsibilities of the employee's position can be performed through a telework arrangement and to address any service concerns.

When evaluating employee requests for telework, supervisors should consider whether certain portions of the employee's work are portable and lend themselves to telework, as discussed in the section on Duties Appropriate for Telework. The request and approval process should consist of a conversation between the supervisor and employee with respect to the amount and frequency of telework given the duties of the position and operational needs of the department. Supervisors must approve or deny the employee's telework request within 14 calendar days.

Restructuring of the position's duties and responsibilities within the position to develop a workload that can be accomplished through telework is allowable provided it does not negatively impact service delivery or performance, however, a position's duties and responsibilities may not be altered. For example, removing a task from a telework candidate and assigning it to another employee in order to meet the standards for telework is not acceptable.

If an employee's telework request is denied, HOC must identify in writing how the request as submitted could lead to the erosion of the level and/ or quality of the services provided by the requesting employee's position.

Continued Participation in Telework

Employees must maintain competencies in critical areas to perform successfully in a telework environment. It is the responsibility of the supervisor to periodically assess performance to ensure the employee maintains performance standards for their position in a telework environment.

Supervisors must provide employees with information concerning how the employee's performance will be measured under a telework arrangement and provide coaching and feedback, where necessary to achieve these objectives.

Successful telework hinges on the following:

- Strong time management skills
- Strong communication skills
- Ability to prioritize
- Proficiency with technology
- Meeting the Workspace Requirements

Computer Requirements

Employees participating in the HOC Telework Program must have an HOC issued laptop to properly interface with the HOC Network systems. The Information Technology (IT) Division will not send technicians to the off-site location to perform service.

Candidates selected for the Telework Program and their supervisors will be required to attend a training provided by the Human Resources Office to familiarize themselves with troubleshooting standard telework problems (such as using VMware, contacting IT etc.).

TOOLS AND EQUIPMENT

HOC Provided Tools and Equipment

Employees participating in the Telework Program will be responsible for the cost, purchase, and maintenance of additional office equipment and supplies necessary to properly furnish the workspace used for telework. Consumable office supplies typically used by the employee in the course of business at HOC will be provided by HOC. If in doubt, the employee is advised to discuss their needs with their supervisor.

While HOC will provide standard consumable office supplies, supplies will not to be delivered to the telework location by HOC. It is the responsibility of the employee to pick up the supplies at HOC offices and transport them to their home office.

Employees can bring home IT related equipment that is currently provided for their exclusive use (e.g., a laptop, second monitor, or docking station) with the Division Director's and IT's approval. Such requests shall not be unreasonably denied. Shared equipment must remain at the office (e.g. printers, copiers). HOC will not provide duplicate items, equipment, or devices unless approved by ADA Accommodation.

Employee-Provided Equipment/Utilities

Unless equipment is provided by HOC, the teleworker is responsible for the purchase, installation, and maintenance of all equipment and services needed to telework. HOC shall not be responsible for the purchase, maintenance, repair, and operational costs of any personal devices. Employees are responsible for ensuring access to bandwidth to perform their assigned duties. Employees are expected to acquire

internet service and other general utilities at their own expense. The teleworker must have adequate broadband speed necessary to conduct HOC business remotely (a minimum of 15 Mbps).

The use of personal mobile devices for HOC work is permitted but devices must always be password protected and encrypted. Teleworking employees are eligible for the cell phone stipend. Documents, information, and emails concerning HOC business remain the property of HOC when they are stored on personal devices. Sensitive information must not be stored or accessed on non-HOC controlled devices.

Workspace

Employees participating in the Telework Program must designate a specific workspace for telework. The home office must be maintained by the employee in a clean, professional, and safe condition. To ensure that these conditions are met, the following standards apply:

- Employees must arrange an appropriate workspace at their home where noise levels can be controlled.
- Employees must be able to take telephone calls and participate in online video meetings with minimal distractions while maintaining appropriate confidentiality.
- The teleworker must have a comfortable office chair with adequate back support. The Agency will not provide furniture for the employee's remote workspace unless an ADA request is approved.
- Entryways to the workspace must be clear of obstructions at all times.
- The workspace must be neat, clean, and free of obstructions.
- The workspace must be free of potential hazards that could cause physical harm such as frayed wires, bare conductors, loose wires, exposed wires to the ceiling, frayed or torn carpeting seams, uneven floor surfaces, etc.
- Electrical outlets must be properly grounded and three pronged. Surge protectors may serve this purpose.
- Phone lines, electrical cords, and extension wires must be properly secured behind furniture to ensure no danger of entanglement.
- Lighting must be sufficient for reading and writing.
- Consistent with the Agency's expectations of information security for employees working in an HOC office, teleworking employees will be expected to ensure the protection of documents at their home office. Steps include the use of a locked file cabinet and desk, regular password maintenance, and other steps appropriate for the job and the environment.
- Temperature is comfortable and can be adjusted as needed.
- Homeowner's insurance and any changes in rates or coverage are the responsibility of the employee. Any increase in the teleworker's home utility costs is the responsibility of the employee.

The employee's off-site workspace is also considered an extension of the Agency's workspace. Therefore, the Agency maintains liability for job-related accidents that occur in the off-site workspace during the employee's working hours. Please note that Workers Compensation liability is limited to the designated workspace as opposed to all areas of the home. HOC assumes no responsibility for the employee's personal property. Work related in-person meetings are not to be conducted at an employee's home under any circumstances.

In accordance with HOC's Incident/Accident procedures, accidents occurring at the telework location must immediately be reported to the Human Resources Office and the employee's direct supervisor. The employee is also required to complete an Incident/Accident Report and forward the completed form to their supervisor, their Division Director, and Human Resources within 24 hours of the incident. Any accidents occurring in a telework location may include an inspection of the work-site as directed by HOC's Worker's Compensation administrator.

WORK SCHEDULE/TIME AND ATTENDANCE

The Telework Agreement outlines which work day(s) the employee will telework. Telework Agreements must be structured around circumstances which require the physical presence of the employee in the traditional work setting. For example, critical processes that can only be performed at the traditional work location, or standing meetings in which the employee's physical presence is required.

Consideration should also be given to the work flow of the employee's position, and the work flow of the department to which the employee is assigned to ensure that performance or service will not be negatively affected.

Participants in the Telework Program must adhere to the Telework Work Schedule that is approved. In addition, the supervisor may require the employee to report to the traditional work setting on planned telework days based on identified operational needs or exigent circumstances that require the employee to be on-site to perform duties that could not be performed remotely via telework**.**

Employees in the Telework Program continue to follow the Agency's Time and Attendance standards and adhere to their approved Work Schedule, including work hours, while teleworking. Flexible Work Schedules and Compressed Work Schedules are allowed in a telework arrangement. Telework employees must obtain advance supervisory approval before performing work in excess of their regular work schedule. As always, Overtime and accrual of Compensatory Time Leave must be approved by the employee's supervisor in advance. Requests for leave use must also be approved in advance. With prior supervisory approval, employees may change telework days during a specific week.

CUSTOMER SERVICE, PERFORMANCE, AND TELEWORK

All HOC employees are required to maintain the Customer Service standards for the Housing Opportunities Commission. When an application for telework is submitted, it is important that telework participants and their supervisors discuss the effect of telework on customer service.

Telework employees and their supervisors must develop standard procedures to ensure no loss in service delivery as a result of telework.

Employees participating in the Telework Program are expected to provide the same level of service as would be provided as though they were in the office, including reviewing and responding to email and phone messages. Supervisors and telework applicants should also consider the manner of communication between each other while the employee is teleworking.

SECURITY

Teleworking employees must follow the same Commission and Departmental security and privacy practices that are required at the primary workplace. HOC may assess or enforce additional security protections on personally owned devices systems or systems. HOC business must never be conducted from a non-HOC email address or from an open Wi-Fi such as restaurants, coffee shops, retail shops, etc.

TERMS AND CONDITIONS OF TELEWORK AGREEMENTS

A. While teleworking, the employee is bound by all HOC rules, policies, practices, and instructions as if they were working at the official duty station.
B. To maintain optimal customer service, teleworkers should have their camera on when meeting with customers virtually. Teleworkers are also required to have cameras on in internal virtual meetings when requested by the host.
C. Telework employees will be rated consistent with the performance expectations outlined in their Performance Plan and Review Document.
D. A teleworker may also have a Flex Time or Compressed Work Schedule.
E. The employee understands that they must comply with the terms of their Telework Agreement. If performance requirements or conduct expectations are not met, the supervisor will follow the procedures for discipline or performance coaching and feedback provided in HOC Personnel Policy and the Collective Bargaining Agreement, as appropriate.
F. Under no circumstances are work-related in-person meetings to be conducted at a remote work location.
G. If an HOC employee who typically teleworks on a given day is needed to be physically present at the worksite due to identified operational need, they may be required to change their telework schedule for a period not to exceed 10 working days. Employees must be prepared to report to the office with 24 hours advanced notice.
H. Employees who provide direct customer service or who perform unique functions may be required to report to the office on the same day in extraordinary circumstances (such as multiple unscheduled absences of on-site workers). Volunteers will be solicited first. Should there not be sufficient volunteers, employees shall be mandated to report in order of inverse seniority.

DISCONTINUATION OF TELEWORK

Telework participation may end due to any of the following conditions:

- The employee no longer meets the qualifications for the Telework Program.
- The employee's performance has been negatively affected or the department's service level declines as a result of the employee's participation in the Telework Program.
- The teleworker develops a pattern of not being responsive after repeated coaching and feedback from their supervisor.
- In instances when an employee has received a conduct-related disciplinary suspension, telework may be suspended for up to 90 days following completion of the suspension.

- Repeated failure of an employee to abide by any material portion of the Telework Agreement.
- HOC's **Executive Director or designee** needs to **temporarily suspend** the telework arrangement to carry out the missions of government **during** a demonstrated situation of emergency that requires the employee's physical presence to manage the emergency.
- A telework participant requests to discontinue their participation in the Telework Program.

To properly document and evaluate all reasons for discontinuation from the Telework Program, completion of a Telework Discontinuation Form is required. Employees that would like to challenge the discontinuation can go through the appeals process (outlined in the appeals section of this document).

APPEAL PROCESS

The Union and the Employer share a joint interest in resolving disputes arising from an employee's telework request. To minimize these disputes, the parties agree to utilize the following process:

Step 1: A written request appealing the denial must be presented to the immediate supervisor, Division Director and HR by the Union within 14 calendar days from the date of the denial of the telework request. Within 14 calendar days of receiving the written request, a representative from the Department, HR, Labor Relations, and the Union must make reasonable efforts to informally resolve the matter prior to the panel review identified in the section below.

Step 2: If the matter is not fully resolved in Step 1, the Union may, within 5 days of the conclusion of the timeframe in Step 1, file a request with HR to convene a three (3) member panel. The panel will be comprised of one representative from the Union, one representative from management and a mutually agreed upon mediator. Panelists will not review appeals of employees working within their department. Similar to the ADR process, each side will be permitted to make a brief presentation before the panel not to exceed 20 minutes, with each side having the opportunity to respond not to exceed 5 minutes each. The panel members will then have the opportunity to question the respective parties, after which the panel will caucus in private and present a recommendation.

Step 3: If the recommendation is not adopted, the Union may invoke arbitration in accordance with the Collective Bargaining Agreement. The Union shall be required to establish that denial of the telework request violated the Collective Bargaining Agreement.

DATA SHARING – REPRESENTED EMPLOYEES ONLY

The Employer shall share Telework Application denials along with supporting documentation provided by the supervisor to the Union within five (5) business days of receipt of request from the employee or the Union.

M E M O R A N D U M

TO: Housing Opportunities Commission of Montgomery County
Administrative and Regulatory Committee

VIA: Kayrine Brown, Acting Executive Director

FROM: Staff: Lynn Hayes Division: Housing Resources Ext. 9622
Guidy Paul Ext. 9553

RE: Authorization to Revise Administrative Plan for the Housing Choice Voucher Program to add clarity to Chapters 4, 7, 8, and 21

DATE: May 16, 2022

STATUS: Consent _____ Deliberation __X__ Status Report _____ Future Action _____

OVERALL GOAL & OBJECTIVE:

To request that the Administrative and Regulatory Committee join staff's recommendation to the Housing Opportunities Commission of Montgomery County ("HOC") to adopt revisions to HOC's Administrative Plan for the Housing Choice Voucher program to update and clarify Chapters 4, 7, 8, and 21 of the Plan (the "Revisions"), and authorize the Acting Executive Director, or her designee, to implement the revisions to the Administrative Plan for the Housing Choice Voucher Program ("Administrative Plan").

BACKGROUND:

HUD provides the outline of basic policies and procedures for the administration of the Housing Choice Voucher ("HCV") program in the Code of Federal Regulations ("CFR") at 24 CFR Part 982, Subpart E. Beyond the policies outlined in the CFR, Public Housing Authorities ("PHA") must develop Agency-specific policies and procedures on matters for which the PHA has discretion to establish local policies. These Agency-specific policies are written in the PHA's Administrative Plan.

The administrative plan must be in accordance with HUD's regulations and requirements, and cover specific policies, including waitlist preferences, voucher extensions, and special housing. As such, HOC is recommending revisions to chapters 4, 7, 8, and 21 of the Administrative Plan. The detailed changes are provided in Exhibits A, B, C, and D.

An overview of the recommended changes includes the following:

- Chapter four (4) details the administration of the waitlist and the six adopted waitlist

preferences. Staff propose an amendment to the first preference, to include forced displacement of families resulting from a fire, flood damage, and natural disaster.

- Chapter seven (7) details the verification processes used to determine program eligibility, including the verification of income. Staff propose that self-employed individuals must certify that a minimum of 51% of their business is conducted in Montgomery County.

- Chapter eight (8) details the voucher issuance process. Staff propose that voucher extensions are granted to all customers who request an extension prior to the voucher expiration date for a maximum search time of 180 days. The current policy is applicable only to disabled customers for a maximum term of 150 days. A completed search record is required with a minimum of 10 entries. A Family may request a reasonable accommodation if additional search time is needed in excess of 180 days.

- Chapter 21 details the HCV Homeownership Program. This program is limited to twenty-five (25) participants of which three (3) slots are designated for disabled families. The administration of the HCV Homeownership Program is a collaborative effort between the Housing Resources Division and Mortgage Finance Division. Annually, the Area Median Income ("AMI") for Montgomery County is updated. This income is used to determine the minimum income requirement for participation in the homeownership program. The current requirement has increased from $24,000 to $40,000.

The recommended changes will ultimately increase the opportunities for the residents of Montgomery County to find safe, affordable housing and reduce the risk of homelessness.

As part of the process for making revisions to a PHA's Administrative Plan, public comment is required. Accordingly, HOC will provide a 30-day public comment period, which will conclude with a public hearing on July 6, 2022, on the Administrative Plan revisions. During the comment period, HOC will make a draft of the proposed revisions to the Administrative Plan available on the Agency's website as well as in hard copy form at all four of HOC's primary offices. Also during the comment period, HOC staff will meet and discuss these proposed revisions with HOC's Resident Advisory Board ("RAB"), seeking the RAB's comments and endorsement of these proposed changes. Notice of the comment period and public hearing will be advertised in a local newspaper in Montgomery County.

ISSUES FOR CONSIDERATION:

Does the Administrative and Regulatory Committee wish to join staff's in its recommendation to the Housing Opportunities Commission of Montgomery County to adopt revisions to HOC's Administrative Plan for the Housing Choice Voucher program to update revisions and clarifications to Chapters 4, 7, 8 and 21 of the Plan, and authorize the Executive Director, or her designee, to implement the revisions to the Administrative Plan for the Housing Choice Voucher Program?

TIME FRAME:

For discussion by the Administrative and Regulatory Committee at its meeting on May 16, 2022. For formal Commission action on July 6, 2022.

STAFF RECOMMENDATION & COMMISSION ACTION NEEDED:

Staff recommends that the Administrative and Regulatory Committee join staff in its recommendation to the Housing Opportunities Commission of Montgomery County to adopt revisions to HOC's Administrative Plan for the Housing Choice Voucher program to update revisions and clarifications to Chapters 4, 7, 8 and 21 of the Plan, and authorize the Executive Director, or her designee, to implement the revisions to the Administrative Plan for the Housing Choice Voucher Program.

EXHIBIT A

Chapter 4

ESTABLISHING PREFERENCES AND MAINTAINING THE WAIT LIST [24 CFR Part 5, Subpart D; 982.54(d)(1); 982.204, 982.205, 982.206]

INTRODUCTION

It is HOC's objective to ensure that families are placed in the proper order on the wait list and selected from the wait list for admission in accordance with the policies in this Administrative Plan.

This chapter explains how HOC will administer its consolidated wait list for all of its housing programs, including the tenant-based and project-based voucher wait lists, hereinafter referred to as the consolidated list or master list. The tenant-based wait list has ~~five~~ six local preferences that HOC adopted to meet local housing needs, define the eligibility criteria for the preferences, and explain HOC's system of applying them. The wait list for housing subsidized with project-based vouchers is maintained as a sub list within the consolidated list. Any family selected to be housed utilizing a project-based voucher is only eligible for a specific bedroom sized unit based on their family size.

By maintaining an accurate wait list, HOC is able to perform the activities which ensure that an adequate pool of qualified applicants is available, so that program funds are used in a timely manner. Each family on the tenant-based wait list may also have its name on the project-based wait list.

A. MANAGING THE WAIT LIST

Opening and Maintaining the Wait List

Opening of the wait list will be announced with a public notice stating that applications for public housing, Housing Choice Voucher and all other wait lists maintained by the **Housing Opportunities Commission of Montgomery County (HOC)** will again be accepted. The public notice will state where, when, and how to apply. The notice will be published in a local newspaper of general circulation and also by any available minority media, including social media. The public notice will state any limitations on who may apply. Wait lists for all sub-jurisdictions and Countywide will be opened and closed at the same time.

The notice will state that applicants already on wait lists for other housing programs must apply separately for this program and such applicants will not lose their place on other wait lists when they apply for public housing. The notice will include the Fair Housing logo and slogan, and will be in compliance with Fair Housing requirements.

HOC intends for the wait list to remain open indefinitely; however, if the Executive Director decides to close the list, the closing of the wait list will also be announced with a public notice. This public notice will state the date the wait list will be closed, and it will be published in a local newspaper of

general circulation and by any available minority media, including social media.

Organization of the Wait List

In July 2015, HOC merged its existing sub-jurisdictional wait lists for the Housing Choice Voucher program and all other housing programs into one combined wait list, referred to herein interchangeably as merged list, master list, merged master list, or wait list, except as specifically noted.

In conjunction with the merge of all of HOC's wait lists, HOC opened its merged master wait list for all programs, and left the merged list open indefinitely or until such time as a determination is made by the Executive Director that there is cause to close the wait list, at which time proper notice will be posted in a local newspaper of general circulation and by any available minority media, including social media.

Only one application may be submitted and it must be submitted by the head of household or his/her designee.

The wait list is maintained in accordance with the following guidelines:

1. The application will be a permanent file. Any contact between HOC and the applicant will be documented in the electronic applicant file.

2. All applications will be maintained in order of date and time of application, and applicable preference(s).

3. Under the merged wait list, one master list is maintained electronically through a proprietary program. All applications and updates to an application are submitted electronically through a proprietary on-line web portal. Paper and telephone submissions are not permitted. To the extent an applicant requires assistance, upon request, staff from HOC is available to assist with electronic submissions.

4. All applicants must give notice of any changes to their application within two weeks of a change. Changes include: change of mailing address, change of email address, change of phone number, change in family composition, change in income, or changes in factors affecting preference points. As noted in paragraph 3, all changes must be done electronically because paper and telephone submissions are not accepted. To the extent an applicant requires assistance, upon request, staff from HOC is available to assist with electronic update submissions.

5. The master wait list is updated daily and applicants' wait list profiles are accessible via the internet on a 24-hour basis.

6. For the Housing Choice Voucher program, HOC maintains one merged master list in order of date-time stamp and any applicable preference(s). However, within the master list there are sub-sorted separate lists for certain programs and properties. This includes the Choice Mobility wait list for those customers eligible for

project-based to tenant-based subsidy conversion. See Chapter 22 of this Administrative Plan for more information.

7. HOC entered into Housing Assistance Payments (HAP) contracts to subsidize units at several properties that are operated by third-party managers and/or owners. The individual, property-specific wait lists for these properties are included within the master list but are sorted separately to only reflect applicants who satisfy the various property and programmatic eligibility criteria. More specifically, the details regarding these property-specific wait lists are as follows:

   i. HOC maintains separate wait lists for Arcola Towers, Elizabeth House, Holly Hall, and Waverly House, which are housing facilities operated for the benefit of senior and/or disabled customers.

   ii. HOC entered into a HAP contract to subsidize units at Emory Grove, Ken-Gar, Parkway Woods, Sandy Spring Meadow, Seneca Ridge, Town Centre Place, and Washington Square as required as part of the Rental Assistance Demonstration (RAD) program, and required Housing Choice Vouchers. The individual wait lists created for these RAD properties are included in the merged master list but are sorted separately to reflect only those applicants who are eligible for these properties.

   iii. HOC entered into HAP contracts to subsidize units at several properties that are managed by third-party managers and/or owners. These properties provide supportive services to at-risk populations in the form of Housing Choice Vouchers. Applicants for these programs must meet stringent requirements and are ranked by date and time of application only. The individual wait lists created for these properties are included in the merged master list but are sorted separately to reflect only those applicants who are eligible for these properties.

8. Contact between HOC and wait list applicants for the purposes of selection from the list is documented in the applicant's wait list file.

Implementation of RAD Wait List Provisions

Former public housing (PH) applicants and residents receive priority consideration on the site-based wait lists created within *HOC Housing Path*, HOC's electronic wait list. Prior to the opening of the HOC Housing Path wait list, HOC mailed to all former PH wait list applicants a post card notifying them of the new wait list and instructed them to submit an application. The following policies describe how former PH applicants and residents receive priority consideration for housing at all of HOC's RAD-converted properties and at properties with Project-Based Voucher (PBV) assistance provided using the non-competitive selection process created by the Housing Opportunities Through Modernization Act (HOTMA), and described in Chapter 22, Section G of this Administrative Plan.

In order to provide former PH applicants with the best opportunity to be housed at one of the RAD properties, HOC adopted and follows the procedures listed below:

- Analyze HOC Housing Path to identify former PH wait list applicants and residents that have submitted a new application.
- Issue notices to former PH wait list applicants and residents informing them that they are eligible to receive priority consideration for housing at RAD properties, and instruct them to respond to the notice if they would like to be considered.
- Former PH applicants and residents who respond, but have not submitted a new HOC Housing Path application will be instructed to do so.
- For those families who respond to the notice and/or have submitted a new HOC Housing Path application, HOC will create a separate pool of applications that will receive priority consideration for vacancies at HOC's RAD properties.
- As vacancies become available at RAD properties, applicants will be selected from the priority pool based on their date and time of application to Housing Path.

B. WAIT LIST CUSTOMERS (FAMILIES)

All wait list applicants are required to maintain an e-mail address. To the extent an applicant chooses to use the e-mail address of another person, the applicant is solely responsible for receiving information sent to the listed email address and lack of access to that account is not considered a valid excuse for missing notices. To the extent a family does not have an e-mail address, HOC can assist the family in obtaining a free email account. The applicant is responsible for notifying HOC of any change in their e-mail address. HOC maintains public use computers at all of its HUB locations. Public use computers are also widely available at other public locations such as local libraries. To the extent an applicant requires assistance, upon request, staff from HOC is available to assist with electronic submissions.

All wait list applicants are required to list an address in their Housing Path application. If the applicant is homeless or does not have a permanent address, the applicant can choose to list the address of another person, so long as it is not the address of a current voucher holder. This address is used to send any paper correspondence to the applicant, including required paperwork as part of the selection process. The applicant is solely responsible for receiving information sent to the listed address and lack of access to mail at that address is not considered a valid excuse for missing notices or paperwork. The applicant is responsible for notifying HOC of any change in address.

Treatment of Single Applicants

Single applicants are treated as any other eligible family on the wait list for the tenant-based and project-based voucher wait lists.

C. WAIT LIST [24 CFR 982.204]

Tenant-Based Voucher

HOC uses a consolidated wait list for the admission of all of its housing programs. The

consolidated list includes a sub list for admissions to the tenant-based voucher assistance program.

Except for Special Admissions, applicants are selected from the consolidated wait list in accordance with the policies, preferences, and income targeting requirements defined in this Administrative Plan.

HOC will maintain information that permits proper selection from the wait list.

The wait list contains the following information for each applicant listed:

- Applicant Name
- Family Unit Size (number of bedrooms family qualifies for under HOC's subsidy standards)
- Date of application
- Qualification for any local preference(s)
- Racial or ethnic designation of the head of household
- Targeted program qualifications

Project-Based Voucher

HOC maintains separate sub lists for admissions to the project-based voucher (PBV) assistance program. Any applicant that submits an application to the master wait list is also considered for inclusion on the PBV wait list.

Except for Special Admissions, applicants are selected from HOC's wait list in accordance with the policies, preferences, and income targeting requirements defined in this Administrative Plan.

Families are selected from the PBV wait list based on the bedroom size of the unit available at the time of selection.

HOC must maintain information that permits proper selection from the wait list.

The wait list contains the following information for each PBV applicant listed:

- Applicant Name
- Family Unit Size (number of bedrooms family qualifies for under HOC's subsidy standards)
- Date of application
- Qualification for any local preference(s)

. Racial or ethnic designation of the head of household

. Targeted program qualifications

D. SPECIAL ADMISSIONS [24 CFR 982.54(d)(e), 982.203]

If HUD awards HOC program funding that is targeted for specifically named families, HOC must admit these families under a Special Admission procedure.

Special admissions families are admitted outside of the regular wait list process. They may not have to qualify for any preferences, nor are they required to be on the program wait list. HOC administers two Special Programs and maintains separate records of these admissions.

The Family Unification Program (FUP):

The Family Unification Program (FUP) qualifies for special admissions as long as the individuals referred to HOC meet the program definition.

> Family Unification Program-Eligible Family (A family that the Public Child Welfare Agency (PCWA) has certified as a family for whom a lack of adequate housing is a primary factor in the imminent placement of the family's child, or children, in out-of-home care, or in the delay of discharge of a child, or children, to the family from out-of-home care, and that the HOC has determined is eligible for a Housing Choice Voucher.)
>
> Family Unification Program-Eligible Youth (A youth that the Public Child Welfare Agency (PCWA) has certified to be at least 18 years old and not more than 24 years old (has not reached his/her 25th birthday) who left foster care at age 16 or older and who does not have adequate housing, and that HOC has determined is eligible for a Housing Choice Voucher.)

Emergency Housing Vouchers (EHV):

HOC administers 118 Emergency Housing Vouchers (EHVs). Eligible EHV applicants are referred to HOC from the Continuum of Care (CoC) via the Department of Health and Human Services (HHS). HOC can accept direct referrals outside of HHS to facilitate an emergency transfer in accordance with the Violence Against Women Act (VAWA) as outlined in HOC's Emergency Transfer Plan, or if HHS lacks a sufficient number of eligible families to refer. HOC must enter into Memorandum of Understanding (MOU) with a Victims Service Provider (VSP) to accept EHV referrals apart from HHS.

HOC must maintain a separate waitlist for EHV referrals at initial leasing and for any turnover vouchers. HOC cannot issue an EHV subsequent to September 30, 2023. Provided that the re-issuance date is prior to September 30, 2023 the term of the EHV may extend beyond September 30, 2023.

EHV Eligibility Criteria:

Eligible applicants must meet one of the four eligibility categories:

- Homeless,
- At risk of homelessness,
- Fleeing or attempting to flee domestic violence, dating violence, sexual assault, stalking or human trafficking, or
- Recently homeless and for whom providing rental assistance will prevent the family's homelessness or having high risk of housing instability.

EHV customers are not required to meet the local residency preference to live or work in Montgomery County. Additionally, income targeting requirements are not applicable for EHV families. EHV households can range from extremely low incomes (30% AMI) to low incomes (80% AMI).

HOC cannot deny program admission for the following reasons, pursuant to Title 24 part 982.552 and 982.55of the Code of Federal Regulations (CFR):

- If any member of the family has been evicted or terminated from federally assisted housing
- The family owes rent or other amounts owed to a Public Housing Authority ("PHA") in connection with Section 8 or Public Housing assistance
- The family has not reimbursed any PHA for amounts paid to an owner under a Housing Assistance Payment ("HAP") Contract for rent, damages to the unit or other amounts owed by the family under the lease
- The family breached an agreement with the PHA to pay amounts owed to a PHA, or amounts paid to an owner by a PHA
- The family would otherwise be prohibited admission under alcohol abuse standards established by the PHA
- The PHA determines that any household member is currently engaged in or has engaged in drug-related criminal activity, during a reasonable time before the admission

HOC will deny program admission for the following reasons pursuant to Title 24 part 982.553 of the CFR:

- If any member of the household has been convicted of drug-related criminal activity for the manufacture or production of methamphetamine on the premises of federally assisted housing
- If any member of the household is subject to a lifetime registration requirement under a

State sex offender registration program

- If any household member is currently engaged in, has engaged in violent criminal activity within the last 12 months
- If any household member has committed fraud, bribery, or any other corrupt or criminal act in connection with any Federal housing program within the previous 12 months.
- If any household member engaged in or threatened abusive or violent behavior toward HOC personnel within the previous 12 months

Voucher Issuance/Lease Term

HOC will issue the EHV voucher for a term of 120 days. The initial lease term for EHV households can be for a period less than 12 months, regardless of whether the shorter term is the prevailing market practice.

Services

HOC will assist EHV households by providing the following services based on documented need based and funding availability:

- Housing Location - EHV applicants will receive housing location assistance from HOC and/or the CoC. This includes helping the family identify and visit available units, providing transportation assistance and directions, assisting with the completion of rental applications and HOC forms and helping to find an accessible unit that meets the needs of a disabled household.
- Transportation Assistance – HOC will provide transportation assistance to EHV households to help them view and select housing units. HOC will provide up to $150 in transportation assistance per EHV household based on documented need and funding availability.
- Security Deposit - HOC will provide security deposit assistance to EHV households to help them secure housing. HOC will provide up to $2,500 in security deposit assistance per EHV household based on documented need and funding availability. If refundable, the security deposit will be refunded to HOC for future use of eligible EHV households.
- Application Fee/Holding Fee - HOC will provide application and/or holding fee assistance to EHV households to help them secure housing. HOC will provide up to $200 in application and/or holding fee assistance per EHV household based on documented need and funding availability.
- Moving Expenses - HOC will provide moving assistance to EHV households. HOC will provide up to $1,800 moving expenses per EHV household based on documented need and funding availability.
- Essential Household Items - HOC will provide EHV households with assistance to secure essential household items. HOC will provide up to $200 in assistance for essential household items per EHV household based on documented need and funding availability.
- Renters Insurance - HOC will provide EHV households with assistance to secure

renter's insurance. HOC will provide up to $175 in assistance for renter's insurance per EHV household based on documented need and funding availability.

- Furniture - HOC will provide EHV households with assistance to secure furniture. HOC will provide up to $1,000 in assistance for furniture per EHV household based on documented need and funding availability.

Portability

EHV applicants can immediately port to another jurisdiction of their choice. The requirement to have a legal domicile in Montgomery County at the time of the application submission is waived. HOC cannot restrict an EHV family from exercising portability options because they are a non-resident applicant.

If the EHV family moves to another jurisdiction that does not administer an EHV Program, the receiving PHA may absorb the family into its regular HCV program or bill the initial PHA.

If the EHV family moves to another jurisdiction that administers an EHV program, the receiving PHA may only absorb the EHV family with an available EHV allocated voucher. If the PHA does not have an EHV available to absorb the family, it must bill the initial PHA.

The EHV administration of the voucher is in accordance with the receiving PHA's EHV policies.

Initial Certification Exam

HOC can accept income calculations and verifications from third party providers or an examination that HOC conducted on behalf of the family for another subsidized housing program in lieu of conducting an initial examination of income as long as the income was calculated in accordance with the rules outlined at Title 24 CFR Part 5 within the last six months, and the family certifies there has been no change in income or the family composition in the interim. At the time of the family's annual reexamination, HOC must conduct the annual reexamination of income as outlined in 24 CFR 982.516.

EHV applicants may provide third-party documentation which represents the applicant's income within the 60 day period prior to admission or voucher issuance but is not dated within 60 days of HOC's request.

HQS Inspections

HOC can pre-inspect available units that EHV Families may be interested in leasing. If an EHV family selects a unit that passed a HQS inspection within 45 days of the date of the Request for Tenancy Approval (RFTA) Form, the unit may be approved as long as it meets all other conditions under Title 24 part 982.305 of the CFR.

Interim Examinations

When adding a family member after the EHV family has been placed under a Housing Assistance Payment (HAP) Contract, the regulations at 24 CFR 982.551(h)(2) apply. Other than the birth, adoption or court-awarded custody of a child, the HOC must approve additional family members and may apply its regular screening criteria in doing so.

EHV applicants may provide third-party documentation which represents the applicant's income within the 60 day period prior to admission or voucher issuance but is not dated within 60 days of HOC's request.

The following are examples of types of program funding that may be designated by HUD for families living in a specified unit.

1. A family displaced because of demolition or disposition of a public or Indian housing project;
2. A family residing in a multifamily rental housing project when HUD sells, forecloses or demolishes the project;
3. For housing covered by the Low Income Housing Preservation and Resident Homeownership Act of 1990;
4. A family residing in a project covered by a project-based Section 8 HAP contract at or near the end of the HAP contract term; and
5. A non-purchasing family residing in a HOPE 1 or HOPE 2 project.

Applicants who are admitted under Special Admissions, rather than from the wait list, are identified in HOC's database with special codes.

At turnover:

If a voucher issued to an FUP-eligible family or FUP-eligible youth under the FUP program is terminated, the voucher is reissued to the extent practicable, to another FUP-eligible family or FUP-eligible youth. If the award on turnover is not practicable, FUP vouchers may be used by HOC for such families based upon local needs.

If a customer served through Special Admissions in the FUP program is on an HOC Program Admissions Wait List (Tenant Based Voucher or Project Based Voucher), the client remains eligible on the wait list for the period of time the list is active. If a client is selected from the Program Wait List and utilizes the voucher, the FUP voucher is reissued, to the extent practicable, to another FUP-eligible family or FUP-eligible youth.

E. WAIT LIST PREFERENCES [24 CFR 982.207]

When a family is selected from the wait list, the family is invited to an interview and the verification process begins. It is at this point in time that the family's wait list preference(s) are verified. To qualify for a preference, an applicant must provide verification that shows he or she qualified either at the time of the initial application or at the time of selection from the wait list. However, placement based upon preference is dependent on the family still qualifying for the preference at the time of selection.

If the family no longer qualifies to be near the top of the list, because the family does not qualify for a preference, then the family's preference status is removed. Importantly, however, the family will remain on the wait list based upon their original date and time of application. HOC must notify the family in writing of this determination and give the family the opportunity for an informal hearing to appeal the decision.

Once a preference is verified, the family completes a full application, presents Social Security number information, citizenship/eligible immigrant information, and signs the Consent for Release of Information forms.

An applicant is not granted any local preference for the tenant-based and project-based voucher wait lists if any member of the family was evicted from housing assisted under a HUD 1937 Housing Act program during the past three years because of drug-related criminal activity or felonious charged criminal activity.

HOC will grant an exception to such a family if:

- The responsible member has successfully completed a rehabilitation program;
- The evicted person clearly did not participate in or know about the drug-related activity; and/or

☐ The evicted person no longer participates in any drug related criminal activity.

If an applicant makes a false statement in order to qualify for a local preference, HOC will deny the local preference.

F. LOCAL PREFERENCES [24 CFR 5.410]

HOC offers public notice when changing its preference system and the notices are publicized using the same guidelines as those for opening and closing the wait list.

HOC uses the following local preference system:

First Local Preference – Displacement: Families who are displaced as a result of a fire, flood, natural disaster, State or County redevelopment project, or a change in the nature of a project that is part of the County plan for maintaining affordable housing, and who are referred by the County Executive's Office. A signed certification from the County Executive's office is required for the family to qualify for this preference. [Two Points]

Second Local Preference – Residency preference for families who live, work, or have a bona fide offer to work in Montgomery County. To qualify for this preference, evidence is required either at the time of application or at the time of selection from the wait list. HOC will treat graduates of, or active participants in, education or training programs in Montgomery County as residents of Montgomery County if the education or training program is designed to prepare individuals for the job market. To qualify and satisfy this preference, graduates must have graduated after the initial application for housing. [One Point]

Third Local Preference – HUD funded 2006 Main Stream Disabled (MSD) program; 15 units. [Two Points]

Fourth Local Preference – Veterans: Preference is given for ten (10) veterans and their families. The applicant must be at least 18 years old and a veteran.

HOC verifies the preference with a list of homeless veterans and their families provided by the Montgomery County Department of Health and Human Services (DHHS). [Three Points]

Fifth Local Preference – Families with Histories of Homelessness: Preference is given for ten (10) families with histories of homelessness who are currently housed within the Montgomery County Homeless Continuum of Care. The applicant must be at least 18 years old and have at least one minor child (under the age of 18) within the household.

HOC verifies the preference by receiving direct referrals from the Montgomery County Department of Health and Human Services (DHHS). [Three Points]

Sixth Local Preference – HUD funded 2017/2018 Mainstream Disabled (MSD) Grant program: Preference is given for Non-Elderly Disabled (NED) families who meet at least one of the following criteria:

1. Transitioning out of institutional or other segregated settings;
2. At serious risk of institutionalization;
3. Homeless; or
4. At risk of becoming homeless.

NED is defined as disabled persons aged 18-62 and can include any member of a household. Eligibility for this preference is initially indicated based on responses to questions on HOC's wait list, which are designed to capture these criteria. Once a NED family is called up for a subsidy based on this preference, HOC staff conducts comprehensive verification of the preference qualifications, as explained in Section M of this Chapter. [Three Points]

Treatment of Single Applicants

Single applicants are treated as any other eligible family on the wait list for the tenant-based and project-based voucher wait lists.

G. INCOME TARGETTING

In accordance with the Quality Housing and Work Responsibility Act of 1998, each fiscal year HOC reserves a minimum of seventy-five (75) percent of its Section 8 new admissions for families whose incomes do not exceed thirty (30) percent of the area median income (AMI). HUD refers to these families as "extremely low-income families." HOC must admit families who qualify under the

Extremely Low-Income limit to meet the income targeting requirement, regardless of preference. This policy applies to the tenant-based and project-based voucher wait lists.

HOC's income targeting requirement does not apply to low-income families continuously assisted, as provided for under the 1937 Housing Act.

HOC is also exempted from this requirement when HOC provides assistance to low income or moderate-income families entitled to preservation assistance under the tenant-based voucher program as a result of a mortgage prepayment or opt-out.

H. INITIAL DETERMINATION OF LOCAL PREFERENCE QUALIFICATION

[24 CFR 5.415] May 2017

At the time of application, an applicant's entitlement to a local preference may be made on the following basis:

> An applicant's certification that they qualify for a preference is accepted without verification at the pre-application. When the family is selected from the wait list for the final determination of eligibility, the preference is verified. To Qualify for the preference, an applicant must provide verification that shows he or she qualified either at the time of the pre-application or at the time of certification.

If the preference verification indicates that an applicant does not qualify for the preference, the applicant is returned to the wait list (tenant-based or project-based) without the local preference, and given an opportunity for an office meeting.

I. TARGETED FUNDING [24 CFR 982.203]

When HUD awards special funding for certain family types, families who qualify are placed on the regular wait list. When a specific type of funding becomes available, the tenant-based and project-based voucher wait lists are searched for the first available family meeting the targeted funding criteria. HOC reserves the right to use this assistance under the "Interim Use" policy. [See Glossary under "Interim Use" for definition].

Applicants who are admitted under targeted funding which are not identified as a Special Admission are identified by codes in the automated system. HOC has the following "Targeted" Programs:

- Veterans Affairs Supportive Housing (VASH)
- Mainstream Allocation Plan for Persons with Disabilities
- Voucher allocation for Non-Elderly Persons with Disabilities in Support of Designated Housing Plans

For any voucher allocation for Non-Elderly Persons with Disabilities (NED) in Support of Designated Housing Plans, HOC identifies a non-elderly disabled family, as defined by HUD, on HOC's wait list that will not be housed due to an approved or submitted Designated Housing Plan.

At turnover:

Re-issuance upon turnover of vouchers in the Non-Elderly Persons with Disabilities in Support of Designated Housing Plans 2008 allocation will be to Non-Elderly Persons with Disabilities on the wait list.

5.410] **Change in Circumstances**

Changes in an applicant's circumstances while on the wait list may affect the family's entitlement to a preference. Applicants are required to update their on-line application when their circumstances of change.

Cross-Listing of Different Housing Programs and Section 8 [24 CFR 982.205(a)]

HOC maintains a consolidated master wait list for all of its housing programs. An applicant is considered for admission to any program for which they are eligible until such time that documentation is presented which establishes a customer as ineligible for a given housing program(s). If a customer is determined ineligible for the voucher program, their application is maintained on the consolidated wait list so that they may continue to be considered for other housing opportunities.

Other Housing Assistance [24 CFR 982.205(b)]

Other housing assistance means a federal, State, or local housing subsidy, as determined by HUD, including public housing.

HOC may not take any of the following actions because an applicant has applied for, received, or refused other housing: [24 CFR 982.205(b)]

. Refuse to list the applicant on the wait list for tenant-based voucher assistance;

J. PREFERENCE AND INCOME TARGETING ELIGIBILITY [24 CFR

. Deny any admission preference for which the applicant is currently qualified;

. Change the applicant's place on the wait list based on a preference, date of application, or other factors affecting selection under HOC's selection policy; or

. Remove the applicant from the wait list.

However, HOC may remove the applicant from the wait list for tenant-based assistance if HOC has offered the applicant assistance under the Project-Based Voucher program.

K. ORDER OF SELECTION [24 CFR 982.207(e)]

HOC's method for selecting applicants from a preference category leaves a clear audit trail which

can be used to verify that each applicant was selected in accordance with the method specified in the Administrative Plan. **Tenant-Based Voucher Wait List**

Local Preferences

HOC provides the following system to apply local preferences:

> Each preference receives an allocation of points. The more preference points an applicant receives, the higher the applicant's position on the wait list.

Among Applicants with Equal Preference Status

Among applicants with equal preference status, the tenant-based voucher wait list was organized by the lottery selection process for the first 365 days after the wait list was opened in the summer of 2015. Thereafter, applicants with equal preference status on the tenant-based voucher wait list are organized by date and time stamp.

Project-Based List

HOC provides the following system to apply local preferences:

Each preference receives an allocation of points. The more preference points an applicant receives, the higher the applicant's position on the wait list.

The PBV sub list is organized by family size and the corresponding bedroom size as follows:

- One and two person families are eligible for a one-bedroomunit.
- Three and four person families are eligible for a two- bedroom unit.
- Five and six person families are eligible for a three- bedroom unit.
- Seven and eight person families are eligible for a four- bedroom unit.

Exceptions to this policy are made in accordance with HOC's policies of reasonable accommodation for persons with disabilities.

The number of persons per bedroom is subject to compliance with the Montgomery County Code, Chapter 26-5, Space, Use, and Location. Paragraph (b) of Chapter 26-5 is shown below:

> b) *Floor area, sleeping.* In every dwelling unit of two or more rooms, every room occupied for sleeping purposes by one occupant must contain at least 70 square feet of habitable space, and every room occupied for sleeping purposes by more than one occupant must contain at least 50 square feet of habitable space for each occupant. However, in a mobile home every room occupied for sleeping purposes by one occupant must contain at least 50 square feet of habitable space; by 2 occupants, at least 70 square feet of habitable space; and by more than 2 occupants, at least an additional 50 square feet of habitable space for each additional

occupant.

Among Applicants with equal preference status, the PBV wait list is organized by the regular date-time selection process for each bedroom size.

L.1 PROJECT-BASED VOUCHER REFERRALS

Applicants referred to HOC for housing subsidy through PBVs by way of Offender Reentry programs sponsored by the Silver Spring Interfaith Housing Coalition and Threshold Services, Inc. are granted an eligibility criminal background exception. The participant does not have rights to the HOC Grievance Procedures.

The eligibility exception is not extended to the following individuals:

1. Persons convicted of manufacturing or producing methamphetamine;

2. Any person evicted from federally assisted housing for a serious violation of the lease (and for three years following the eviction);

3. Any person who fails to sign and submit consent forms to obtain information in accordance with the Administrative Plan Part 5, subparts B and F;

4. Any person required under HUD regulation to establish citizenship or eligible immigration status;

5. Any person subject to a life time registration requirement under a state sex offender registration program; and

6. Any persons convicted for violent felonies.

L.2 PROJECT-BASED VOUCHER REFERRALS

In an effort to minimize displacement of families, if a unit that is to be included in the PBV contract is occupied by an eligible family, the in-place family must be placed on the program wait list. When eligibility is determined, the family must be given an absolute selection preference and referred to the project owner for an appropriately size PBV contract.

A preference will be extended through the PBV program (only) for services offered. In selecting families, HOC may give a preference to disabled families who need services offered at a particular project. This preference (more specifically a referral) is limited to the population of families with disabilities that significantly interfere with their ability to obtain and maintain themselves in housing who, without appropriate supportive services, are not able to maintain themselves in housing.
Selection of applicants in the targeted funding Family Unification Program (FUP) 2008 allocation are completed in conjunction with referrals from the Montgomery County Department of Health and Human Services (MCHHS). HOC will accept families certified by the MCHHS as eligible applicants

for FUP. HOC will compare the names provided with the names on the current HOC wait list. Any referred family on the HOC wait list is served first. Those families referred and not on the HOC wait list will be added to the wait list and served based on date of referral or on a first come first served basis.

M. FINAL VERIFICATION OF PREFERENCES [24 CFR 5.415]

Preference information on pre-applications is updated as applicants are selected from the wait list. At that time, HOC will obtain necessary verifications of preference(s) at the interview and by third party verification.

Subsection A – Secondary Review/Credit Checks

Before issuing vouchers to applicant families, HOC requests a credit report of all new applicant families, all adults (persons 18 years of age and older) who will reside in the assisted household. The credit report is reviewed by HOC. Applicant households claiming they have zero income automatically undergo a credit check review. The information contained in the credit check is used to confirm the information provided to HOC by the family. Specially, the credit report is used to confirm:

1. **Employment:** A credit report will list any employers the applicant has listed in any recent credit applications. If the credit report reveals employment for any adult household member within the last 12 months that was not disclosed, the family will be asked to provide additional documentation to resolve the discrepancy. Failure to disclose current employment may result in denial of participation in the Housing Choice Voucher and Section 8 programs.

2. **Aliases:** A credit report can provide information on other names that have been used for the purposes of obtaining credit. Common reasons for use of other names include a recent marriage or a divorce. If an alias has not been disclosed to HOC, the family will be asked to provide additional evidence of the legal identity of all adult family members.

3. **Current and previous addresses:** A credit report can provide a history of where the family has lived. This is particularly important because HOC provides a residency preference. If the family has provided one address to HOC and the credit report indicates a different address, the family will be asked to provide additional proof of residency. This may include a history of utility bills, bank statements, school enrollment records for children, credit card statements, and/or other relevant documentation. Failure to provide adequate proof could result in denial of the residency preference.

   Credit card and loan payments: A credit report will usually include a list of the family's financial obligations. Examples of the items that may show up include car loans, mortgage loans, student loans, and credit cards payments. HOC will review this information to confirm the income and asset information provided by the family. If the family's current financial obligations (total amount of current monthly

2. The applicant fails to respond to an electronic or written request for information or

payments) exceed the amount of income reported by the family, HOC will ask the family to disclose how they are currently meeting their financial obligations. Accounts that have been charged off or are significantly delinquent are not included in this calculation. Failure to provide adequate proof of income could result in denial of participation in the Housing Choice Voucher and Section 8 programs.

5. **Multiple Social Security Numbers:** A credit report may list multiple Social Security numbers if an adult family member has used different Social Security numbers to obtain credit. If the credit report information does not match the information provided by an adult family member, the family member or head of household will be required to obtain written confirmation of the Social Security number that was issued to him/her from the Social Security Administration.

Applicant families are not issued vouchers until all discrepancies between the information provided by the applicant family and the information contained in the credit report have been cleared by the applicant family and approved by HOC.

When discrepancies are found, the family will be contacted by HOC. In most cases, the family will be allowed a maximum of ten (10) business days to provide the additional information. On a case-by-case basis, as a reasonable accommodation, the family may be granted additional time. If additional time is granted, the family receives written notification of the new deadline. No second or additional extensions will be granted. Failure to provide the required information to HOC could result in denial of participation in the Housing Choice Voucher and Section 8 Programs.

When the credit report reveals multiple discrepancies which require interview appointments, HOC will schedule up to two interview appointments. An additional appointment may be scheduled as a reasonable accommodation. Failure to appear at the interview session could result in denial of participation in the Housing Choice Voucher and Section 8 Programs.

N. **PREFERENCE DENIAL** [24 CFR 5.415]

If HOC denies a preference, HOC notifies the applicant in writing of the reasons why the preference was denied and offer the applicant an opportunity for an informal review to appeal the decision. If the preference denial is upheld as a result of the review, or the applicant does not request a review, the preference is removed from the applicant's entry on the wait list, returning the applicant to their regular date-time positioning. Applicants may exercise other rights if they believe they are a victim of discrimination.

If the applicant falsifies documents or makes false statements in order to qualify for any preference, they will be removed from the wait list.

O. **REMOVAL FROM THE WAIT LIST AND PURGING** [24 CFR 982.204(c)]

HOC will not remove an applicant's name from the wait list unless:

1. The applicant requests in writing that their name be removed; a request to declare their continued interest in the program; or

3. The applicant does not meet either the eligibility or suitability criteria for the program.

4. The applicant refuses two housing units without good cause.

Obligation to Annually Confirm Application Information

Each year, or at such time as HOC determines reasonable, HOC will issue notice to all applicants on the wait list requesting that each applicant confirm their continued interest in remaining on the wait list. Failure to renew the information in a timely manner will result in removal from the wait list.

HOC will provide notice to wait list applicants to confirm their continued interest and set a date by which their renewal must be completed. HOC will send notices thirty days, fifteen days, five days, and one day prior to the date when that renewal or confirmation is due.

All notices under this Section are sent by HOC electronically to the last known e-mail address listed on the application. Wait list applicants may also request text message notifications. If a family does not have an e-mail address, HOC can assist the family in obtaining a free email account. It will be the applicant's sole responsibility to check that email account from time to time and to respond to any email and/or SMS text from HOC. To the extent an applicant requires assistance, upon request, staff from HOC is available to assist with electronic submissions.

Should an applicant not respond to the request to confirm their continued interest in remaining on the wait list by renewing their application or to their notification of selection for a program for any reason, prior to the established deadline, the applicant is removed from the wait list. Reasons for non-response, resulting in removal from the list, include (but are not limited to) negligence in completing the electronic update/application in a timely manner and relocation resulting in a return of the e-notice to HOC with no forwarding email address provided. Applicants removed from the wait list will receive a notification identifying their removal from Housing Path.

Missed Appointments

All applicants who fail to keep a scheduled appointment with HOC are sent a written notice of termination of the process for eligibility. That written notification of termination may be sent as an attachment to an e-mail.

HOC will allow the family to reschedule an appointment for good cause. Generally, no more than one opportunity is given to reschedule without good cause, and no more than two opportunities are given for good cause. When good cause exists for missing an appointment, HOC will work closely with the family to find a more suitable time. Applicants are advised of their right to an informal review before being removed from the wait list.

Notification of Negative Actions

Any applicant whose name is being removed from the wait list will be notified by HOC, in writing, that they have ten (10) calendar days from the date of the written correspondence to present mitigating circumstances or request an informal review. The letter will also indicate that their name will be removed from the wait list if they fail to respond within the timeframe specified. HOC's system of removing applicant names from the wait list will not violate the rights of persons with disabilities. If an applicant claims that their failure to respond to a request for information or updates was caused by a disability, HOC will verify that there is in fact a disability, that the disability is what caused the failure to respond, and then provide a reasonable accommodation. An example of a reasonable accommodation would be to reinstate the applicant on the wait list based on the date and time of their original application.

Purging the Wait List

HOC will update and purge its wait list as needed to ensure that the pool of applicants reasonably represents the interested families for whom HOC has current information, i.e. applicant's address, family composition, income category, and preference.

EXHIBIT B

Chapter 7

VERIFICATION PROCEDURES

[24 CFR Part 5, Subparts B, D, E and F; 982.108]

INTRODUCTION

HUD regulations require that the factors of eligibility and Total Tenant Payment/Family Share be verified by the PHA. PHA staff will obtain written verification from independent sources whenever possible, or will document in tenant files why third party verification was impossible to obtain.

Applicants and program participants must provide true and complete information to the PHA whenever information is requested. The PHA's verification requirements are designed to maintain program integrity. This Chapter explains the PHA's procedures and standards for verification of preferences, income, assets, allowable deductions, family status, and changes in family composition. The PHA will obtain proper authorization from the family before requesting information from independent sources.

A. METHODS OF VERIFICATION AND TIME ALLOWED [24 CFR 982.516]

The PHA will verify information through the five methods of verification acceptable to HUD in the following order:

1. Upfront Income Verification through HUD's Enterprise Income Verification system, see HOC's EIV policy
2. Third-Party Written Verification
3. Third-Party Oral Verification
4. Review of Documents
5. Certification/Self-Declaration

The PHA will verify information through a secondary review through third party credit reports.

The PHA will allow 14 days for return of third-party verifications and 14 days to obtain other types of verifications before going to the next method. The PHA will document the file as to why third party written verification was not used.

For applicants, verifications may not be more than 60 days old at the time of voucher issuance. For participants, they are valid for 60 days from date of receipt.

Upfront Income Verification (W-UIV)

The verification of income, before or during a family re-examination, through an independent source that systemically and uniformly maintains income information in a computerized form for a large number of individuals.

The UIV data is used to validate client reported income and supplement client provided documents. When the client disputes the UIV data, the PHA must request written third party verification.

Acceptable Verification:

UIV plus current client provided documents or

UIV plus current client provided documents plus written third-party verification

Tenant-provided documents should be dated within the last 120 days of the reexamination, pay stubs should be current and consecutive.

The PHA will use state or federal records of child support payments to document and calculate income

Projecting Annual Income through UIV:

When UIV data is not substantially different than client-reported income:

If UIV data is less than client reported income, use client provided documents to calculate anticipated annual income.

If UIV data is greater than client reported income, use UIV data to calculate anticipated annual income, unless client can provide the PHA with acceptable documentation to verify a change in circumstances.

When UIV data is substantially different than client reported income:

The PHA must request written third-party verification from the discrepant income source.

Third-Party Written Verification

Third-party verification is used to verify information directly with the source. Third-party written verification forms will be sent and returned via first class mail. The family will be required to sign an authorization for the information source to release the specified information.

Verifications received electronically directly from the source are considered third party written verifications.

Third-Party Oral Verification

Oral third-party verification will be used when written third party verification is delayed or not possible. When third-party oral verification is used, staff will be required to complete a Certification of Document Viewed or Person Contacted form, noting with whom they spoke, the

date of the conversation, and the facts provided. If oral third party verification is not available, the PHA will compare the information to any documents provided by the Family. If provided by telephone, the PHA must originate the call.

Review of Documents

In the event that third-party written or oral verification is unavailable, or the information has not been verified by the third party within two weeks, the PHA will annotate the file accordingly and utilize documents provided by the family as the primary source if the documents provide complete information.

All such documents, excluding government checks, will be photocopied and retained in the applicant file. In cases where documents are viewed which cannot be photocopied, staff viewing the document(s) will complete a Certification of Document Viewed or Person Contacted form or document.

The PHA will accept the following documents from the family provided that the document is such that tampering would be easily noted:

- Printed wage stubs
- Computer print-outs from the employer
- Signed letters (provided that the information is confirmed by phone)
- Other documents noted in this Chapter as acceptable verification

The PHA will accept photocopies after review of the original documents.

If third-party verification is received after documents have been accepted as provisional verification, and there is a discrepancy, the PHA will utilize the third party verification.

The PHA will not delay the processing of an application beyond 14 days because a third party information provider does not return the verification in a timely manner.

Self-Certification/Self-Declaration

When verification cannot be made by third-party verification or review of documents, families will be required to complete a self-certification.

Subsection – Secondary Review/Credit Checks

The Housing Authority uses credit reports obtained from a third party source as a secondary review of income verifications for all adult household members (non student persons 18 years of age and older) who reside in the assisted household and claim zero income. The secondary review includes a comparison between the information contained in the credit report, for each adult household member and the information provided by the family to the Housing Authority for eligibility purposes (Personal Declaration). Specifically, the Housing Authority reviews the credit report to verify:

Employment: If the credit report reveals employment during the subsidized period that has not been disclosed to the Housing Authority, the family will be required to provide documentation that the employment did not occur or provide information regarding the amount of earnings received during the employment period. If a family contends that the employment was made up for the purposes of obtaining credit or was erroneously placed on the credit report, the family must supply a letter from the employers listed confirming such information. If the family failed to disclose employment for a period longer than six months, the Housing Authority may purpose termination of the family's housing assistance and seek repayment of any overpayment. If the family failed to disclose employment for less than six months, the family will be required to attend a counseling interview and re-sign all program documents reinforcing the family's obligations. The family will also be required to repay any housing subsidy overpayment. A recurrence of this violation could result in termination from the Housing Choice Voucher and Section 8 programs.

Assets: The credit report information will be used to verify assets, particularly large items such as real property. If the credit report reveals that the family owns property, the family will berequired to provide the appropriate documentation regarding the property. If all documentation confirms that the family or any household member owns real estate property that was purposely concealed, the Housing Authority will propose termination of assistance and seek repayment of any overpayment amount.

Aliases: A credit report can provide information on other names that have been used for the purposes of obtaining credit. Common reasons for use of other names include a recent marriage or a divorce. If an alias has not been disclosed to the Housing Authority, the family will be asked to provide additional evidence of the legal identity of all adult family members.

Current and previous addresses: A credit report can provide a history of where the family has lived. This is particularly important because the Housing Authority provides a residency preference. If the family has provided one address to the Housing Authority and the credit report indicates a different address, the family will be asked to provide additional proof of residency. This may include a history of utility bills, bank statements, and school enrollment records for children, credit card statements or other relevant documentation. Failure to provide adequate proof could result in denial of the residency preference.

Credit card and loan payments: A credit report will usually include a list of the family's financial obligations. Examples of the items that may show up include car loans, mortgage loans, student loans and credit cards payments. The Housing Authority will review this information to confirm the income and asset information provided by the family. If the family's current financial obligations (total amount of current monthly payments) exceed the amount of income reported by the family, the Housing Authority will ask the family to disclose how they are currently meeting their financial obligations. Accounts that have been charged off or are significantly delinquent are not included in this calculation. Failure to provide adequate proof of income could result in denial of participation in the Housing Choice Voucher and Section 8 programs.

Multiple Social Security Numbers: A credit report may list multiple Social Security numbers if an adult family member has used different Social Security numbers to obtain credit. If the credit report information does not match the information provided by an adult family member, the family member or head of household will be required to obtain written confirmation of the Social Security

number that was issued to him/her from the Social Security Administration.
A family will not be issued a voucher until all discrepancies between the information provided by the applicant family and the information contained in the credit report have been cleared by the applicant family and approved by the Housing Authority. When discrepancies are found, the family will be contacted by the Housing Authority. In most cases, the family will be allowed a maximum of ten business days to provide the additional information. On a case-by-case basis, as a reasonable accommodation, the family may be granted additional time. If additional time is granted, the family receives written notification of the new deadline. No second or additional extension will be granted. Failure to provide the required information to the Housing Authority could result in denial of participation in the Housing Choice Voucher and Section 8 Programs. When the credit report reveals multiple discrepancies which require interview appointments, the Housing Authority will schedule up to two interview appointments. An additional appointment may be scheduled as a reasonable accommodation. Failure to appear at the interview session could result in denial of participation in the Housing Choice Voucher and Section 8 Programs.

B. RELEASE OF INFORMATION [24 CFR 5.230]

Adult family members will be required to sign the HUD 9886 Release of Information/Privacy Act form.

In addition, family members will be required to sign specific authorization forms when information is needed that is not covered by the HUD form 9886, Authorization for Release of Information/Privacy Act Notice.

Each member requested to consent to the release of specific information will be provided with a copy of the appropriate forms for their review and signature.

Family refusal to cooperate with the HUD prescribed verification system will result in denial of admission or termination of assistance because it is a family obligation to supply any information and to sign consent forms requested by the PHA or HUD.

C. COMPUTER MATCHING

Where allowed by HUD and/or other State or local agencies, computer matching will be done.

The PHA will utilize the HUD established Enterprise Income Verification (EIV)/Upfront Income Verification (UIV) tool for obtaining Social Security benefits, Supplemental Security Income, benefit history and tenant income discrepancy reports from the Social Security Administration (Refer to EIV policy).

A. INITIAL LEASE UP [24 CFR 5.233]

For each New Admission (form HUD-50058 action type 1) Income Report

- PHAs must review the Income Report to confirm/validate family-reported income within 90 days of the admission date.

- Any income discrepancies must be resolved with the family within 30 days of the Income Report date

For each Historical Adjustment (form HUD-50058 action type 14) Income Report

- PHAs must review the Income Report to confirm/validate family-reported income within 90 days of the PIC submission date

- Any income discrepancies must be resolved with the family within 30 days of the Income Report date

When computer matching results in a discrepancy with information in the PHA records, the PHA will follow up with the family and verification sources to resolve this discrepancy. If the family has unreported or underreported income, the PHA will follow the procedures in the Program Integrity Addendum of the Administrative Plan.

D. ITEMS TO BE VERIFIED [24 CFR 982.516]

All income not specifically excluded by the regulations.

Full-time student status including High School students who are 18 or over.

Current assets including assets disposed of for less than fair market value in preceding two years.

Child-care expense where it allows an adult family member to be employed or to further his/her education.

Total medical expenses of all family members in households whose head or spouse is elderly or disabled.

Disability assistance expenses to include only those costs associated with attendant care or auxiliary apparatus for a disabled member of the family, which allow an adult family member to be employed.

Disability for determination of preferences, allowances or deductions.

U.S. citizenship/eligible immigrant status.

"Preference" status.

Familial/Marital status when needed for head or spouse definition.

Verification of Reduction in Benefits for Noncompliance:

The PHA will obtain written verification from the welfare agency stating that the family's benefits have been reduced for fraud or noncompliance before denying the family's request for rent reduction.

E. VERIFICATION OF INCOME [24 CFR 982.516]

This section defines the methods the PHA will use to verify various types of income.

Employment Income

Verification forms request the employer to specify the:

Dates of employment

Amount and frequency of pay

Date of the last pay increase

Likelihood of change of employment status and effective date of any known salary increase during the next 12 months

Year to date earnings

Estimated income from overtime, tips, bonus pay expected during next 12

months. Acceptable methods of verification include, in this order:

1. Employment verification form completed by the employer.
2. Four current consecutive pay stubs or earning statements, which indicate the employee's gross pay, frequency of pay or year to date earnings.
3. W-2 forms plus income tax return forms.

Self-certification or income tax returns signed by the family may be used for verifying self- employment income, or income from tips and other gratuities.

Employment verification must reflect a home base in Montgomery county or 51 percent of business is conducted within Montgomery county.

Applicants claiming self-employment income must provide documentation that 51 percent of the business is conducted within Montgomery county.

Applicants and program participants may be requested to sign an authorization for release of information from the Internal Revenue Service for further verification of income.

In cases where there are questions about the validity of information provided by the family, the PHA will require the most recent federal income tax statements.

Where doubt regarding income exists, a referral to IRS for confirmation will be made on a case-by-case basis.

Social Security, Pensions, Supplementary Security Income (SSI), Disability Income

Acceptable methods of verification include, in this order:

1. Utilize the HUD established Enterprise Income Verification (EIV)/Upfront Income

Verification (UIV) tool for benefits, benefit history and tenant income discrepancy reports from the Social Security Administration (Refer to EIV policy).

2. Benefit verification form completed by agency providing the benefits.

3. Award or benefit notification letters prepared and signed by the providing agency.

4. Computer report electronically obtained or in hard copy.

Unemployment Compensation

Acceptable methods of verification include, in this order:

1. Utilize the HUD established Enterprise Income Verification (EIV)/Upfront Income Verification (UIV) tool for benefits and benefit history reports from the Unemployment Compensation agency.

2. Verification form completed by the unemployment compensation agency.

3. Computer report electronically obtained or in hard copy, from unemployment office stating payment dates and amounts.

4. Payment stubs.

Welfare Payments or General Assistance

Acceptable methods of verification include, in this order:

1. PHA verification form completed by payment provider.

2. Written statement from payment provider indicating the amount of grant/payment, start date of payments, and anticipated changes in payment in the next 12 months.
3. Computer-generated Notice of Action.

4. Computer-generated list of recipients from Welfare Department.

Alimony or Child Support Payments

Acceptable methods of verification include, in this order:

1. Copy of a separation or settlement agreement or a divorce decree stating amounts and types of support and payment schedules.

2. State or federal records of child support payments.

3. A notarized statement or affidavit signed by the person providing the support. This document must include amount of support, payor name, address, and phone number

4. Copy of 3 latest check and/or payment stubs from Child Support Enforcement. For verbal third party the PHA must record the date, amount, and number of the check.

5. Family's self-certification of amount received and of the likelihood of support payments being received in the future, or that support payments are not being received.

If payments are irregular, the family must provide:

A copy of the separation or settlement agreement, or a divorce decree stating the amount and type of support and payment schedules.

A statement from the agency responsible for enforcing payments to show that the family has filed for enforcement.

A notarized affidavit from the family indicating the amount(s) received.

A welfare notice of action showing amounts received by the welfare agency for child support.

A written statement from an attorney certifying that a collection or enforcement action has been filed.

Net Income from a Business

In order to verify the net income from a business, the PHA will view IRS and financial documents from prior years and use this information to anticipate the income for the next 12 months.

Acceptable methods of verification include:

1. IRS Form 1040, including:
   Schedule C (Small Business)

   Schedule E (Rental Property Income)

   Schedule F (Farm Income)

2. If accelerated depreciation was used on the tax return or financial statement, an accountant's calculation of depreciation expense computed using straight-line depreciation rules.

3. Audited or un-audited financial statement(s) of the business.

4. Credit report or loan application.

5. Documents such as manifests, appointment books, cashbooks, bank statements, and receipts will be used as a guide for the prior 180 days (or lesser period if not in business for 90 days) to project income for the next 12 months. The family will be advised to maintain these documents in the future if they are not available.

6. Family's self-certification as to net income realized from the business during previous years.

Child Care Business

If an applicant/participant is operating a licensed day care business, income will be verified as with any other business.

If the applicant/participant is operating a "cash and carry" operation (which may or may not be licensed), the PHA will require that the applicant/participant complete a form for each customer which indicates: name of person(s) whose child (children) is/are being cared for, phone number, number of hours child is being cared for, method of payment (check/cash), amount paid, and signature of person.

If the family has filed a tax return, the family will be required to provide it.

The PHA will conduct interim reevaluations every year and require the participant to provide a log with the information about customers and income.

If childcare services were terminated, third-party verification will be sent to the parent whose child was cared for.

Recurring Gifts

Acceptable methods of verification include, in this order:

- A notarized statement or affidavit signed by the person providing the assistance giving the purpose, date and value of gifts. This document should include the payor name, address and phone number.
- A self-certification provided by the family that contains the following information: The person who provides the gift, the value of the gifts, the dates of the gifts and the purpose of the gifts.

Zero Income Status

Families claiming to have no income will be required to execute verification forms to determine that forms of income such as unemployment benefits, TANF, SSI, etc. are not being received by the household.

The PHA will request information from the State Employment Development Department.

The PHA will run a credit report if information is received that indicates the family has an unreported income source.

Full-time Student Status

Only the first $480 of the earned income of full time students, other than head, co-head, or spouse, will be counted towards family income.

Financial aid, scholarships and grants received by full time students is not counted towards family income.

Verification of full time student status includes:

Written verification from the registrar's office or other school official; or school records which show a sufficient number of credits to be considered a full-time student by the educational institution attended.

School records, such as an official report card, indicating enrollment for sufficient number of credits to be considered a full-time student by the educational institution.

F. **INCOME FROM ASSETS** [24 CFR 982.516]

*VERIFICATION OF ASSESTS

Asset Accounts with Interest Income and Dividends with current balance exceeding $1,000

Acceptable methods of verification include, in this order:

1. Verification forms from a financial institution or broker.

2. Passbook, account statements, certificate of deposit, bonds, or financial statements completed by a financial institution or broker including current interest rates and dividends.

3. Broker's statements showing value of stocks or bonds and the earnings credited the family. Earnings can be obtained by oral broker's verification or current newspaper quotations.
4. IRS Form 1099 from the financial institution provided that the PHA must adjust the information to project earnings expected for the next 12 months.

Interest Income from Mortgages or Similar Arrangements

Acceptable methods of verification include, in this order:

1. Amortization schedule showing interest for the 12 months following the effective date of the certification or recertification.

2. A letter from an accountant, attorney, real estate broker, the buyer, or financial institution stating interest due for the next 12 months. (A copy of the check paid by the buyer to the family is not sufficient unless of a breakdown of interest ispresent.

Net Rental Income from Property Owned by Family

Acceptable methods of verification include, in this order:

1. IRS Form 1040 with Schedule E (Rental Income)

2. A copy of latest rent receipts, leases, or other documentation of rent amounts.

3. Documentation of allowable operating expenses of the property: tax statements, insurance invoices, bills for reasonable maintenance and utilities, and bankstatements or amortization schedules showing monthly interest expense.

4. Lessee's written statement verifying rent payments to the family and family's self-certification as to the net income realized.

Verification for assets to determine the current cash value

(the net amount the family would receive if the assets were converted to cash).

Quotes from a stock broker or realty agent as to the net amount family would receive if they liquidated securities or real estate.

Real estate tax statements if the approximate current cash value can be deduced from the assessment.

Financial statements from business assets

Copies of closing documents showing the selling price and the distribution of the sales proceeds.

Appraisals of personal property held as an investment.

Family's self certification describing assets or cash held at the family's home or in a safe deposit boxes.
Assets Disposed of for Less than Fair Market Value (FMV) During the Two Years Preceding the Effective Date of Certification or Recertification

For all Certifications and Recertifications, the PHA will obtain the Family's certification as to whether any member has disposed of assets for less than fair market value during the two years preceding the effective date of the certification or recertification.

If the family certifies that they have disposed of assets for less than fair market value, verification if required that shows: (a) all assets disposed of for less than FMV, (b) the date they were disposed of, (c) the amount the family received, and (d) the market value of the assets at the time of disposition. Third party verification will be obtained whenever possible.

H. VERIFICATION OF ALLOWABLE DEDUCTIONS FROM INCOME

[24 CFR 982.516]

Child Care Expenses

Written verification from the person who receives the payments is required. If the child care provider is an individual, s/he must provide a statement of the amount they are charging the family for their services. Additionally, the family must provide two months of cancelled checks or cancelled cashier money orders verifying the child care costs.

Verifications must specify the child care provider's name, address, telephone number, Social Security Number, the names of the children cared for, the number of hours the child care occurs, the rate of pay, and the typical yearly amount paid, including school and vacation periods.

Family's certification as to whether any of those payments have been or will be paid or reimbursed by outside sources.

Medical Expenses

Families, who claim medical expenses will be required to submit a certification as to whether or not any expense payments have been, or will be, reimbursed by an outside source. All expense claims will be verified by one or more of the methods listed below:

Written verification by a doctor, hospital or clinic personnel, dentist, pharmacist, of (a) the anticipated medical costs to be incurred by the family and regular payments due on medical bills; and (b) extent to which those expenses will be reimbursed by insurance or a government agency.

Written confirmation by the insurance company or employer of health insurance premiums to be paid by the family.

Written confirmation from the Social Security Administration of Medicare premiums to be paid by the family over the next 12 months. A computer printout will be accepted.

For attendant care:

A reliable, knowledgeable professional's certification that the assistance of an attendant is necessary as a medical expense and a projection of the number of hours the care is needed for calculation purposes.

Attendant's written confirmation of hours of care provided and amount and frequency of payments received from the family or agency (or copies of canceled checks the family used to make those payments) or stubs from the agency providing the services.

Receipts, canceled checks, or pay stubs that verify medical costs and insurance expenses likely to be incurred in the next 12 months.

Copies of payment agreements or most recent invoice that verify payments made on outstanding medical bills that will continue over all or part of the next 12 months.

Receipts or other record of medical expenses incurred during the past 12 months that can

be used to anticipate future medical expenses, which includes regular visits to doctors or dentists, for "general medical expenses". For non-prescription drugs verification is needed from a medical professional stating that these drugs are prescribed is also needed along with receipts. One time, nonrecurring expenses from the previous year will not be included.

The PHA will use mileage at the IRS rate, or cab, bus fare, or other public transportation cost for verification of the cost of transportation directly related to medical treatment.

Assistance to Persons with Disabilities [24 CFR 5.611(c)] In All Cases:

Written certification from a reliable, knowledgeable professional that the person with disabilities requires the services of an attendant and/or the use of auxiliary apparatus to permit him/her to be employed or to function sufficiently independently to enable another family member to be employed.

Family's certification as to whether they receive reimbursement for any of the expenses of disability assistance and the amount of any reimbursement received.

Attendant Care:

Attendant's written certification of amount received from the family, frequency of receipt, and hours of care provided.

Certification of family and attendant and/or copies of canceled checks family used to make payments.

Auxiliary Apparatus:

Receipts for purchases or proof of monthly payments and maintenance expenses for auxiliary apparatus.
In the case where the person with disabilities is employed, a statement from the employer that the auxiliary apparatus is necessary for employment.

I. VERIFYING NON-FINANCIAL FACTORS [24 CFR 982.153(b)(15)]

Verification of Legal Identity

In order to prevent program abuse, the PHA will require applicants to furnish verification of legal identity for all family members.

The documents listed below will be considered acceptable verification of legal identity for adults. If a document submitted by a family is illegible or otherwise questionable, more than one of these documents may be required.

Certificate of Birth, naturalization papers.

- Church issued baptismal certificate
- Current, valid Driver's license
- U.S. military discharge (DD 214)

□ U.S. passport

□ Department of Motor Vehicles Identification Card

□ Hospital records

Documents considered acceptable for the verification of legal identity for minors may be one or more of the following:

□ Certificate of Birth

□ Adoption papers

□ Custody agreement

□ Health and Human Services ID

□ School records

Verification of Marital Status

Verification of divorce status will be a certified copy of the divorce decree, signed by a Court Officer.

Verification of a separation may be a copy of court-ordered maintenance or other records.

Verification of marriage status is a marriage certificate.

Familial Relationships (pages 7-16 and 7-17)

Certification will normally be considered sufficient verification of family relationships. In cases where reasonable doubt exists, the family may be asked to provide verification.

The following verifications will always be required if applicable:

□ Verification of relationship:

- □ Official identification showing names
- □ Birth Certificates
- □ Baptismal certificates
- □ Verification of guardianship is:
  - Court-ordered assignment
  - Verification from social services agency

Verification of Permanent Absence of Family Member

If an adult member who was formerly a member of the household is reported permanently absent by the family, the PHA will consider any of the following as verification:

Husband or wife institutes divorce action.

Husband or wife institutes legal separation.

Order of protection/restraining order obtained by one family member against another.

Proof of another home address, such as utility bills, canceled checks for rent, driver's license, or lease or rental agreement, if available.

Statements from other agencies such as social services or a written statement from the landlord or manager that the adult family member is no longer living at that location.

If the adult family member is incarcerated, a document from the Court or correctional facility should be obtained stating how long they will be incarcerated.

Verification of Change in Family Composition

The PHA may verify changes in family composition (either reported or unreported) through letters, telephone calls, utility records, inspections, landlords, credit data, school, employment, or DMV records, and other sources. In cases of domestic violence, stalking, or dating violence, HOC will accept a final order of protection, peace order, or similar court order to remove a household member.

If the family is unable to obtain the above documentation, HOC will accept documentation from the U.S. Postal Service that indicates that the removed household member does not receive mail at the program unit address and a notarized statement from the head of household, the former member or both.

Verification of Disability

Verification of disability must be receipt of SSI or SSA disability payments under Section 223 of

the Social Security Act or 102(7) of the Developmental Disabilities Assistance and Bill of Rights Act (42 U.S.C. 6001(7) or for those who do not receive disability benefits the disability can be verified by appropriate diagnostician such as physician, psychiatrist, psychologist, therapist, rehab specialist, or licensed social worker, using the HUD language as the verification format.

Verification of Citizenship/Eligible Immigrant Status [24 CFR 5.508, 5.510, 5.512, 5.514]

To be eligible for assistance, individuals must be U.S. citizens or eligible immigrants. Individuals who are neither may elect not to contest their status. Eligible immigrants must fall into one of the categories specified by the regulations and must have their status verified by Immigration and Naturalization Service (INS). Family members must declare their status once. Assistance cannot be delayed, denied, or terminated while verification of status is pending except that assistance to applicants may be delayed while the PHA hearing is pending.

Citizens or Nationals of the United States are required to sign a declaration under penalty of perjury.

The PHA will require citizens to provide documentation of citizenship. Acceptable documentation will include at least one of the following original documents:

United States birth certificate

United States passport

Resident alien/registration card

Other appropriate documentation as determined by the PHA

Eligible Immigrants who were Participants and 62 or over on June 19, 1995, are required to sign a declaration of eligible immigration status and provide proof of age.

Non-citizens with eligible immigration status must sign a declaration of status and verification consent form and provide their original immigration documents which are copied front and back and returned to the family. The PHA verifies the status through the INS SAVE system. If this primary verification fails to verify status, the PHA must request within 10 days that the INS conduct a manual search.

Ineligible family members who do not claim to be citizens or eligible immigrants must be listed on a statement of ineligible family members signed by the head of household or spouse.

Non-citizen students on student visas are ineligible members even though they are in the country lawfully. They must provide their student visa but their status will not be verified and they do not sign a declaration but are listed on the statement of ineligible members.

Failure to Provide: If an applicant or participant family member fails to sign required declarations and consent forms or provide documents as required, they must be listed as an ineligible member. If the entire family fails to provide and sign as required, the family may be denied or terminated for failure to provide required information.

Time of Verification

For applicants, verification of U.S. citizenship/eligible immigrant status occurs at the same time as verification of other factors of eligibility for final eligibility determination.

The PHA will not provide assistance to any family prior to the affirmative establishment and verification of the eligibility of the individual or at least one member of the family.

The PHA will verify the U.S. citizenship/eligible immigration status of all participants no later than the date of the family's first annual reexamination following the enactment of the Quality Housing and Work Responsibility Act of 1998.

For family members added after other members have been verified, the verification occurs at the first recertification after the new member moves in.

Once verification has been completed for any covered program, it need not be repeated except that, in the case of port-in families, if the initial PHA does not supply the documents, the PHA must conduct the determination.

Extensions of Time to Provide Documents

The PHA will grant an extension of 30 days for families to submit evidence of eligible immigrant status.

Acceptable Documents of Eligible Immigration

The regulations stipulate that only the following documents are acceptable unless changes are published in the Federal Register:

Resident Alien Card (I-551)

Alien Registration Receipt Card (I-151)

Arrival-Departure Record (I-94)

Temporary Resident Card (I-688)

Employment Authorization Card (I-688B)

Receipt issued by the INS for issuance of replacement of any of the above documents that shows individual's entitlement has been verified

A birth certificate is not acceptable verification of status. All documents in connection with U.S. citizenship/eligible immigrant status must be kept 5 years.

The PHA will verify the eligibility of a family member at any time such eligibility is in question, without regard to the position of the family on the waiting list.

If the PHA determines that a family member has knowingly permitted another individual who is not eligible for assistance to reside permanently in the family's unit, the family's assistance will be terminated for 36 months, unless the ineligible individual has already been considered in prorating the family's assistance.

Verification of Social Security Numbers [24 CFR 5.216]

Social security numbers must be provided as a condition of eligibility for all family members if they have been issued a number, except any member who is older than 62 as of Jan 31, 2010 and receiving assistance as of that date.

At the time any change in family composition is reported to HOC, each new family member will be required to produce a Social Security card or original document issued by a federal or state government agency that provides the Social Security Number of the individual along with other identifying information. HOC will accept HUD prescribed documentation of this information.

If an applicant or participant is able to disclose the Social Security Number but cannot meet the documentation requirements, the applicant or participant cannot become a participant or continue as a participant until the applicant or participant can provide the complete and accurate Social Security Number assigned to each member of the household.

HOC permits a 90-day period during which an applicant family may become a program participant, even if the family lacks the documentation necessary to verify the Social Security Number (SSN) of a family member under the age of six (6) years old. An extension of one additional 90-day period must be granted if HOC determines that, in its discretion, the applicant's failure to comply was due to circumstances that could not reasonably have been foreseen and were outside of the control of the applicant. For example, an applicant may be able to demonstrate timely submission of a request for a Social Security Number, in which case processing time would be the cause of the delay. If the applicant family does not produce the required documentation within the authorized time period, HOC must impose appropriate penalties, in accordance with the Code of Federal Regulations at 24 CFR 5.218.

If merited, HOC will offer a grace period and/or an extension. HOC will implement this provision just as it currently implements the provision for program participants. Specifically, an applicant family with a child under the age of six (6) years may become a participant family, even if the Social Security Number for the child has not been verified at the time of admission. If the Social Security Number has still not been verified at the end of the initial 90-day period, then HOC must determine whether a 90-day extension is merited. If it is not merited, then HOC must follow the provisions of 24 CFR 5.218. If a 90-day extension is merited, then HOC must either verify the Social Security Number for the child by the end of the 90-day extension period or follow the provisions of 24 CFR 5.218.

Failure to provide the required documentation during the recertification process will result in an incomplete recertification action and may subject the family to termination of housing assistance.

Medical Need for Larger Unit

A written certification that a larger unit is necessary must be obtained from a reliable, knowledgeable professional, such as a doctor, social worker, or caseworker.

EXHIBIT C

Chapter 8

VOUCHER ISSUANCE AND BRIEFINGS

[24 CFR 982.301, 982.302]

INTRODUCTION

The PHA's goals and objectives are designed to assure that families selected to participate are equipped with the tools necessary to locate an acceptable housing unit. Families are provided sufficient knowledge and information regarding the program and how to achieve maximum benefit while complying with program requirements. When eligibility has been determined, the PHA will conduct a mandatory briefing to ensure that families know how the program works. The briefing will provide a broad description of owner and family responsibilities, PHA procedures, and how to lease a unit. The family will also receive a briefing packet that provides more detailed information about the program including the benefits of moving outside areas of poverty and minority concentration. This Chapter describes how briefings will be conducted, the information that will be provided to families, and the policies for how changes in the family composition will be handled.

A. ISSUANCE OF VOUCHERS [24 CFR 982.204(d), 982.54(d)(2)]

When funding is available, the PHA will issue Vouchers to applicants whose eligibility has been determined. The number of Vouchers issued must ensure that the PHA stays as close as possible to 100 percent lease-up. The PHA performs a monthly calculation electronically to determine whether applications can be processed, the number of Vouchers that can be issued, and to what extent the PHA can over-issue (issue more Vouchers than the budget allows to achieve lease-up).

The PHA may over-issue Vouchers only to the extent necessary to meet leasing goals. All Vouchers that are over-issued must be honored. If the PHA finds it is over-leased, it must adjust future issuance of Vouchers in order not to exceed the ACC budget limitations over the fiscal year.

B. BRIEFING TYPES AND REQUIRED ATTENDANCE [24 CFR 982.301]

Initial Applicant Briefing

Briefings will be conducted in English.

The purpose of the briefing is to explain how the program works and the documents in the Voucher holder's packet to families so that they are fully informed about the program. This will enable them to utilize the program to their advantage, and it will prepare them to discuss it with potential owners and property managers.

The PHA will not issue a Voucher to a family unless the household representative has attended a briefing and signed the Voucher. Applicants who provide prior notice of inability to attend a briefing will automatically be scheduled for the next briefing. Applicants who fail to attend 2 scheduled briefings, without prior notification and approval of the PHA, may be denied admission based on failure to supply information needed for certification. The PHA will conduct individual briefings for families with disabilities at their home, upon request by the family, if required for reasonable accommodation.

Briefing Packet [24 CFR 982.301(b)]

The documents and information provided in the briefing packet for the voucher program will comply with all HUD requirements. The PHA also includes other information and/or materials that are not required by HUD**.** This information will be provided at the applicant's Initial and the participant's Move Briefing.

The family is provided with the following information and materials

The term of the voucher, and the PHA policy for requesting extensions or suspensions of the voucher (referred to as tolling).

A description of the method used to calculate the housing assistance payment for a family, including how the PHA determines the payment standard for a family; how the PHA determines total tenant payment for a family and information on the payment standard and utility allowance schedule. How the PHA determines the maximum allowable rent for an assisted unit.

For a family that qualifies to lease a unit outside the PHA jurisdiction under portability procedures, the information must include an explanation of how portability works.

The HUD required tenancy addendum, which must be included in the lease.

The Request for Approval of Tenancy form, and a description of the procedure for requesting approval for a unit.

A statement of the PHA policy on providing information about families to prospective owners.

The PHA Subsidy Standards including when and how exceptions are made and how the voucher size relates to the unit size selected.

The HUD brochure on how to select a unit and/or the HUD brochure "A Good Place to Live" on how to select a unit that complies with HQS.

The HUD brochure on lead-based paint and information about where blood level testing is available.

Information on Federal, State and local equal opportunity laws and a copy of the housing discrimination complaint form. The PHA will also include the pamphlet "Fair Housing: It's Your Right" and other information about fair housing laws and guidelines, and the telephone numbers of the local fair housing agency and the HUD enforcement office.

A list of units available for the Section 8 program which is updated monthly and compiled by bedroom size.

If the family includes a person with disabilities, notice that the PHA will provide assistance in locating accessible units.

The Family Obligations under the program.

The grounds on which the PHA may terminate assistance for a participant family because of family action or failure to act.

PHA informal hearing procedures including when the PHA is required to offer a participant family the opportunity for an informal hearing, and how to request the hearing.

Information packet including an explanation of how portability works, including a list of neighboring housing agencies with the name, address and telephone number of a portability contact person at each for use by families who move under portability. (required for PHAs in MSAs)

A family participating in the project-based voucher program will be offered available tenant-based assistance either under the voucher program or under another comparable form of tenant-based assistance as defined by HUD

Information regarding the PHA's outreach program that assists families who are interested in, or experiencing difficulty in obtaining available housing units in areas outside of minority concentrated locations.

The HQS checklist.

Procedures for notifying the PHA and/or HUD of program abuses such as side payments, extra charges, violations of tenant rights, and owner failure to repair.

The family's rights as a tenant and a program participant.

Requirements for reporting changes between annual recertifications.

Information on security deposits and legal referral services.

Exercising choice in residency

Choosing a unit carefully and only after due consideration.

The Family Self-Sufficiency program and its advantages.

If the family includes a person with disabilities, the PHA will ensure compliance with CFR 8.6 to ensure effective communication.

Move Briefing

A full HUD-required move briefing will be held for participants who will be reissued a Voucher to move, and who have been recertified within the last 120 days, and have given notice of intent to vacate to their landlord. This briefing includes incoming and outgoing portable families. The briefings will be conducted in groups. Families who attend group briefings and still have the need for individual assistance will be referred to their Rental Assistance Specialist.

Owner Briefing

Briefing may be held for owners periodically. The purpose of the briefing is to assure successful owner participation in the program. Information provided will include the responsibilities and obligations of the three parties.

C. ENCOURAGING PARTICIPATION IN AREAS WITHOUT LOW INCOME OR MINORITY CONCENTRATION (Regional Opportunity Counseling (ROC) Grant)

At the briefing, families are encouraged to search for housing in non-impacted areas and the PHA will provide assistance to families who wish to do so.

The PHA has areas of poverty and minority concentration clearly delineated in order to provide families with information and encouragement in seeking housing opportunities outside highly concentrated areas.

The PHA provides information about facilities and services in neighboring areas such as schools, transportation, and supportive and social services.

The PHA will investigate and analyze when voucher holders are experiencing difficulties locating or obtaining housing units outside areas of concentration.

The assistance provided to such families includes:

- Providing families with a search record form to gather and record info.
- Direct contact with landlords.
- Counseling with the family.
- Providing information about services in various non-impacted areas.
- Meeting with neighborhood groups to promote understanding.
- Formal or informal discussions with landlord groups.
- Formal or informal discussions with social service agencies.
- Meeting with rental referral companies or agencies.
- Will meet with fair housing groups or agencies as needed or upon request.

D. ASSISTANCE TO FAMILIES WHO CLAIM DISCRIMINATION

The PHA will give participants a copy of HUD form 903 to file a complaint.

E. SECURITY DEPOSIT REQUIREMENTS [24 CFR 982.313]

Leases Effective Prior to October 2, 1995

The amount of Security Deposit that could have been collected by owners under contracts effective prior to October 2, 1995 is:

Under the pre-merger Certificate Program, the owner could have collected a Security Deposit in an amount not to exceed Total Tenant Payment or $50.00, whichever is greater, for non-lease-in-place families.

For the pre-merger Voucher Program, the owner, at his/her discretion, could have collected a Security Deposit in an amount not to exceed (PHA policy):

The greater of 30% of adjusted monthly income or $50 for non-lease-in-place families.

The amount charged to unassisted tenants may not exceed the maximum allowed under state or local law.

The greater of 30% of adjusted monthly income or [amount].

Leases Effective on or after October 2, 1995

The owner is not required to, but may collect a security deposit up to the maximum allowed by State and local law.

Security deposits charged to families may be any amount the owner wishes to charge**,** subject to the following conditions:

Security deposits charged by owners may not exceed those charged to unassisted tenants nor the maximum prescribed by State or local law.

For lease-in-place families, responsibility for first and last month's rent is not considered a security deposit issue. In these cases, the owner should settle the issue with the tenant prior to the beginning of assistance.

F. TERM OF VOUCHER [24 CFR 982.303, 982.54(d)(11)]

During the briefing session, each household will be issued a voucher which represents a contractual agreement between the PHA and the Family specifying the rights and responsibilities of each party. It does not constitute admission to the program which occurs when the lease and contract become effective.

Expirations

The Voucher is valid for a period of at least ninety (90) calendar days from the date of issuance. The family must submit a Request for Tenancy Approval and Lease within the ninety-day period unless an extension has been granted by the PHA.

If the Voucher has expired, and has not been extended by the PHA or expires after an extension, the family will be denied assistance. The family will not be entitled to a review or hearing. If the family is currently assisted, they may remain as a participant in their unit if there is an assisted lease/contract in effect.

Suspensions

When a Request for Approval of Tenancy is received, the PHA will deduct the number of days required to process the request from the 90 day term of the voucher.

Extensions

The PHA ~~will~~ may extend the term up to ~~150~~ 90 days from the voucher expiration date. ~~beginning of the initial term if the family needs and request an extension as a reasonable accommodation to make the program accessibleto and usable by a family member with a disability.~~ If as a reasonable accommodation, the family needs an extension in excess of 180 days, they must request the extension ~~same~~ in writing, prior to the expiration date of the voucher. ~~The PHA may grant such a request.~~

A family may request an extension of the voucher time period. All requests for extensions must be received, in writing, prior to the expiration date of the voucher.

Extensions are permissible at the discretion of the PHA up to a maximum of an additional ~~60~~ 90 days primarily for these reasons:

- Extenuating circumstances such as hospitalization or a family emergency for an extended period of time which has affected the family's ability to find a unit within the initial 90 day period. Verification is required.

- The PHA is satisfied that the family has made a reasonable effort to locate a unit, including seeking the assistance of the PHA, throughout the initial 90 day period. A completed search record **is** required including a minimum of 10 units viewed.

- The family was prevented from finding a unit due to disability accessibility requirements or bedroom unit requirement. The Search Record is part of the required verification.

Assistance to Voucher Holders

Families who require additional assistance during their search may call the PHA Office to request assistance. Voucher holders will be notified at their briefing session that the PHA periodically updates the listing of available units and how the updated list may be obtained.

The PHA will assist families with negotiations with owners and provide other assistance related to the families' search for housing.

After the first 30 days of the search the family is required to maintain a search record.

G. VOUCHER ISSUANCE DETERMINATION FOR SPLIT HOUSEHOLDS

24 CFR 982.315]

In those instances when a family assisted under the Section 8 program becomes divided into two otherwise eligible families due to divorce, legal separation, or the division of the family, and the new families cannot agree as to which new family unit should continue to receive the assistance, and there is no determination by a court, the Director of Rental Assistance shall consider the following factors to determine which of the families will continue to be assisted:

- Which of the two new family units has custody of dependent children.
- Which family member was the head of household when the Voucher was initially issued (listed on the initial application).
- The composition of the new family units, and which unit contains elderly or disabled members.
- Whether domestic violence was involved in the breakup.
- Which family members remain in the unit.
- Recommendations of social service professionals.

Documentation of these factors will be the responsibility of the requesting parties.

If documentation is not provided, the PHA will terminate assistance on the basis of failure to provide information necessary for a recertification.

H. REMAINING MEMBER OF TENANT FAMILY - RETENTION OF VOUCHER

[24 CFR 982.315]

To be considered the remaining member of the tenant family, the person must have been previously approved by the PHA to be living in the unit.

A live-in attendant, by definition, is not a member of the family and will not be considered a remaining member of the Family.

In order for a minor child to continue to receive assistance as a remaining family member:

- The court has to have awarded emancipated minor status to the minor, or
- The PHA has to have verified that social services and/or the Juvenile Court has arranged for another adult to be brought into the assisted unit to care for the child(ren) for an indefinite period.

A reduction in family size may require a reduction in the voucher family unit size.

I. SPLIT HOUSEHOLDS DURING PROGRAM PARTICIPATION

When families currently receiving assistance split, the current head of household retains continual voucher assistance. Remaining family members must separately apply when the waiting list is open to receive assistance.

EXHIBIT D

Chapter 21

HOUSING CHOICE VOUCHER HOMEOWNERSHIP OPTION

A. GENERAL PROVISIONS

The Housing Choice Voucher Homeownership Program of the Housing Opportunities Commission of Montgomery County, Maryland ("HOC") offers eligible participants in the Housing Choice Voucher program, including participants with portable vouchers, the option of purchasing a home with their Housing Choice Voucher assistance rather than renting. This is a program, which is limited to up to twenty-five (25). As many as three (3) slots are designated for households meeting HUD definition of disabled.

Participants will be chosen through the Commission-approved random selection and screening process.

Eligible applicants for the Housing Choice Voucher homeownership program must be participants in the Housing Choice Voucher rental program, may not owe HOC or any other Housing Authority an outstanding debt (unless they are making regular payments on the debt), and must meet the eligibility criteria set forth herein.

Housing Choice Voucher homeownership assistance may be used to purchase a home within Montgomery County (excluding the city of Rockville). HOC also will permit portability of Housing Choice Voucher homeownership assistance to another jurisdiction, provided the receiving jurisdiction operates and has an opening in Housing Choice Voucher homeownership program for which the Housing Choice Voucher homeownership applicant qualifies.

B. FAMILY ELIGIBILITY REQUIREMENTS

Participation in the Housing Choice Voucher homeownership program is voluntary. Each Housing Choice Voucher homeownership applicant must meet the general requirements for admission to the Housing Choice Voucher program as set forth in HOC's Administrative Plan. Such Housing Choice Voucher family also must be "eligible" to participate in the homeownership program. The additional eligibility requirements for participation in HOC's Housing Choice Voucher homeownership program include that the family must: (1) be a first-time homeowner or have a member who is a person with disabilities; (2) with the exception of elderly and disabled households, meet a minimum income requirement without counting income from "welfare assistance" sources; (3) with the exception of elderly and disabled households, meet the requisite employment criteria; (4) be a current participant in the Housing Choice Voucher program; (5) have fully repaid any outstanding debt owed to HOC or any other Housing Authority (unless they are making regular payments); (6) not defaulted on a mortgage securing debt to purchase a home under the homeownership option; and (7) not have any member who has a present ownership interest in a residence at the commencement of home- ownership assistance.

1. First-Time Homeowner.

Each Housing Choice Voucher family, except families with a disabled member, must be a first-time homeowner. A "first-time homeowner" means that no member of the household has had an ownership interest in any residence during the three years preceding commencement of home- ownership assistance. However, a single parent or displaced homemaker who, while married, owned a home with a spouse (or resided in a home owned by a spouse), and no longer owns the home, is considered a "first-time homeowner" for purposes of the Housing Choice Voucher homeownership option; and the right to purchase title to a residence under a lease-purchase agreement is not considered an "ownership interest."

2. Minimum Income Requirement.

(a) Amount of Income.

At the time the family begins receiving homeownership assistance, the head of household, spouse, and/or other adult household members who will own the home must have a gross annual income of ~~$24,000~~ $40,000.

(b) Exclusion of Welfare Assistance Income.

With the exception of elderly and disabled families, HOC will disregard any "welfare assistance" income in determining whether the family meets the minimum income requirement. Welfare assistance includes assistance from Temporary Assistance for Needy Families ("TANF"), Supplemental Security Income ("SSI") that is subject to an income eligibility test, food stamps, general assistance, or other welfare assistance specified by HUD. The disregard of welfare assistance income under this section affects the determination of minimum monthly income in determining initial qualification for the homeownership program. It does not affect the determination of income-eligibility for admission to the Housing Choice Voucher program, calculation of the family's total tenant payment, or calculation of the amount of homeownership assistance payments.

3. Employment History.

With the exception of disabled and elderly households, each family must demonstrate that one or more adult members of the family who will own the home at commencement of homeownership assistance is employed full-time (an average of 30 hours per week) and has been so continuously employed for one year prior to execution of the sales agreement. In order to reasonably accommodate a family's enrollment in the program, HOC will exempt families that include a person with disabilities from this requirement. HOC's Executive Director may also consider whether and to

what extent an employment interruption is considered permissible in satisfying the employment requirement. The Executive Director may also consider successive employment during the one-year period and self-employment in a business.

4. Current Participant in Housing Choice Voucher Program.

Applicants for and new applicants and participants in the Housing Choice Voucher homeownership program must be current participants in the rental program and be in good standing with HOC.

5. Repayment of any Housing Authority Debts.

Applicants in the Housing Choice Voucher program shall be ineligible for participation in the Housing Choice Voucher homeownership program in the event any debt or portion of a debt remains owed to HOC or any other Housing Authority. Nothing in this provision will preclude Housing Choice Voucher participants that have fully repaid such debt(s) from applying for and participating in the Housing Choice Voucher homeownership program (unless they are making regular payments on the debt).

6. Additional Eligibility Factors.

(a) Elderly and Disabled Households.

Elderly and disabled families are exempt from the employment requirements set forth in Section B (3) above. In the case of an elderly or disabled family, HOC will consider income from all sources, including welfare assistance, in evaluating whether the household meets the minimum income required to purchase a home through the Housing Choice Voucher homeownership program.

(b) Participation in FSS Program.

In order to be selected for the homeownership program, all applicants, excluding those with disabilities, must have either successfully graduated from HOC's Family Self-Sufficiency (FSS) Program or be currently enrolled in HOC's FSS Program and completed two years of participation in HOC's Family Self Sufficiency ("FSS") Program prior to completion of homeownership counseling, and be in good standing with the FSS Program, in order to apply for and participate in

the homeownership program. Persons with disabilities must have completed one year of participation in HOC's Family Self Sufficiency ("FSS") Program.

(c) Prior Mortgage Defaults.

If a head of household, spouse, or other adult household member who will execute the contract of sale, mortgage and loan documents has previously defaulted on a mortgage obtained through the Housing Choice Voucher home- ownership program, the family will be ineligible to participate in the homeownership program.

C. FAMILY PARTICIPATION REQUIREMENTS

Once a family is determined to be eligible to enroll in the program, it must comply with the following additional requirements: (1) complete a home- ownership counseling program approved by HOC prior to commencement of homeownership assistance; (2) within three years of completion of counseling, locate and contract for the home it proposes to purchase; (3) submit a sales agreement containing specific components to HOC for approval; (4) allow HOC to inspect the proposed homeownership dwelling to assure that the dwelling meets appropriate housing quality standards; (5) obtain an independent inspection covering major building systems; (6) obtain HOC approval of the proposed mortgage (which must comply with generally accepted mortgage underwriting requirements); and (7) enter into a written agreement with HOC to comply with all of its obligations under the Housing Choice Voucher program.

1. Homeownership Counseling Program.

A family's participation in the homeownership program is conditioned on the family attending and successfully completing a homeownership counseling program provided or approved by HOC prior to commencement of homeownership assistance. The homeownership and counseling program will include home maintenance; budgeting and money management; credit counseling; negotiating purchase price; securing mortgage financing; finding a home; and the advantages of purchasing and locating homes in areas that do not have a high concentration of low-income families.

The counseling agency providing the counseling program shall be approved either by HUD and/or HOC, or the program shall be consistent with the homeownership counseling provided under HUD's Housing Counseling program. HOC may require families to participate in a HOC-approved homeownership counseling program on a continuing basis.

2. Locating and Purchasing a Home.

(a) Locating a Home.

Upon approval for the Housing Choice Voucher home- ownership program and completion of counseling, a family shall have three years to settle on a home to purchase. A home shall be considered located if the family submits a signed sales agreement with the requisite components to HOC. During a Housing Choice Voucher participant's search for a home to purchase, the Housing Choice Voucher rental assistance shall continue pursuant to the Administrative Plan. If a Housing Choice Voucher participant family is unable to locate a home within the time approved by HOC, their Housing Choice Voucher rental assistance through the Housing Choice Voucher program shall continue.

(b) Type of Home.

A family approved for Housing Choice Voucher homeownership assistance may purchase the following type of homes within Montgomery County: a new or existing home with a purchase price at or below the FNMA/FHLMC Single Family Loan Limits, a single-family home, a condominium, a home in a planned use development, a cooperative, a loft or live/work unit, or a manufactured home to be situated on a privately owned lot or on a leased pad in a mobile home park. The home must already exist or be under construction at the time HOC determines the family eligible for homeownership assistance to purchase the unit. The family also may purchase a home in a jurisdiction other than Montgomery County, provided the Housing Authority in the receiving jurisdiction operates a Housing Choice Voucher homeownership program for which the Housing Choice Voucher homeownership applicant qualifies. In such a case, a family's participation in the Housing Choice Voucher home-ownership program will be subject to the Housing Choice Voucher homeownership program and policies of the receiving jurisdiction.

(c) Purchasing a Home.

Once a home is located and a sales agreement approved by HOC is signed by the family, the family shall have up to three (3) months, or such other time as is approved by HOC's Executive Director or set forth in the HOC-approved sales agreement, to purchase the home.

(d) Failure to Complete Purchase.

If a Housing Choice Voucher participant is unable to purchase the home within the maximum time permitted by HOC, HOC shall terminate the participant's enrollment in the home- ownership program. The family may

not re-apply for the Housing Choice Voucher homeownership program until they have completed two additional years of participation in the Housing Choice Voucher program following the initial determination of their eligibility for the homeownership option.

(e) Lease-Purchase

Lease-purchase agreements are not permitted.

(f) Down Payment

The family must meet a minimum homeowner down payment requirement of at least three percent of the purchase price for participation in the Voucher homeownership program. At least one percent of the purchase price must come from the family's personal resources.

3. Sales Agreement.

Prior to execution of the offer to purchase or sales agreement, the financing terms must be provided by the family to HOC for approval. The sales agreement must provide for inspection by HOC and the independent inspection referred to in Section C(4) and must state that the purchaser is not obligated to purchase unless such inspections are satisfactory to HOC. The contract also must provide that the purchaser is not obligated to pay for any necessary repairs. The sales agreement must provide that the purchaser is not obligated to purchase if the mortgage financing terms are not approved by HOC pursuant to Section C(6). The sales agreement must also contain a seller certification that the seller is not debarred, suspended, or subject to a limited denial of participation under 24 CFR part 24.

4. Independent Initial Inspection Conducted.

To assure the home complies with the housing quality standards of the Housing Choice Voucher program, homeownership assistance payments may not commence until HOC first inspects the home. An independent inspection of existing homes covering major building systems also must be completed by a professional selected by the family and approved by HOC. HOC will not pay for the independent inspection. The independent inspection report must be provided to HOC. HOC may disapprove the unit due to information contained in the report or for failure to meet federal housing quality standards.

5. Financing Requirements.

The proposed financing terms must be submitted to and approved by HOC prior to close of escrow. HOC will approve or disapprove the financing terms within five (5) business days. HOC shall determine the affordability of the family's proposed financing. In making such determination, HOC may take into account

other family expenses, including but not limited to child care, unreimbursed medical expenses, education and training expenses and the like. Certain types of financing, including but not limited to, balloon payment mortgages and adjustable rate mortgages, are prohibited and will not be approved by HOC. Seller-financing mortgages shall be considered by HOC on a case by case basis. If a mortgage is not FHA-insured, HOC will require the lender to comply with generally accepted mortgage underwriting standards consistent with those of HUD/ FHA, Ginnie Mae, Fannie Mae, Freddie Mac, the Federal Home Loan Bank of Atlanta, or other private lending institution.

A second trust for closing costs is permitted.

6. Family Compliance with Program Policies.

A family must agree, in writing, to comply with all family obligations under the Housing Choice Voucher program and HOC's homeownership policies. These obligations include (1) attending ongoing home- ownership counseling, if required by HOC; (2) complying with the mortgage terms; (3) not selling or transferring the home to anyone other than a member of the assisted family who resides in the home while receiving homeownership assistance; (4) not refinancing or adding debt secured by the home without prior approval by HOC; (5) not obtaining a present ownership interest in another residence while receiving home- ownership assistance; and (6) supplying all required information to HOC including, but not limited to, annual verification of household income, notice of change in homeownership expenses, notice of move-out, and notice of mortgage default. HOC's Homeownership Family Obligation policies are set forth in Appendix A. Once the home purchase is complete, the family becomes a participant in the HCV homeownership program.

D. AMOUNT OF ASSISTANCE

The amount of the monthly assistance payment will be based on three factors: the voucher payment standard for which the family is eligible, the monthly home- ownership expenses, and the family's household income. HOC will pay the lower of either the payment standard minus the total family contribution ("TFC") or the family's monthly homeownership expenses minus the TFC. The Housing Choice Voucher family will pay the difference.

1. Determining the Payment Standard.

The voucher payment standard is the fixed dollar amount the HOC annually establishes for a unit of a particular size located within the HOC jurisdiction. In the homeownership program, the initial payment standard will be the lower of either (1) the payment standard for which the family is eligible based on family size, or (2) the payment standard which is applicable to the size of the home the

family decides to purchase. The payment standard for subsequent years will be based on the higher of: (1) the payment standard in effect at commencement of the homeownership assistance, or (2) the payment standard in effect at the most recent regular reexamination of the family's income and size. The initial payment standard, for purposes of this comparison, shall not be adjusted even if there is a subsequent decrease in family size.

Exception rents, if in effect for the Housing Choice Voucher rental program, will also apply to the homeownership program.

2. Determining the Monthly Homeownership Expense.

Monthly homeownership expense includes all of the following: principal and interest on the initial mortgage and any mortgage insurance premium (MIP) incurred to finance the purchase and any refinancing of such debt; real estate taxes and public assessments; homeowner's insurance; maintenance expenses per HOC allowance; costs of major repairs and replacements per HOC allowance (replacement reserves); utility allowance per HOC's schedule of utility allowances; principal and interest on mortgage debt incurred to finance major repairs, replacements or improvements for the home including changes needed to make the home accessible; and homeowner association dues, fees or regular charges assessed, if any. Homeownership expenses for a cooperative member may only include HOC approved amounts for the cooperative charge under the cooperative occupancy agreement including payment for real estate taxes and public assessments on the home; principal and interest on initial debt incurred to finance purchase of cooperative membership shares and any refinancing of such debt; home insurance; the allowances for maintenance expenses, major repairs and replacements and utilities; and principal and interest on debt incurred to finance major repairs, replacements, or improvements, including changes needed to make the home accessible.

3. Determining the Total Family Contribution

The TFC is that portion of the homeownership expense that the family must pay. It is generally 30% of the family's adjusted income plus any gap between the payment standard and the actual housing cost. All family income (including public assistance) will be counted to determine the family's adjusted monthly income for purposes of determining the amount of assistance.

4. Payment to Family or Lender.

HOC will provide the lender with notice of the amount of the housing assistance payment prior to close of escrow and will pay HOC's contribution towards the family's homeowner expense directly to the family unless otherwise required by the lender. The family will be responsible to submit the entire mortgage payment to the lender unless the lender requires direct payment of HOC's contribution.

E. TERMINATION OF HOUSING CHOICE VOUCHER HOMEOWNERSHIP ASSISTANCE

1. Grounds for Termination of Homeownership Assistance.

(a) Failure to Comply with Family Obligations under Housing Choice Voucher Program or HOC's Homeownership Policies.

A family's homeownership assistance may be terminated if the family fails to comply with its obligations under the Housing Choice Voucher program, HOC homeownership policies, or if the family defaults on the mortgage. If required, the family must attend and complete ongoing homeownership and housing counseling classes. The family must comply with the terms of any mortgage incurred to purchase and/or refinance the home. The family must provide HOC with written notice of any sale or transfer of any interest in the home, any plan to move out of the home prior to the move, the family's household income and homeownership expenses on an annual basis, any notice of mortgage default received by the family, and any other notices which may be required pursuant to HOC homeownership policies. Except as otherwise provided in this Section, the family may not convey or transfer the home to any entity or person other than a member of the assisted family while receiving homeownership assistance.

(b) Occupancy of Home.

Homeownership assistance will only be provided while the family resides in the home. If the family moves out of the home, HOC will not continue homeownership assistance commencing with the month after the family moves out. Neither the family nor the lender is obligated to reimburse HOC for homeownership assistance paid for the month the family moves out.

(c) Changes in Income Eligibility.

A family's homeownership assistance may be changed in the month following annual recertification of the household income, but participation in the Housing Choice Voucher Homeownership program shall continue until such time as the assistance payment amounts to $0 for a period of six (6) consecutive months.

(d) Maximum Term of Homeownership Assistance.

Notwithstanding the provisions of Section E(1), subparagraphs (a) through (c), except for disabled and elderly families, a family may receive Housing Choice Voucher homeownership assistance for not longer than ten (10) years from the date of close of escrow unless the initial mortgage incurred to finance purchase of the home has a term that is 20 years or longer, in which case the maximum term is 15 years. Families that qualify as elderly at the commencement of homeownership assistance are not subject to a maximum term limitation. Families that qualify as disabled families at the commencement of homeownership assistance or at any time during the provision of homeownership assistance are not subject to a maximum term limitation. If a disabled family or elderly family ceases to qualify as disabled or elderly, the appropriate maximum term becomes applicable from the date homeownership assistance commenced provided, however, that such family shall be eligible for at least six additional months of homeownership assistance after the maximum term becomes applicable. The time limit applies to any member of the household who has an ownership interest in the unit during any time that homeownership payments are made or is a spouse of any member of the household who has an ownership interest.

2. Procedure for Termination of Homeownership Assistance.

A participant in the Housing Choice Voucher Homeownership program is a family who has purchased a home in this program Participants shall be entitled to the same termination notice and informal hearing procedures as set forth in the Administrative Plan of the HOC for the Housing Choice Voucher program.

E. CONTINUED PARTICIPATION IN HOUSING CHOICE VOUCHER PROGRAM

1. Default on FHA-Insured Mortgage.

If the family defaults on an FHA-insured mortgage, HOC may permit the family to move with continued Housing Choice Voucher rental assistance if the family demonstrates that it has (a) conveyed title to the home to HUD or its designee as required by HUD, and (b) moved from the home within the period established or approved by HUD.

2. Default on non-FHA-Insured Mortgage.

If the family defaults on a mortgage that is not FHA-insured, HOC may permit the family to move with continued Housing Choice Voucher rental assistance if the family demonstrates that it has (a) conveyed title to the home to the lender, to HOC or to its designee, as may be permitted or required by the lender; and (b)

moved from the home within the period established or approved by the lender and/or HOC.

3. Continued Housing Choice Voucher Rental Assistance

HOC will determine on a case-by-case basis, in compliance with federal law and regulations, if a family terminated from the home- ownership program will remain eligible Housing Choice Voucher rental assistance.

G. HOC ADMINISTRATIVE FEE

For each month that homeownership assistance is paid by HOC on behalf of the family, HOC shall be paid the ongoing administrative fee described in 24 C.F.R. §982.152(b).

H. WAIVER OR MODIFICATION OF HOMEOWNERSHIP POLICIES

The Executive Director of HOC shall have the discretion to waive or modify any provision of the Housing Choice Voucher homeownership program or policies not governed by statute or regulation for good cause or to comply with changes in HUD regulations or directives.

APPENDIX A: HOUSING CHOICE VOUCHER HOMEOWNERSHIP OBLIGATIONS

This form is to be signed by the home buyer(s) in the presence of the Housing Opportunities Commission's (HOC) Homeownership Program Coordinator. The Coordinator will explain any and all clauses which you, the home buyer(s), may not understand.

The following paragraphs describe your responsibilities under the Housing Choice Voucher Homeownership Program. If you or members of your household do not meet these responsibilities through your actions or your failure to act, you may be determined ineligibile for or terminated from the Housing Choice Voucher Homeownership Program.

1. Family Obligations: You must comply with all Family Obligations of the Housing Choice Voucher Program, excepting only the prohibition against owning or having an interest in the unit. Family Obligations §§ 982.551(c),(d),(e),(f),(g) and (j) do not apply to the Housing Choice Voucher Homeownership Program.

2. Housing Counseling: All applicant family members (i.e. those who will be signing the purchase offer and loan documents) must satisfactorily complete a HOC provided or approved counseling program prior to commencement of homeownership assistance. HOC may require any or all applicant family members to attend additional housing counseling classes as a condition of continued assistance.

3. Employment History: With the exception of disabled and elderly households, each family must demonstrate that one or more adult members of the family who will own the home at commencement of homeownership assistance is employed full-time(an average of 30 hours per week) and has been so continuously employed for one year prior to execution of the sales agreement. In order to reasonably accommodate a family enrollment in the program, HOC will exempt families that include a person with disabilities from this requirement. HOC's Executive Director may also consider whether and to what extent an employment interruption is considered permissible in satisfying the employment requirement. The Executive Director may also consider successive employment during the one-year period and self-employment in a business.

4. Purchase Contract: You must include contract conditions in any Offer to Purchase that give HOC a reasonable time (a) to inspect the home for compliance with HUD's Housing Quality Standards, (b) to review and approve a professional home inspection report obtained by you from a HOC approved inspector, and (c) approve the terms of your proposed financing. Advise your real estate broker, agent or Realtor of these requirements. You must settle on a home within three years of completion of home ownership counseling.

5. Mortgage Obligations: You must comply with the terms of any mortgage incurred in the purchase of the property and must notify HOC's Homeownership Program Counselor within five (5) days of receipt of any late payment notice or default notice.

6. Occupancy: You must occupy the unit as your principal residence. You may not transfer, sell, or assign any interest in the property without HOC's prior written consent. You may not rent or lease any part of the premises without HOC's prior written consent. You must notify HOC in writing at least 30 days prior to moving out of the house for a period of 30 days or longer or prior to any sale, transfer, assignment, lease or other form of alienation of the assisted property.

7. Maintenance: You must maintain the property in a decent, safe and sanitary manner in compliance with County codes and other prevailing standards. You must allow HOC to inspect the property within one-week of a demand by HOC to conduct an inspection. You must correct any notice of deficiency issued by HOC within the time limit specified in the notice. If you fail to adequately maintain the property, HOC may divert the maintenance and replacement reserves portions, if applicable, of the Homeownership Assistance Payment to an escrow account to be used to pay for reasonable and necessary maintenance expenses.

8. Annual Re-examination: You must annually provide HOC with current information regarding family income and composition in a format required by HOC.

9. Refinancing: You must notify HOC in writing of any proposal to refinance the original purchase mortgage or of any proposal to encumber the property with secondary financing and obtain HOC's written approval of such financing prior to executing any loan documents.

10. Default: In the event of a default on your mortgage obligation, you must cooperate with HOC and the lender to minimize any loss to the lender in order to maintain your eligibility to continue as a participant in the Housing Choice Voucher Program.

By signing below, I attest that I have read and understand my obligations as an applicant and a participant in the Housing Choice Voucher Homeownership Program and I agree to abide by these responsibilities. I understand that HOC may determine me ineligible for homeownership assistance if I violate my obligations after the purchase of a home, but that I may request an informal hearing of any notice of termination prior to it becoming effective.