ENTERPRISE INFORMATION SECURITY STANDARDS

Commonwealth of Massachusetts
Executive Office of Health and Human Services

I. CONTENTS

II. PURPOSE AND INTRODUCTION

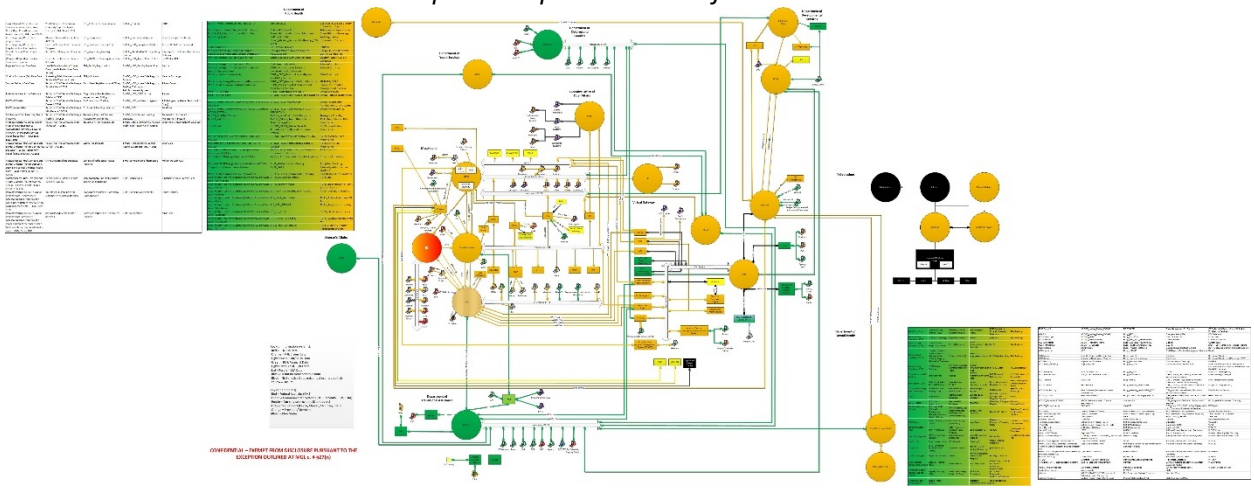
The EOHHS Information Security Office's mission is to safeguard EOHHS's and its Agencies' collective data in any form and prevent the inappropriate use, exfiltration, or manipulation of that data. The Security Office works constantly to maximize preservation of the confidentiality, availability, and integrity of EOHHS data through the promulgation, implementation, and enforcement of administrative, physical, and technical safeguards.

This document outlines the specific ways such data should be preserved. It provides the bare minimum standards that apply to all Information Resources in the EOHHS Environment and within third party environments contracted for by EOHHS or which use, process, or maintain EOHHS data. These have been drafted with an eye towards:

- Federal and State legal requirements
- Specific data source contractual requirements
- Commonwealth enterprise policies and standards (available at: https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards)
- Extant good practice at Agencies and within Information Systems
- Other factors as appropriate

The need for this broadly applicable set of standards is clear when looking at the EOHHS Environment in its entirety.

Table 1: Graphical Representation of EOHHS Environment



As illustrated in Table 1, all Information Systems in the EOHHS Environment are connected, either directly or through other Information Systems which share data downstream. Few systems in the EOHHS Environment are truly independent of that environment. To the extent those applications are used to support Agency operations alongside other applications and their data can impact Agency operations, they are not independent.

Additionally, very little—if any—physically held data (e.g.: paper documents, filing cabinets holding documents, etc.) maintained in the EOHHS Environment exists independently of EOHHS's Information Systems. Those physical data stores either come from Information Systems or are used to populate

information into Information Systems. As such, all physical instances of data—or physical instances of information— maintained in the EOHHS Environment or by a third party fall within the purview of these Information Security standards.

Because of the extreme interconnectedness of all data held (in any form) at EOHHS, and to promote the common security of data shared among the EOHHS enterprise, these common controls are designed to protect all data with the same high standards no matter where it is used, processed, or maintained within the EOHHS Environment. However, due to the state of standardization across EOHHS, not all applications existing or in development can strictly adhere to this *Enterprise Information Security Standards* (also referred to as "Document"). The Security Office strongly recommends that all Information Systems strive to achieve compliance with this Document, however any gaps will be identified and tracked through gap assessments being conducted of the EOHHS Environment. EOHHS and Agency process must be updated to achieve compliance with applicable standards within twenty-four (24) months from publication of this Document. Compliance timelines have been included with each standard. Achieving compliance may be completed by implementing a corrective action plan with additional reasonable timelines for conformance—supported by business necessity and technical requirements—outlining why compliance cannot be attained within the timelines outlined in this Document. Such corrective action plans must follow the guidelines outlined in *Section III, Requests for Non-Conformance*. Additionally, all applications procured or developed after the publication date of version 1.0 of this Document must be developed in conformance with these requirements.

Additionally, EOHHS is bound by state and federal laws, contracts, and processes to comply with various notification procedures in the event of a loss of data, an impact of service, or a data breach, whether it happens at EOHHS or with one of its third party vendors, providers or other teaming partners. EOHHS will also face associated negative press, fines, and other penalties associated with loss of confidentiality, integrity, or availability of the data. As such, these standards also act as a guideline with regard to the security requirements EOHHS must push down to any third party vendor.

The Security Office has been tasked with preserving the confidentiality, integrity, and availability of all EOHHS Information Resources. As such, this Document outlines the minimum acceptable requirements at EOHHS for the information security controls outlined herein. Agencies may develop their own documentation to supplement and exceed these requirements, which are generic for the EOHHS Environment at large, and are encouraged to do so. Agencies may not undertake any action or promulgate documentation to supplant or undermine the controls or activities described in this Document, whether specifically identified as intended to do so or not.

These *Enterprise Information Security Standards* supersede all EOHHS and/or Agency documentation existing before the publication date of this Document which also covers the same subject matter as these standards or any portion thereof. No other EOHHS or Agency documentation covering the same subject matter as these *Enterprise Information Security Standards*, unless as expressly required to be developed by these *Enterprise Information Security Standards*, shall be effective without the review and approval of the EOHHS Security Office.

The consequences for violating these *Enterprise Information Security Standards* are serious. By violating this policy, you create an immediate and automatic audit finding for your Agency. These Audit findings could result in significant negative press for your Agency, additional oversight and reporting requirements, and fines. In addition, depending on the objectives violated and the method of violation, you may be subject to discipline including termination of employment, civil penalties including monetary

fines, and criminal penalties including jail time. Conformance to these policies will be actively monitored on an ongoing basis and violations will be reported to Agency and Secretariat executive staff.

III. REQUESTS FOR NON-CONFORMANCE

Any non-conformance to these standards could have dire and unintended impacts to other Information Resources or Information Systems in the EOHHS Environment. Additionally, the failure to appropriately record non-conformance to standards and any activities undertaken to minimize the impact to EOHHS's security posture could result in audit findings, fines, and other penalties. Given the nature of these controls and the interconnectedness of the EOHHS Environment, no individual Agency group is appropriately equipped to approve non-conformance to these standards. The process outlined in this section will detail how a request for non-conformance should be made and processed. For promotion of vulnerabilities from a lower to a production environment, or for risk acceptance of ongoing vulnerabilities, see the *Authorization to Operate and Operational Risk Assessment Policy and Process*.

a. All requests for non-conformance should be submitted to the EOHHS Security Office mailbox at: EOHHS-SecurityOffice@MassMail.State.MA.US. All requests must include "Request for Non-Conformance" in the title and the application/program name for which a request for non-conformance is sought.

The body of the email should describe:

i. the request being made,
ii. the justification,
iii. any compensating controls put in place to address the security gap (or a reason why there is no security gap)
iv. timelines to address the security gap
v. the name, title, and contact information of the individual responsible for the request

b. The request will be evaluated by the Security Office, which may seek additional information from the requester, members of EOHHS and/or impacted Agency legal teams, impacted Agency operations, and the EOHHS SCIO and/or impacted ACIOs. Response times may vary depending on the request, but all requests will be addressed within forty-eight (48) hours of receipt.

c. Once the Security Office has completed its evaluation, it will provide a memorandum to the requester outlining any research performed, recommendations, and agreed-upon timelines during which there will be a security gap.

d. Quarterly, the Security Office will meet with requesters to discuss the status of implementation of compensating controls or closing the security gap. Biennially, the Security Office will circulate the master list of requests for non-conformance to Agency and IT leadership for review and analysis.

IV. SECURITY PLANNING

a. Policy Statement

EOHHS must develop, maintain, and disseminate a security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

b. Security Planning Standards

This information security plan outlines the minimum functions necessary to ensure the effective and efficient operations of the Secretariat in a way that maximizes the safety of sensitive information. While many of the organizational roles and responsibilities are outlined herein, not all specific roles and responsibilities are identified. It is the responsibility of application teams and business units to ensure that they appropriately identify critical or material positions within their respective organizations. Information security planning is a comprehensive, organization-wide effort to ensure that information in all forms is protected.

i. *Roles and Responsibilities*

1. Agency heads and Secretariat Chief Information Officer – these individuals are responsible for business unit and information technology planning and setting priorities for their respective organizations. These individuals are also accountable for the responsible development of programs and systems within their purview. This includes considerations of legal and policy compliance; implementation of industry standard best practices; and ensuring appropriate custodianship of constituent data that protects the confidentiality, integrity, and availability of that data.
2. Agency management teams and Assistant Chief Information Officers – these individuals are responsible for direct oversight, management and implementation of business unit and information technology planning and projects as well as for the development of programs and systems within their purview.
3. Chief Security Officer – this individual is responsible for the creation and verification of standards at EOHHS to support the responsible development of programs and systems at EOHHS.
4. EOHHS Staff – these individuals are responsible for following acceptable rules of behavior, including the *EOHHS Acceptable Use Policy*. Additionally, these individuals are responsible for ensuring the confidentiality, integrity, and availability of data maintained by EOHHS and its Agencies.

ii. *Information Resource Security Plans*

All Information Resources and business units must complete a security plan. This security plan must cover, at a minimum, the following topics:

1. How the information resource or business process operates consistently with enterprise architecture or planning;
2. The boundaries of the information resource or business process;
3. How the information resource or business process supports Agency operations and the Agency mission;
4. The security posture, security requirements and risk level of the information resource or business process;
5. Relationships and interconnections between the information resource or business process and other information resources or business processes;
6. Security controls in place based on the NIST 800-53 standards appropriate to that application as expressed by these *Enterprise Information Security Standards*, security controls not in place, and planned remediation or workarounds (including compensating controls);
7. How the information resource or business process architecture/design protects the confidentiality, integrity, and availability of information; and
8. Any assumptions about internal or external services and their impact to security.

These requirements will be satisfied by compliance with:

- *Section VIII, Inventory and Classification*,
- *Section IX, Assessment and Monitoring*,
- The EOHHS IT Control Plan,
- *The EOHHS Technology Office Secretariat Application Reference Manual*, and
- *The Project Integration Process & Controls Guide*.

The security plan must be reviewed and updated no less frequently than every three years.[1] While the security plan should be communicated to relevant internal and external authorized parties, it should be safeguarded from inappropriate disclosure that would compromise the security of the Information Resource.

iii. *Rules of Behavior*

The rules of behavior for use of EOHHS information resources is outlined in *Section V, Acceptable Use and Information Security Training*. Agency management teams and ACIOs are responsible for devising plans to ensure review, attestation, and compliance with the Acceptable Use Policy.

V. ACCEPTABLE USE AND INFORMATION SECURITY TRAINING

a. Purpose and Introduction

The key to ensuring a safe and secure environment is by having a staff that is competent and capable with respect to information security. No matter how secure and airtight an

[1] Pursuant to 45 CFR § 95.621, for APD-funded operations and Information Resources, this is every two years.

organization's technical environment, if its employees cannot handle information appropriately, each of those employees poses a significant vulnerability to the organization.

This *Section V, Acceptable Use and Information Security Training*, will offer the requirements for training and provide managers and staff the tools they need to ensure the EOHHS Environment is adequately protected against external and internal threats.

Agencies are encouraged to develop information security training in addition to the requirements outlined in this section. If, at the time of publication of this policy, Agencies have documentation they believe satisfies the requirements herein for acceptable use or information security training, or if the Agency develops any related documentation after the publication of this policy, the Security Office must review and approve of such documentation before implementation.

b. Policy Statement

All EOHHS employees must review and acknowledge the *EOHHS Acceptable Use Policy* within one (1) month of hire and on an annual basis thereafter, as determined by EOHHS. All EOHHS employees must take EOTSS and EOHHS training within one (1) month of hire and on an annual basis thereafter. If an EOHHS employee has not met these requirements, they shall not be provided access to Information Resources in the EOHHS Environment. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Acceptable Use Standards

The *EOHHS Acceptable Use Policy* details its purpose, requirements and scope. In summary, the Acceptable Use Policy explains the difference between appropriate and inappropriate—or permissible and impermissible—use of Information Resources across EOHHS.

In the event that any staff is found to have violated the Acceptable Use Policy, depending on factors such as the magnitude of the violation(s), the number of violation(s), and the kind of violation(s), those staff may be disciplined. Such discipline may include limitation of or removal of rights to access Information Resources, suspension or termination of employment, or civil and criminal penalties such as fines and incarceration.
The current version of record of the *EOHHS Acceptable Use Policy* is hosted on PACE and is attached to this document as Attachment 1. Older versions of the *EOHHS Acceptable Use Policy* may be stored elsewhere but should not be relied upon for compliance purposes.

Agencies may not under any circumstances create documentation to supplant or replace the *EOHHS Acceptable Use Policy*. Agencies may, however, create documentation that effectively supplements or adds to the *EOHHS Acceptable Use Policy* based on demonstrated and legitimate Agency need. Agencies are strongly encouraged to do so where the *EOHHS Acceptable Use Policy* has perceived deficiencies based on the quality or kind of data being handled by the Agency or based on legal compliance. Any supplementary materials, whether or not identified as such, must be reviewed and approved by the Security Office prior to publication and dissemination to staff. Such supplementary materials will be made effective by appending them to the *EOHHS Acceptable Use Policy* as an exhibit.

d. Information Security Training Standards

All EOHHS staff must review and acknowledge the EOHHS Information Security Training, or an approved alternative, within one (1) month of hire and prior to accessing any Information Resources in the EOHHS Environment and then on an annual basis thereafter as defined by EOHHS. The EOHHS Information Security Training shall consist of two components:

i. Any required EOTSS information security training generally made available to EOHHS staff, and
ii. Any required EOHHS information security training.

EOHHS has published the EOHHS Information Security Training on PACE. Previous versions of the EOHHS Information Security Training may be stored elsewhere but should not be relied upon for compliance purposes. At a minimum, all staff are required to take that calendar year's information security training posted to PACE. The Security Office has also developed other information security training for specific types of data that may be required based on job duties and role.

All EOHHS staff must take information security training that covers the following subject matter:

- Definition of sensitive information,
- An explanation of the need to safeguard sensitive information,
- How to protect sensitive information,
- Least access privilege,
- Password requirements,
- Kinds of data breaches and attack vectors,
- Email management,
- Incident reporting, and
- Steps that staff can take to prevent a data breach.

The current EOHHS information security training is deemed to meet the requirements of Executive Order 504 training for EOHHS employees. Additionally, the training is designed to contain information that is intended to meet the training requirements of the HIPAA Security Rule and applicable Third Party Agreements.

Agencies may create documentation that effectively supplants or replaces the EOHHS Information Security Training. Agencies may also create documentation that effectively supplements or adds to the EOHHS Information Security Training. Agencies are strongly encouraged to do so where the EOHHS Information Security Training has perceived deficiencies based on the quality or kind of data being handled by the Agency or based on legal compliance. Any supplanting or supplementary materials, whether or not identified as such, must be reviewed and approved by the Security Office prior to publication and dissemination to staff.

VI. ACCESS CONTROL

a. Purpose and Introduction

Access Control, in the broadest sense, deals with who has access to what and how. The standards outlined in this Access Control section address specific requirements about how permission to view, use, change, or update Information Resources should be granted, modified, and revoked in the EOHHS Environment. For access controls for facilities themselves, please see *Section XVII, Physical and Environmental Protections*.

Agencies may—and are encouraged to—promulgate desk level procedures and standards to implement the requirements outlined herein for their Information Resources. Agencies may already have access control documentation. This Access Control standard is not intended to supplant those documents. Care should be taken to ensure those standards conform to the requirements expressed herein. Agencies may not implement documentation, standards, or requirements that supplant these Access Control standards or modify, compromise, or circumvent the underlying controls in this document in any way.

While this document is drafted with a focus to managing access to Information Systems, the process outlined herein can—and should—be applied to all EOHHS Information Resources in whatever form and to all processes which utilize such data.

b. Policy Statement

All EOHHS Information Resources must have appropriate access controls in place to prevent unauthorized access. All access to Information Resources must be appropriate based on role, employment status, and business need. All Information Resource Owners must have the ability to control, audit, and terminate access to Information Resources. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

c. Access Control Standards

Every Information Resource must have clearly defined and readily identifiable Owners. Owners must be capable of independently making material decisions and modifications with respect to the direction and operations of the Information Resource. In the event an Information Resource does not have a clearly defined and readily identifiable Owner upon request, the Chief Operating Officer (or equivalent position) and ACIO of the Agency to which the Information Resource is associated and/or belongs shall be assigned such roles by default. In the event an Information Resource does not belong to a specific Agency, the EOHHS Assistant Secretary for Administration and Finance and SCIO shall be assigned to such roles by default.

i. *Defining Roles and Accounts*

Information Resource Owners are responsible for identifying Roles and accompanying accounts in the Information Resource. To simplify the relationship

between Roles and accounts: Roles address business function and accounts address technical access based on business function. Those Owners must ensure implementation of the following requirements when defining Roles and accounts:

1. **Roles:** Each Information Resource must have clearly defined and documented Roles (including group Roles) based on responsibility, business need, staff role, or other logical association. The documentation of such Roles must include criteria for membership in that Role and an overview of the permissions granted to that role.

2. **Types of Roles:** Each identified Role must have an accompanying account, permission group, or other configuration which defines the access permissions an individual with that Role will have with respect to the Information Resources. Roles and accounts should be pared on a one-to-one basis. Multiple accounts may have the same access permissions to an Information Resource if necessitated by their accompanying Roles.

3. **Least Privilege:** Assignment of permissions and capabilities must be narrowly tailored and follow the Principle of Least Privilege. Each individual, Role, and account may have only the minimum level of access required to perform their authorized function.

   For example, a normal desktop user should not have administrator-level access on their machine and should not be able to change basic system settings or install new software; similarly, a web application should not be run with administrator rights (or root in the Linux/Unix context) to the operating systems on which it runs. At a minimum, Information Resources must have the following separate Roles and associated Accounts defined by EOTSS standard *IS.003 Access Management*:

   a. User Account
   b. System (or Application) Account
   c. Service Account
   d. Administrator (or Root) Account
   e. Firecall (or breakglass/emergency recovery) Account

4. **Ability to Review Access Controls:** All Information Resources must have a type of account (included in or in addition to the above) that is capable of reviewing lists of all individuals authorized to access an Information Resource and the accounts assigned to those individuals.

5. **Limit and Audit Privileged Accounts:** For any Accounts or Roles that have broad access to information or the ability to modify Information Resource operations (“privileged” accounts or roles), Owners must develop a mechanism to ensure that (a) account creation and use are expressly authorized based on well-defined criteria; (b) accounts are limited to the individuals whose function requires broad privilege; (c) account creation and use is tracked and auditable; and (d) appropriate mechanisms are in

place to timely offboard privileged accounts. For example, an employee providing desktop support may need to be able to elevate to administrator-level access on workstations in the group they support, but should not be able to use administrator-level access on workstations in areas of the organization they do not support, nor on servers administered by a separate group.

6. **Logical Separation:** Accounts must ensure logical separation of access to different components and data within the Information Resource based on Role. That logical separation must ensure that accounts and individuals have only the minimal amount of access necessary to fulfill their business and technical requirements. Additionally, Owners must ensure that such access constraints are uniformly enforced (across Information Resources and in each instance of access). Access must be constrained, procedurally or logically, in a way that ensures that account holders are generally prohibited from:

    a. Passing information to unauthorized individuals;
    b. Inappropriately downloading or saving information;
    c. Inappropriately passing information to other Information Resource components;
    d. Sharing account information or otherwise granting their account privileges to others;
    e. Changing security attributes to data, Information Resources, or Information Resource components;
    f. Changing security attributes for newly created data or Information Resources; or
    g. Changing how access control is governed.

    Notwithstanding the foregoing, Owners may define privileged accounts which do permit some or all of the above if business requirements warrant.

ii. *Assigning Accounts*

Information Resource Owners are responsible for developing, documenting, implementing, and auditing the processes for assigning Roles and accounts. These processes must meet the following requirements:

1. **Documented Process:** Owners must ensure that there is a documented process for approving, creating, modifying, monitoring, and terminating accounts and/or Roles in the Information Resource. Such process must account for:

    a. Defining who can approve the creation of new Roles and types of accounts;
    b. Defining who can approve the creation of new accounts for individuals, modifying existing accounts, and terminating accounts;

c. Defining how monitoring of accounts in and access to the Information Resource occurs; and
d. Defining the conditions under which accounts and Roles can be created, enabled, modified, disabled, and/or removed.

In addition, the process should identify the roles of one or more individuals responsible for approving, administering, monitoring, and terminating access to the Information Resource. The individual(s) must be readily identifiable upon request. If the individual(s) are not, that role will default to the applicable ACIO.

2. **Change Documentation:** With respect to account creation, modification, and termination, Owners must ensure that they receive appropriate and timely information to support a change with an account. It is the shared responsibility of Owners and the individuals best suited to know when an account should be created, changed, or decommissioned. Such individuals may include the end user, the end user's manager (if applicable), the end user's organization (if a third party), human resources, and others. Owners should determine what information sources are most appropriate to support account determinations and coordinate appropriately to receive that data. Account creation, modification, and termination cannot occur spontaneously and must be (a) supported by request documentation; and (b) recorded when such action is taken.

3. **Least Privilege with Multiple Accounts:** Some individuals may have different Roles with respect to the Information Resource and, therefore, multiple different sets of access rights. Owners should ensure that individuals accessing the Information Resource utilize the account or access rights associated with the Role being performed. For example, if an individual is both an administrator and developer for an Information Resource (where they have greater access rights as an administrator), that individual must only use the administrator access for their administrator Role and not for their developer role. Users are also responsible for ensuring that they do not misuse their more privileged accounts to perform work inappropriately in a Role for which they do not require a heightened level of access. Under no circumstances may a user access or fulfill a non-privileged Role with a privileged account. All activities undertaken with a Privileged account must be logged, and such logs either (a) shared automatically with EHS log-correlation service; or (b) maintained for at least 180 days.

4. **Identification & Authorization:** All Information Resources must require identification and authorization procedures for users to access the Information Resource. Access to Information Resources must require controls such as user credentialing and passwords meeting EOTSS and EOHHS standards. For legacy Information Resources not requiring identification and authorization procedures, a supplemental security plan must be provided which explains why user actions do not require

identification and authorization and which demonstrates compensating controls for user authentication.

5. **Central Identity Management:** Wherever possible, Information Systems shall be designed and implemented to use central identity management services (IDM) provided by EOHHS or the Commonwealth, such as Active Directory, LDAP, or web-based authentication protocol. Owners are free to use groups/roles defined in the IDM system, or to use IDM only to authenticate users, managing and assigning roles entirely within their Information System.

6. **Logging of Identification Attempts:** Every login attempt, whether successful or rejected, and whether or not using a central identity management service, must be logged. Wherever possible, these logs must be shared automatically with EOHHS log-correlation services, such as SolarWinds, and unless such log forwarding is in place, Information System Owners are responsible for maintaining the identification logs for at least 180 days. Wherever possible, these logs must include source IP address or other source-identifying information.

iii. *Access to Information and Data Management*

Information Resource Owners are responsible for ensuring appropriate access to information and management of the data in their Information Resource. Those Owners must ensure implementation of the following requirements when managing data within their Information System:

1. **Information Sharing:** Information within an Information Resource should not be shared outside of that Information Resource unless the data recipient abides by the requirements outlined and referenced in these *EOHHS Enterprise Information Security Standards*. With respect to determinations in the EOHHS Environment, the EOHHS Security Office is undertaking application risk assessments and gap analyses. Consequently, the EOHHS Security Office has determined that EOHHS is making progress toward a generally effective control environment. As such, information sharing within EOHHS and among EOHHS Information Resources is deemed appropriate based on information security considerations. Owners must still take care to ensure appropriate custody of their information. Owners must continue to ensure that sharing of data external to EOHHS is appropriately evaluated against these standards, documented, authorized, and supported by written agreement holding external parties to at least the same standards required of EOHHS, including compliance with relevant Third Party Agreements.

2. **Protect Data Transmission:** Owners must enforce appropriate control over the transmission mechanisms for data. Some data must be encrypted before being transmitted outside an Information System, outside the EOHHS Environment, or outside the MAGNet environment. When

transmitting data outside of the EOHHS Environment or interfacing with an Information Resource outside of the EOHHS Environment, Owners must establish and document rules and procedures governing data transmission, processing, and storage. See *Section XVI, System and Communications* for more information.

3. **Oversee and Manage Authorizations:** Owners must also facilitate information sharing by maintaining oversight of Information Resources. Authorized administrators of access must determine whether access to its Information Resources is appropriate, based on but not limited to, the user's roles, business justifications and other standards consistent with those outlined herein. When applicable, Owners may employ either automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

4. **Previous Logons:** Owners must ensure that the Information Resource notifies the user, upon successful logon and/or access to the system, of the date and time of the last successful logon and/or access.

5. **Concurrent Sessions:** Owners must ensure that the Information Resource limits the number of concurrent sessions for each Role and account to one concurrent session, unless required by business, programmatic, or technical need. For any account, role, or Information Resource that allows multiple concurrent sessions, Information Resource Owners must (a) document why this is allowed; and (b) ensure that auditable events (including successful logins, re-authorizations, file additions/modifications/deletions, and changes to security attributes) are traceable to a specific session.

6. **Session Time-Out:** All Information Systems must automatically terminate a user's session (timeout) and conceal or remove information displayed on-screen after no more than 15 minutes of user inactivity. Upon session termination, the user must be required to reenter credentials to reestablish access to the Information System.

7. **Protect Physical Information Resources:** Owners must develop and enforce policies governing physical copies of data, including practices for the creation and distribution of physical copies of sensitive data, consistent with the Secretary of State's Record Retention Schedule. Access to physical Information Resources must be controlled based upon requirements provided by the Business Owner. If physical copies are required, Owners must ensure that they are maintained in a locked and secure environment accessible by key, badge swipe, PIN-entry pad, guard, or other authorization mechanism. Paper documents containing sensitive information may not be left unattended in the open where they can be easily taken. If electronic sensitive information is printed or otherwise converted into paper-based sensitive information, it must be printed to a non-publicly-accessible location and must be picked up immediately. Sensitive information in

physical Information Resources may not be left unattended, especially in public spaces or shared office settings. Owners must be cognizant of more restrictive compliance requirements under various Third Party Agreements, depending on the type of data contained within an Information System.

8. **Minimize Duplication of Electronic Information:** Owners must restrict the creation of unnecessary or duplicative collections of sensitive information and ensure that non-authoritative electronic copies of Information Resources are securely deleted or destroyed as soon as they are no longer needed. Such electronic files should never be stored locally on a user's computer or on shared drives, calendars, collaborative tools, external parties' systems, or anywhere on the internet without prior authorization.

9. **Control the Release of Information:** Prior to releasing information pursuant to a public records request, litigation, or other similar request for data, Owners must engage trained EOHHS staff who are authorized to post information onto a public-facing system or application or release data to the requesting third party. These trained individuals must review the proposed content to ensure that the proposed release does not contain nonpublic information, and if it does, remove or redact such information such that it cannot be recovered from the publicly released information.

10. **Automate Key Account-Management Practices:** Within one (1) calendar year of the issuance of this Document, Owners must certify and demonstrate that the following account management functionality has been automated:

    a. Information Resource account management – this can include measures like automated emails notifying Owners when users are terminated or their roles change, necessitating a change in their account, monitoring of account usage, automated alerts around atypical account usage, etc.
    b. Automated removal of any temporary accounts, which also includes any "emergency" accounts that may be created.
    c. Automatic disabling of Information Resource accounts that are inactive for 60 days or more and that meet other criteria, defined by the Owner, for account inactivity.
    d. Automatic auditing of account creation; modification; enabling, disabling, and removal action. Additionally, Information Resource rules must be created to distinguish between appropriate and inappropriate action and which will be used to automatically notify the Owners of inappropriate actions.
    e. Automatic logging and auditing of all privileged account activity, as well as the execution of privileged functions.
    f. Automatic prevention of non-privileged users from executing privileged functions. This should include the inability to circumvent, disable, or otherwise modify systems and functionality designed to

protect an Information Resource from modification, improper access, other malicious activity, and accidental harm.

11. **Data Mining Protections:** Within one (1) calendar year of the issuance of this Document, EOHHS must gauge the feasibility of, and employ if feasible, techniques to detect and prevent unauthorized data mining within Information Resources. These techniques should be designed to protect against users' unauthorized discovery and extraction of anomalies, patterns, and correlations within large data sets. They may include, but are not limited to: limiting the types of responses provided to database queries, limiting the allowed frequency of database queries to increase the work factor needed to extract or infer information from such databases, and notifying appropriate personnel when atypical database queries, accesses, or workloads occur.

iv. *Access Reviews*

In order to support and enforce these standards, Owners must ensure implementation of periodic access reviews for each of their Information Resources, taking into consideration the following standards:

1. **Personnel and Procedures:** Owners must ensure that sufficient personnel, procedures, and systems are in place to effectuate the access controls they adopt. Access enforcement will be based on the decisions of these authorized systems or individuals.

2. **Review Schedule:** Information Resource access must be reviewed and updated to reflect changes to operational, business, or IT requirements, based on the following schedules:

    a. **Annual Policy Review:** All Information Resource access policies and procedures must be reviewed at least yearly.
    b. **Annual Access Log Sampling:** A random sampling of Information Resource accounts must be reviewed (audited) at least once annually to ensure that access was (i) granted; and (ii) used appropriately. Such review must be designed to verify to a high degree of certainty that appropriate processes were followed and access grants were proper.
    c. **Unused Accounts:** Information Resource accounts must be reviewed (manually or automatically) at least every 60 days to determine whether or not such accounts are still actively in use. Accounts that have not been used within the past 60 days must at least be disabled to prevent access using that account. Managers should determine a timeline and process for documenting and re-enabling such disabled accounts based on criteria such as legitimate business need, including being notified by the account holder that they still require use of the account. Managers must determine a

timeline for deletion of disabled accounts that remain unused; however, such timeline may not exceed 180 days.

d. **After an Event:** Access control policies and procedures must be reviewed and updated for any Information System or Resource identified by the SCIO or appropriate ACIO as having been involved in an Event.
e. **As Needed:** Access control policies and procedures must be reviewed and updated as needed, as systems, roles, and personnel change.

v. *Wireless and Remote Access*

Owners of any Information Resource or Information System that is accessible via a wireless connection, from a mobile device, or from outside MAGNet (e.g., from the internet) ("remote availability") must establish controls for all such wireless, mobile, and remote access connections, including:

1. **Documented Authorization:** Documented usage restrictions, configuration requirements, and procedural guidance must be put into place before making the system remotely available, including per-user and per-device authorization processes to be completed prior to granting remote or wireless access.

2. **Minimum Necessary Amount of Wireless, Mobile Device, and Remote Access:** Access to wireless, mobile, and remote-access connections must be limited to the minimum amount necessary required to accomplish the authorized function. Instances in which remote users are granted access to privileged data must be documented with the business justification for the level of access.

3. **Monitoring:** Manual and/or automated processes that manage, monitor and track all remote accesses through audit logs and network access control points.

VII. AUDIT AND ACCOUNTABILITY

a. Purpose and Introduction

In support of access control monitoring and ensuring the confidentiality, integrity, and availability of Information Resources, Owners must ensure that they are able to assess and verify who accessed what with respect to their Information Resources. The controls outlined herein are predominately targeted at Information Systems, but physical Information Resources should be similarly safeguarded to the extent feasible.

b. Policy Statement

All EOHHS Information Resources must have records for access to those resources managed and reviewed by Owners to ensure only appropriate and authorized access to Information

Resources occurs. Information Systems must generate logs which are capable of being absorbed by Commonwealth and EOHHS enterprise logging tools. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

c. Audit and Accountability Standards

i. *Audit Events*

At a minimum, records for access to information Resources must identify:

1. Who accessed the Information Resource,
2. When the Information Resource was accessed,
3. What was accessed,
4. Whether or not data was taken (appropriately or inappropriately),
5. Whether or not any modification was made (for Information Systems), and
6. From where the access occurred (for Information Systems, if applicable).

These six pieces of information will provide a sufficient baseline for Information Resource Owners and the EOHHS Security Office to determine if improper access was made to an Information Resource and its data.

Owners must also determine what events will trigger automated alerts. Some of those events are outlined in *Section VI, Access Controls*. At a minimum, Owners must identify rules and methods for identifying the following events:

1. Disruption of Service (DOS) and Distributed Disruption of Service (DDOS) attacks;
2. Brute forcing passwords through excessive log-on attempts; and
3. Unauthorized exfiltration or access of data through indicators like file transfer size or volume of access, timing, irregular account usage, and other indicators.

Owners must also implement active monitoring for all administrative or otherwise privileged accounts which permit read access to all data in an Information System or modify access to some or all of the Information System.

Owners must develop such rules as soon as reasonably practicable, but no later than: 1) the EOHHS Security Office requests such information when implementing aggregated logging for existing Information Systems or 2) upon deployment of a new Information System to production. These events and audit rules must be reviewed and confirmed or updated annually to ensure new perceived threats are appropriately monitored.

Owners must ensure that all audit logs contain a timestamp for creation of the log of the event. All such logs must be recorded in Eastern Standard Time.

ii. *Storage Capacity and Review*

The EOHHS Security Office will only maintain audit logs in an aggregated logging system for events that generate an alert and will maintain such records for sixty (60) days. All other audit logs will be maintained on an as-needed basis and the oldest audit records which have not generated an alert will be deleted on an as-needed basis to free storage.

The EOHHS Security Office will perform an initial review of all alerts to ensure that the alert is genuine. In the event it is, the alert will be forwarded immediately to the Owners of the Information System generating the alert. The EOHHS Security Office will also mobilize its forensic and incident response units to address any potential malicious activity. If appropriate, the EOHHS Security Office will also report incidents to EOTSS pursuant to *Section XI, Incident Response and Security Incident Response Team*.

Owners are encouraged, but not required to, keep logs for longer. In the event an application has not been ingested into an aggregated logging system, within one (1) year of promulgation of these *EOHHS Enterprise Information Security Standards* Owners must produce, review, and store logs as outlined in this *Section VII, Audit and Accountability* and produce a copy of events that generate an alert to the EOHHS Security Office within twenty four (24) hours of generation of the alert for review and analysis.

iii. *Audit System Integrity and Failures*

Audit logging systems employed in the EOHHS Environment must be developed consistently with these standards to assure the integrity of data and security of that system. Access should be provided consistent with the principles of least access. Audit logging systems must also be monitored to verify the continued integrity of generated audit files and events. Such logging must be performed in a way that review of any audit log does not modify the original content or time ordering of those logs. In the event an audit logging system is compromised, an alert must be generated notifying the Owner of such event. In the event an audit logging system fails, the audit logging system should be stopped, flushed, the source of the failure identified and repaired, and then restarted.

iv. *Additional Requirements for Systems Accessing Internal Revenue Service Federal Tax Information*

Owners are responsible for developing procedures defining access requirements and protection of audit information among external organizations when audit information is transmitted across agency boundaries. This requirement applies to outsourced hosting with data centers or cloud providers.

VIII. INVENTORY AND CLASSIFICATION

a. Purpose

The purpose of this Document is to outline both the need and the method for carrying out an inventory of EOHHS's applications and information. This Document is intended to satisfy Steps 1, "Categorize Information Systems" of the National Institute of Standards and Technology ("NIST") Risk Management Framework Security Lifecycle.[2] Furthermore, the processes outlined herein was drafted to conform to the precepts outlined in Federal Information Processing Standards ("FIPS") Publication ("Pub") 199, *Standards for Security Categorization of Federal Information and Information Systems* and NIST SP 800-60, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*.

FIPS Pub 199 outlines that an information system inventory and classification is necessary to mitigate the potential impact of a loss of confidentiality, integrity, or availability. For clarification:

i. A loss of confidentiality is defined as, "the unauthorized disclosure of information."[3]
ii. A loss of integrity is defined as "the unauthorized modification or destruction of information."[4]
iii. A loss of availability is defined as "the disruption of access to or use of information or an information system."[5]

The Security Office has been tasked with preserving the confidentiality, integrity, and availability of all data used or maintained by the Secretariat. It will accomplish that goal through the implementation of administrative, physical, and technical safeguards. The exercise outlined in this Document is the critical foundational step to implementing such safeguards with respect to Information System resources. It represents the first step toward compliance with requirements imposed by law, agreement, or otherwise.

The information and system classification serves two purposes. First, it makes EOHHS aware of what data is in use, maintained or transmitted and where that occurs. Second, it is designed to direct the implementation of controls that have been determined to reduce the likelihood of a loss of confidentiality, integrity, or availability of EOHHS data. This is one of many tools that will be used to safeguard EOHHS data. It should, however, be noted that these tools will not completely prevent the loss of confidentiality, integrity, or availability of EOHHS data and that constant vigilance should be exercised to mitigate threats to EOHHS data.

---

[2] National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013), at 8.
[3] Federal Information Processing Standards ("FIPS") Publication ("Pub") 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004), at 2.
[4] *Id.*
[5] *Id.*

While this *Section VIII, Inventory and Classification* is drafted with a focus to classifying and inventorying Information Systems, the process outlined herein can (and arguably should) be applied to all data the EOHHS enterprise in whatever form it exists and to all processes which utilize data.

b. Policy

All Information Systems in the EOHHS Environment shall be appropriately identified and classified.

EOHHS will accomplish this requirement by ensuring that a Form is completed for all Information Systems. Based on the contents of the Form, the Security Office will assign a classification to the Information System for the purpose of applying appropriate security controls to the Information System to help ensure the preservation of the confidentiality, integrity, and availability of the information contained therein. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Information System Inventory and Data Inventory Standards

The Information System and Data Inventory portion of this Document is designed to provide an overview of Information System functionality, interconnections between a System and other Systems, and types of data contained in a System. This process is generally started by using one of the Forms.

The following process should be followed for every Information System:

i. For all current Information Systems for which a Form has not been completed, the EOHHS Security Office should identify the appropriate Owner to fill out the Form for a specific Information System. If this is a new Information System, the Owner should fill out and update the Form, as appropriate, during system design and submit it to the Security Office.
ii. In the event an Owner identifies that the Form is inappropriate to catalogue information about the Information System, the EOHHS Security Office should work with that Owner to gather the types of information being solicited by the Form (e.g.: data in the Information System, data flows, Information System architecture, vendor access, etc.).
iii. The Owner should fill out the Form, making sure to respond to every applicable question and/or field. All Information Systems in the EOHHS Environment must have a Form completed for them, without exception. It is also critical that the Form reflect the most true and accurate version of information about an Information System.
iv. The EOHHS Security Office and program staff may later determine that a different scope of controls should apply to a system than other than as indicated in the Form due to factors not reflected in the form. However, such a determination will be impossible without the Form being filled out completely and as accurately as possible about an Information System.
v. After receipt of the Form, the EOHHS Security Office will review the Form and work with the Owner to address any outstanding questions.

vi. The EOHHS Security Office will then verify that for the interfacing system table in Question 7 of the Form that every system listed has a completed Form. If not, then the EOHHS Security Office will pursue completion of a Form for the system(s) which lack completed Forms.
vii. The EOHHS Security Office will then assign a categorization level to the system, as outlined in the Information System, Process, and Data Classification Standards immediately below.

d. Information System, Process, and Data Classification Standards

After determining the function and data contained in an Information System, the EOHHS Security Office will assign a classification to that system based on the function and data. The classification will operate as a recommendation of the level of administrative, physical, and technical security controls that the EOHHS Security Office believes applies to the system.

In order to assign a classification to specific information or an Information System, the EOHHS Security Office will use the following matrix:

Data Classification information type/system = {(**confidentiality**, impact), (**integrity**, impact), (**availability**, impact)}

Impact, as used in the matrix, is the potential impact to a system of a loss of confidentiality, integrity, or availability, which can be one of the four following categories:

i. *No Impact* or *Not Applicable (NA)*: this would apply if one of the factors of confidentiality, integrity, or availability do not apply to the data and/or system. For example, a database of public records which is itself a public record would reflect that confidentiality is not applicable.

When applied to determining the impact of a loss of confidentiality, this impact level corresponds to "Low Sensitivity" information, as that term is defined in the EOTSS **Enterprise Information Security Standards: Data Classification** document.[6]

ii. *Low*: As defined by FIPS Pub 199:

The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor

[6] *Enterprise Information Security Standards: Data Classification*, EOTSS, Aug. 25, 2017, http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-information-security-standards.html.

damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.[7]

When applied to determining the impact of a loss of confidentiality, this impact level most closely corresponds to "Medium Sensitivity" information, as that term is defined in the EOTSS **Enterprise Information Security Standards: Data Classification** document.[8]

iii. *Moderate*: As defined by FIPS Pub 199:

The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.[9]

When applied to determining the impact of a loss of confidentiality, this impact level most closely corresponds to "High Sensitivity" information, as that term is defined in the EOTSS **Enterprise Information Security Standards: Data Classification** document.[10]

iv. *High*: As defined by FIPS Pub 199:

The loss of confidentiality, integrity, or availability could be expected to have a severe or **catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening

[7] *Id.* (emphasis in original).
[8] *See Supra* note 6.
[9] See Supra note 7 (emphasis in original).
[10] *See Supra* note 6.

injuries.[11]

When applied to determining the impact of a loss of confidentiality, this impact level would also constitute "High Sensitivity" information, as that term is defined in the EOTSS **Enterprise Information Security Standards: Data Classification** document.[12]

e. The below process will be followed to appropriately classify each Information System in the EOHHS Environment:

i. The Security Office will make an initial assessment of impact level for confidentiality, integrity, and availability based on the data provided in the Form.

ii. The Security Office will then assign an initial classification to the Information System applying the high-watermark principle: the highest impact level assigned to the system will control the overall impact level of the system. Additionally, the Security Office may assign classifications to different stages of an Information System or Process.

Example 1: EOHHS is conducting a procurement. While the procurement team is deliberating, the procurement team group score may be classified as follows:

DC_{scores} = {(**confidentiality**, *moderate*), (**integrity**, *low*), (**availability**, *low*)}
DC_{scores} = moderate

At the conclusion of deliberations, a vendor is selected and the other vendors are made aware of the selection. Any of the vendors may request a debriefing and the procurement team group score is considered a public record. At that time, the score may be classified as follows:

DC_{scores} = {(**confidentiality**, *NA*), (**integrity**, *low*), (**availability**, *moderate*)}
DC_{scores} = moderate

After the period for debriefing has expired, the score is still public records, but the urgency of maintaining such score might be determined to be lower. As such, the score may be classified as follows:

DC_{scores} = {(**confidentiality**, *NA*), (**integrity**, *low*), (**availability**, *low*)}
DC_{scores} = low

Consequently, until the predetermined criteria are met to change the classification (here, the expiration of the debriefing period) the data in the foregoing example should be considered "moderate" impact. Notably, it is considered moderate for different reasons. Prior to selection it is considered confidential, but after selection

[11] *See Supra* note 7, at 3 (emphasis in original).
[12] *See Supra* note 6.

it needs to be available for distribution to respondents. However, after the occurrence of such predetermined criteria the data in the foregoing example may be considered "low" impact because it is neither confidential, nor does it urgently need to be made available.

iii. The Security Office will then report its initial data classification to the Information System Owner. The Information System Owner may review the data classification and suggest modifications based on factors including:

1. Legal or statutory requirements,
2. Factors that may impact the assessment of confidentiality, integrity, or availability of information (e.g.: negative impacts from malicious use of data, reduction of public confidence in EOHHS if the data were inaccurate, etc.)[13]
3. Additional situational considerations (similar to those demonstrated in Example 1, above) or organizational considerations (e.g.: considerations of agency mission, etc.)[14]
4. Data sharing, and
5. Use of the data.

Such modifications will typically increase the initial classification of the Information System or data (or component impacts), but in some cases may justify lowering the initial classification.

iv. After discussion with the Information System Owner, the Security Office will assign a final data classification and categorization to the Information System. The Security Office will report such final data classification to the Information System Owner.

v. The final data classification will serve as the basis for the (1) imposition of security controls on the Information System and (2) the security controls against which the Information System will be audited.

IX. ASSESSMENT AND MONITORING

a. Purpose and Introduction

It is impossible to safeguard an environment where the issues, gaps and vdc xdeficiencies of that environment are unknown. Beginning in September, 2017, the EOHHS Security Office implemented a continuous monitoring program focusing on assessments of information systems, facilities, and operations in the EOHHS Environment.

The purpose of these assessments is to develop a baseline for the implementation of physical, technical, and administrative safeguards for Information Systems designed to

[13] *See generally*, NIST SP 800-60, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories," at 20-23.
[14] *See generally, Id.* at 23-24.

protect the confidentiality, integrity, and availability of information across EOHHS. The assessments are based on the controls outlined in NIST SP 800-53, r4.

These assessments rely on the efforts of innumerable EOHHS staff, the EOHHS Security Office, and external vendors. While the EOHHS Security Office strives to completely address the needs of the EOHHS enterprise, the sheer size, magnitude and complexity of the enterprise may impact the ability to do that. Owners are encouraged to perform self-assessments using the mechanisms outlined herein. Copies of all assessments should be provided to the EOHHS Security Office as soon as reasonably practicable.

Assessments performed by the EOHHS Security Office are effectively independent. The Security Office creates standards for the EOHHS enterprise, but is not responsible for enforcement or implementation of those standards. Additionally, because members of the EOHHS Security Office do not report directly to ACIOs or Agencies, those entities will be organizationally unable to impact the impartiality of the EOHHS Security Office.

b. Policy Statement

All EOHHS Information Systems must undergo assessments based on the controls outlined in NIST SP 800-53, r4. Schedules for such assessments will be determined as further outlined in this *Section VIII, Assessment, Authorization, and Monitoring*. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

c. Assessment, Authorization, and Monitoring Standards

i. *Assessment Process*

1. The EOHHS Security Office will work with Agencies, the ACIOs and CISO to determine Secretariat priority for assessments to be conducted by the EOHHS Security Office. The EOHHS Security Office shall maintain a list of assessments and indicate progress of such assessments for the purpose of reporting progress on such assessments. Information Systems identified for assessment will be chosen based on criteria outlined in the Form.

2. To initiate an assessment, the EOHHS Security Office will conduct a kickoff meeting with application support staff, facility management, or Agency management. Typically, an assessment questionnaire is provided to staff immediately prior to, at, or after this meeting.

   The assessment questionnaires are designed to provide a comprehensive view of the EOHHS, Agency, and application environments based on a review of the NIST SP 800-53, r4 standards.

3. After the kickoff meeting, the Respondents will complete the questionnaire and return it to the EOHHS Security Office for review. In the event the questionnaire is deemed incomplete based on a lack of detail in the responses or if it is missing supporting documentation, the EOHHS Security

Office will engage in an iterative process with Respondents to reasonably complete the assessment questionnaire.

4. Upon completion of the assessment questionnaire, the EOHHS Security Office will aggregate the responses and supporting documentation of the available assessment responses of: EOHHS, Agency, facility, and application. These aggregate reports can take the following representative forms:

    a. Agency and/or Facility Security Plans,
    b. HIPAA Security Risk Assessments,
    c. System Security Plans,
    d. Other forms as required or requested by the Agency

5. Upon completion of an aggregate report, the EOHHS Security Office will review the narrative and supporting documentation in the aggregate report against the NIST SP 800-53, r4 standards. Any perceived deficiencies or gaps will be recorded in a POA&M in a format that identifies, at a minimum:

    a. The kind of gap or defect;
    b. The impact of the gap or defect;
    c. The risk posed by the gap or defect, including the likelihood or magnitude of harm;
    d. Suggested remediation or mitigation of the gap or defect; and
    e. Agreed-upon timelines for remediation of the gap or defect based on the risk of the gap or defect and the priority of remediation and/or resource commitment by the Agency.

6. The EOHHS Security Office will monitor progress on the POA&M with the Respondents on at least a quarterly basis.

7. The EOHHS Security Office will revalidate its assessments on a triennial basis by default. It will revalidate assessments on a biennial basis for APD-funded systems.

ii. *Interconnection Agreements*

Prior to sharing data in any form, internal and external Agencies typically enter into Information Sharing Agreements (ISAs) or other Third Party Agreements with trading partners which outline the security and privacy requirements of any shared data. At a minimum, all ISAs entered into by EOHHS or its Agencies with an entity external to EOHHS must include a reference to compliance with applicable NIST SP 800-53 standards. Internal interconnections are deemed to be authorized based on conformance with these EOHHS Enterprise Information Security Standards. Such interconnections will be recorded based on the Form.

iii. *Monitoring*

The assessment program outlined in this *Section IX, Assessment and Monitoring* is

only one component of the EOHHS continuous monitoring program. The results of those assessments will be correlated with the information generated in *Section VIII, Inventory and Classification*; *Section VII, Audit and Accountability*; *Section X, Authorization to Operate and Operational Risk Assessment*; and any available vulnerability assessments or penetration tests generated by Information System Owners, EOHHS, and EOTSS to ensure that Information Resources are adequately protected on an ongoing basis. The specifics of this continuous monitoring program may be documented in separate desk level procedures. This information will be used by the EOHHS Security Office, including by its forensic and incident response units, to safeguard the environment and to identify and address any potential malicious activity. If appropriate, the EOHHS Security Office will also report this information to EOTSS pursuant to *Section XI, Incident Response and Security Incident Response Team*.

X. AUTHORIZATION TO OPERATE AND OPERATIONAL RISK ASSESSMENT

a. Purpose

The purpose of this section is to outline the process(es) needed to request an Authorization to Operate (ATO) or an Operational Risk Assessment which would assist with promoting a System from Development or Testing to Production where that Information System might not fully meet Commonwealth, EOHHS, and/or an Agency's information security controls. This promotion to Production with a security variance is accomplished in a safe and well-managed fashion by documenting and recording the variance, the vulnerability, the risk to proceed, and any remediation steps. This documentation will provide the relevant decision maker with facts necessary to make reasonably informed decisions about introducing security vulnerabilities into the EOHHS Environment.

Both the ATO and the Operational Risk Assessment are tools that identify the types and severity of Risks that a System as-designed poses to the data it contains and to the broader EOHHS Environment. The ATO is the tool by which business and technical stakeholders for a System can sign off on deploying a new System to production with security vulnerabilities. The Operational Risk Assessment is the tool by which business and technical stakeholders for a System can sign off on promoting changes to a currently extant system to production with security vulnerabilities, assist with tracking and updating ongoing vulnerabilities, and address newly discovered vulnerabilities.

Risk is something that could potentially result in an adverse situation for the Commonwealth. Reputational damage, loss of PHI/PII data, or data corruption are typical outcomes when Risk is taken without additional considerations on how it might be avoided, mitigated or accepted. When Risk appears and/or is identified, it should be carefully reviewed and options researched to assist with any decisions that are made.

Prior to making the determination to deploy a System into Production or implement code changes with known Risks or security faults, the Information System decision maker should perform adequate due diligence, such as obtaining an assessment for operating with Risks by contacting the Security Office for assistance with identification and cataloguing such risks. The Security Office will assist with gathering the options and discuss with Owners and

other stakeholders to help make the risks more manageable.

The Authority to Operate (ATO) permits Agency personnel to understand and accept the Risk of the status of the System at the time of deployment into Production. The sign off will need to come from the Agency's ACIO and corresponding business contact.

An Operation Risk Assessment is intended to document potential risks at the time of deployment of a System to Production or when enhancements, fixes or feature changes are made to an existing environment. The resolution or mitigation of the risks should be documented as part of sign off to ensure they will be addressed. The Operational Risk Assessment will also serve as a documentation and justification document for Auditors and other external third parties to demonstrate a high level of sophistication and thoughtfulness with respect to security vulnerabilities.

An ATO will usually be paired with the Operational Risk Assessment however the Operational Risk Assessment can be completed without an ATO for systems already in Production.

b. Policy

Any System in the EOHHS Environment that has any known Risks when deployed to Production must be appropriately documented via an ATO and/or Operational Risk Assessment. Appropriate steps to address or mitigate a Risk should be considered and done as a function of the development process. In the event that remediation or mitigation measures are not scheduled for timely deployment or change, the ATO and/or Operational Risk Assessment will be elevated for enhanced review. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Authority to Operate and Operational Risk Assessment Standards

The ATO and Operational Risk Assessment processes generally start with an Owner contacting the System and Support Desk and filling out a Project Intake Form to engage the EOHHS Security Office to review the integrity of their System. However, if the EOHHS Security Office has been engaged during the procurement and design process for the System and/or solution, then a Project Intake Form will not be required (as one should have been completed for the overall effort). Both processes follow the same general steps and have been outlined as a unified process with exceptions noted, as applicable, below.

After a Project Intake Form is completed, the ATO process continues when the EOHHS Security Office identifies from the Project Intake form or circumstances surrounding the System implementation process that the Owner will bring a new System online with vulnerabilities. Similarly, the Operational Risk Assessment process continues when the EOHHS Security Office identifies from the Project Intake form or otherwise that the Owner plans to promote System changes to Production which may include vulnerabilities. Where possible, if the Owner anticipates that one or more aspects of the System will not conform to applicable information security requirements or industry best security practices, the Owner should identify what they believe to not conform.

Upon identification that vulnerabilities exist, the EOHHS Security Office will follow the following process:

i. The EOHHS Security Office will investigate how the Owner determined that a System needs to be deployed to Production with security vulnerabilities. This investigation will include, but are not limited to:

    1. A review of potential mitigating steps that could be undertaken, such as a workaround or compensating control that will make up for the security vulnerability; and
    2. A review of the completed and/or updated Gap Analysis Questionnaire. *See* Gap Analysis Questionnaire Process (in process, please contact the EOHHS Security Office for more Information).

ii. The EOHHS Security Office will review the Gap Analysis Questionnaire with the Owner to identify and confirm the vulnerabilities sought to be introduced into Production.

iii. The EOHHS Security Office will draft a Memorandum with the appropriate information for the System at issue. The Gap Analysis will be attached to the ATO and be incorporated therein as of the date of Approval. Based on the vulnerabilities identified, the EOHHS Security Office will list the vulnerabilities and Risks, providing the following information in the Memorandum:

    1. Title of Vulnerability/Risk being captured.
    2. Overview of Vulnerability/Risk being captured.
    3. Recommendations for remediation, if any (including workarounds and compensating controls) and how they might be applied. The EOHHS Security Office may also provide detailed recommendations how they would help mitigate the risk.
    4. Summation of the rating of the Vulnerability/Risk. The Risk will be rated using the standards outlined in the EOTSS policy titled “Information Security Risk Management Standard”, IS.010. Vulnerabilities will ultimately be assigned a rating of “Low”, “Moderate”, “High” and “Critical”.
    5. An aggregate risk rating for the System based on the individual risk ratings. If the aggregate risk rating is found to be a High or Critical, the EOHHS Security Office will inform the Owner and contact the EOHHS Risk Governance Team to determine next steps with respect to ongoing management of the System’s ongoing security posture.

        Note: In the event the aggregate Risks posed by the System will impact data from Secretariats or entities external to EOHHS, the Risks will be escalated to the EOTSS Risk Governance Committee.

iv. The EOHHS Security Office will review the Memorandum with the Owner to mitigate, to the extent possible, any outstanding Risks. While the EOHHS Security Office recommends that Owners attempt to mitigate all Risks, the EOHHS Security Office has determined that the following constitutes generically acceptable levels of

Risk:

Low	No more than six (6)
Moderate	No more than two (2)
High	None
Critical	None

Although the aforementioned levels of Risk are considered generally acceptable, specific instances of Risk may not be.

v. In the event the EOHHS Security Office and Owner are unable to bring the number of outstanding Risks below the levels set as acceptable, or in the event the System has one or more "High" or "Critical" Risks, the EOHHS Security Office will convene the EOHHS Risk Governance Team and escalate the Memorandum to them. The EOHHS Risk Governance Team will review the Memorandum and attempt to make recommendations for options to mitigate some of the more significant Risks to the System.

Note: In the event the Risks posed by the System will impact data from Secretariats or entities external to EOHHS, the Risks will be escalated to the EOTSS Risk Governance Committee.

vi. After reviewing the Memorandum with the Owner and/or the EOHHS Risk Governance Team (or the EOTSS Risk Governance Committee) and receiving approval from either the Owner or the EOHHS Risk Governance Team, the System or its modifications may be promoted to Production. Acceptance should be written, but may occur without written Acceptance in the following circumstances:

1. Promotion of the System to Production without signing the Memorandum, or;
2. Failure by the business and/or technical contact to sign the Memorandum thirty (30) days after: 1) the issuance of the Memorandum or 2) the conclusion of the Risk Governance Team reviewing the Memorandum, whichever is later.

vii. On an ongoing and periodic basis, the EOHHS Security Office will request updates from the Owner about progress to resolution of Risks and vulnerabilities. In the event the Owner is unable to demonstrate meaningful progress to resolution of Risks and vulnerabilities, the EOHHS Security Office will contact the EOHHS Risk Governance Team to determine next steps with respect to ongoing management of the System's ongoing security posture.

viii. By December 1, 2019, Agencies must provide a list of representative for the EOHHS Risk Governance Team that represent the following operational areas and can make decisions on behalf of the Agency with respect to deploying Systems into production with vulnerabilities:

1. Commissioner,
2. Chief Financial Officer,
3. Chief Operating Officer,
4. Agency Chief Information Officer, and
5. General Counsel

Agencies shall update such list on an annual basis, but no later than June 30 of the following year, or when an appointee no longer works for the Agency in the assigned capacity. The EOHHS Security Office will maintain such lists in order to escalate issues and seek approval for promoting vulnerabilities into Production.

XI. INCIDENT RESPONSE AND SECURITY INCIDENT RESPONSE TEAM

a. Purpose

Incident response plays a critical role in any modern enterprise: it provides a mechanism for identifying, stopping, and fixing to the best extent possible any event that could result in a loss of data at an organization. This function has become more critical than ever. Modern business technology has moved beyond its formative stages, where data was maintained and accessed only on desktops in a building. Smart phones, laptops and other portable devices have extended the electronic footprint beyond specific, well-defined physical locations, making information readily available on the go. The proliferated number of endpoints provides many points of entry into a network, which has resulted in an increase of both attempts and successful cyber-attacks from individuals, corporations and organizations looking to gain access to confidential or proprietary data. The complexity of mobile technology and modern interfaces further adds to the burden of ensuring communications and information is not compromised.

This *Section XI, Incident Response and Security Incident Response Team* ensures that an organized and repeatable response can be undertaken immediately when a Security Incident is reported. This Document provides clearly defined processes and procedures that the Security Office and its Security Incident Response Team (SIRT) will use to respond to Security Incidents and ensure that proper handling of the Security Incident and evidence thereof is maintained. The SIRT will investigate a Security Incident; attempt to determine root cause of the Security Incident; manage the Security Incident until it is mitigated, minimized, or stopped; and provide after-action assistance such as an after-action report and/or analysis and provide recommendations to increase security and training activities to mitigate risk on an ongoing basis.

This *Section XI, Incident Response and Security Incident Response Team* defines the minimum acceptable requirements at EOHHS for a Security Incident response. Agencies may have their own related documentation but may not undertake any action or documentation (explicitly identified as such or not) to supplant these standards or process. These standards and process are intended only to cover Incidents which result in impacts to the confidentiality, integrity or availability of data. These standards are not intended to cover incidents which cause physical unavailability of a site, such as because of damage to physical infrastructure, natural disaster, or other physical impacts. These standards are intended to work alongside a physical incident response plan to ensure resumption of data access as quickly as possible.

Additionally, Agencies may also have continuity of operations/business continuity plans in place. Those plans should be intended and designed to address impacts to business operations caused by unavailability of a location or resources. They should not deal with the underlying cause of the lack of access to data, which is the scope and purpose of these standards or a physical incident response plan.

Notwithstanding any statement in these *Enterprise Information Security Standards* to the contrary, while this *Section XI, Incident Response and Security Incident Response Team* activities relate to Agencies' privacy incident response activities, these standards are intended to work in conjunction with Agencies' privacy incident policies/procedures/protocol and should not be construed to replace or supersede those privacy documents. The EOHHS Security Office will make all efforts to appropriately collaborate with Agency privacy offices when a Security Incident arises.

In no event should any EOHHS staff member attempt to address a Security Incident themselves outside of the scope of this *Section XI, Incident Response and Security Incident Response Team*. Any EOHHS staff member that takes any action or inaction that exacerbates the duration, coverage, magnitude, impact or any other quality of an Incident, whether intentionally or unintentionally will be considered a malicious actor with respect to the Incident. In the event that any EOHHS staff is found to be a malicious actor with respect to an Incident, those staff may be disciplined. Such discipline may include limitation of or removal of rights to access Information Resources, suspension or termination of employment, or civil and criminal penalties such as fines and incarceration.

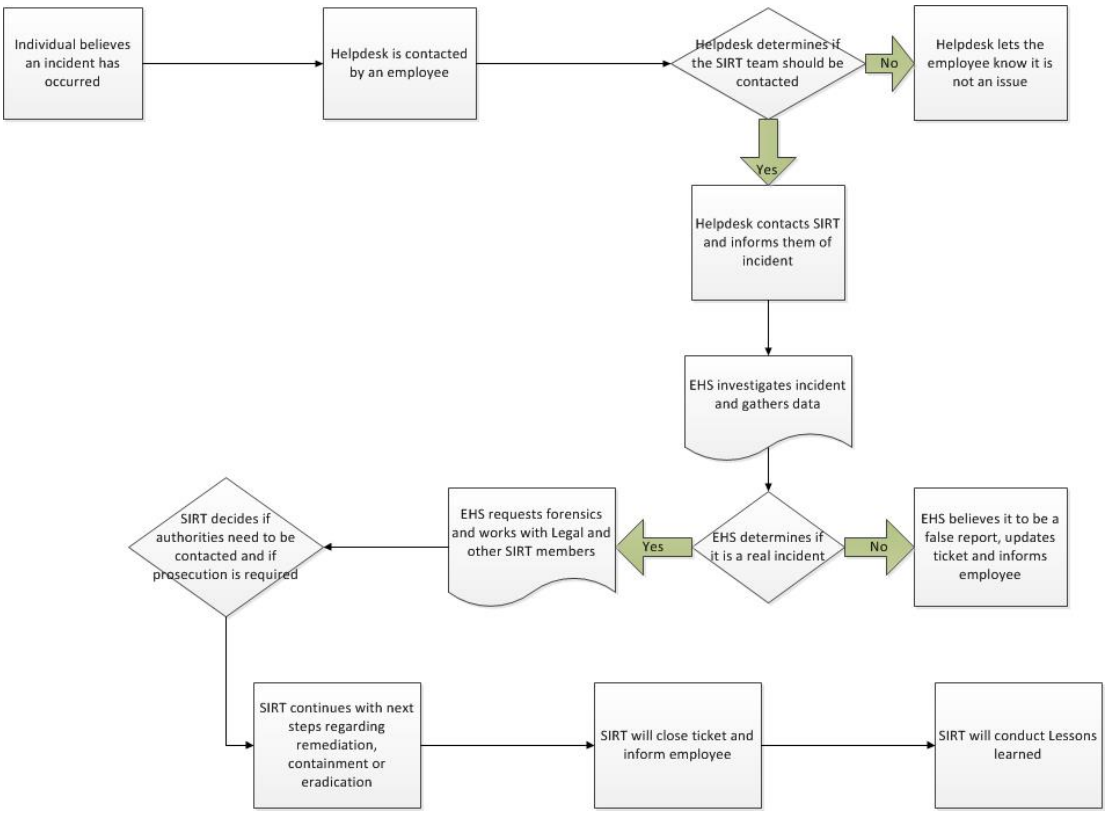
b. Policy

All Reportable Events must be reported, handled, and remediated pursuant to the terms of this *Section XI, Incident Response and Security Incident Response Team*. Agencies must designate individuals who may be contacted in the event of a Reportable Event and who are capable of serving on the SIRT until closure of the Reportable Event. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Incident Response and Security Incident Response Team Standards

i. *Overview of Reportable Event Handling*

The following chart outlines the workflow for how a Reportable Event will be addressed:



ii. *Identification of Reportable Events*

There are a number of ways that a Reportable Event may be identified. While it is impossible to list every possible situation or activity that may be or give rise to a Reportable Event, this document will strive to provide sufficient guidance to make Reportable Events readily identifiable. **As a rule, over report. When in doubt, report.** The EOHHS Security Office will help you identify a Reportable Event and will inform you if the event you reported was not, in fact, a Reportable Event.

Reportable Events fall into two different groups:

- Group 1: ongoing Security Incidents
- Group 2: events that demonstrate environmental weaknesses that could lead to a Security Incident and need to be fixed.

Group 1 is largely reactive. In a Security Incident, Information Resources have already been compromised either through confidential information being given to the wrong party thereby impacting the confidentiality of the data, being unavailable to the people who need them, or when the data is inaccurate such that people who need data are unable to get the right data. Therefore, in a Security Incident, damage has already been done to Information Resources or business processes. Addressing that damage involves stopping the spread and impact of the Security Incident (which could be a current or pending loss of data) and restoring the confidentiality, integrity, and availability of Information Resources as best as possible.

Some examples of Security Incidents are as follows:

- Loss of a mobile device(s) such as laptop, tablet or phone that is unencrypted
    - For encrypted devices, the System and Support Desk should be following their own lost device remediation plan which includes remote wiping of device
- Widespread malware/virus infection
- Confidential information disclosed, altered or destroyed
- Unauthorized changes to system hardware and/or software
- Unauthorized probing or scanning of Commonwealth systems or network
- Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks

Occurrence of nature which requires mobilization of the business continuity team Group 2, which convenes when Reportable Events might not rise to the level of a Security Incident, is largely preventative in nature. The best way to stop a Security Incident is to ensure it never happens. Therefore, the group of Reportable Events covered by this *Section XI, Incident Response and Security Incident Response Team* is broader than just Security Incidents. Reportable Events include any Event in the EOHHS Environment that highlights the potential for a Security Incident to occur. By including this group of Events in the definition of a Reportable Event, the EOHHS Security Office can work to prevent Security Incidents in the EOHHS Environment and/or minimize the potential damage from Security Incidents.

To provide a tangible example of what might constitute a Reportable Event, both of the following situations are Reportable Events:

- someone enters an EOHHS location and steals an EOHHS Information Resource (e.g.: pulling a computer off of a desk and walking out the door with it)
- someone enters an EOHHS location and steals personal property (e.g.: rummaging through peoples' personal effects to take wallets)

In the first situation described above, there is a loss of an EOHHS Information Resource and that Information Resource may also contain sensitive data. In that case, the Security Office has an important role in working with relevant parties to identify how the computer was taken, recover the computer and/ or recover or prevent the dissemination of the data, and ensure that the Security Incident does not reoccur in the future.

In the second situation described above, there is no indication that EOHHS Information Resources have been impacted. However, the situation demonstrates certain vulnerabilities in the environment that permitted the individual to enter an EOHHS location and the target of the theft could have been EOHHS Information Resources. Therefore, in an effort to safeguard EOHHS Information Resources, the latter Event, while not a Security Incident, is a Reportable Event that will be reviewed by the Security Office.

Some EOHHS operations groups use the term "incident" outside the scope of this *Section XI, Incident Response and Security Incident Response Team*. Therefore, such "incidents" are not within the scope of these standards, though they may be required to be reported under other processes. Examples of such "incidents" are:

- Network or server outages at a site unrelated to a DDOS or other attack/action from a third party
- Power outages at a site

Additionally, some Reportable Events which are required to be reported under this policy must also be reported under other policies, such as Agency Privacy Policies. Individuals reporting any Events under this *Section XI, Incident Response and Security Incident Response Team* must ensure that they appropriately report such Events to other groups as necessary.

iii. *Reporting a Reportable Event*

All Reportable Events must be reported to the EOHHS System and Support Desk immediately upon discovery. **You can contact the EOHHS System and Support Desk at (617) 994-5050 or at the email addresses available at http://eohhs-web.ehs.govt.state.ma.us/IT/agency-email-addresses.asp**. As time is of the essence during most Security Incidents, managers or Agencies shall not implement administrative processes that delay reporting of a Reportable Event and which may serve to exacerbate a Reportable Event. Examples of such administrative processes are internal programmatic, department and/or Agency reporting requirements and escalation prior to reporting the Reportable Event to the EOHHS System and Support Desk.

In some situations, a Reportable Event may constitute a Privacy Incident which is reportable to Agency legal counsel, privacy official or other designated contact under an Agency's privacy or security policy. In this case, you should report the Reportable Event to both the EOHHS System and Support Desk under this *Section XI, Incident Response and Security Incident Response Team* and to Agency legal counsel, privacy office or other appropriate official, who will cooperate with the SIRT in their response.

In some situations, a Reportable Event may also require contacting emergency services due to an immediate danger (e.g.: dialing 911 for police or fire). In the event a call to emergency services is necessary, notwithstanding the prior statement to call the EOHHS System and Support Desk first, the reporter shall first call emergency services and when the reporter is out of danger, call the EOHHS System and Support Desk.

The EOHHS System and Support Desk will then open a "Security Incident" ticket and assign it to the ENT.SEC.CSO queue.

iv. *Secretariat Incident Response Team*

Upon assignment of the "Security Incident" ticket to the ENT.SEC.CSO queue, the Security Office will review the ticket and may contact the submitter to determine whether or not the ticket describes a Reportable Event. If the ticket does not, then the Security Office will close the ticket. If the ticket does, then the Security Office will mobilize the core SIRT, composed of the following individuals from the Security Office with the following roles and responsibilities:

- Incident Response Lead / Coordinator - During resolution of the Reportable Event, the Incident Response Lead is tasked with project coordination and ensuring successful resolution and/or remediation of the Reportable Event. Activities in furtherance of those goals may include, but are not limited to: identifying the Reportable Event, triaging resolution of the Reportable Event, coordinating and liaising between relevant groups involved with resolving the Reportable Event, and engaging in appropriate closeout activities for the Reportable Event. When a Reportable Event is not underway, the Incident Response Lead will be responsible for improving EOHHS security; developing desk level procedures to ensure appropriate implementation of this *Section XI, Incident Response and Security Incident Response Team* with Agency stakeholders in order to appropriately address Reportable Events; working towards minimizing the occurrence of a Reportable Event; and working with groups throughout EOHHS to familiarize those groups with and test and operationalize the processes outlined in this *Section XI, Incident Response and Security Incident Response Team*.

In consultation with the Secretariat Security Liaisons and Forensic Analysts, the Incident Response Lead will identify the extent of the Reportable Event and make a determination if resolution of the Reportable Event requires mobilizing a broader SIRT or if the Security Office is able to resolve the Reportable Event. The conditions for mobilizing a broader SIRT will be outlined in relevant Security Office desk level procedures implementing the precepts of this *Section XI, Incident Response and Security Incident Response Team*.

In the event a broader SIRT is required:

1. Agencies must designate and provide to the EOHHS Security Office appropriate points of contact at the Agency who are able to direct on-the-ground identification, containment, and remediation efforts, if required, and secure staff participation and cooperation in identification, containment, and remediation. Agencies may designate whomever they wish, but the EOHHS Security Office recommends representatives from the following (and/or their delegates):

    - Agency Operations,
    - Finance,
    - Site and/or Office Managers,
    - Agency Legal,

- HR and Labor Relations,
- Agency Communications, and
- Agency Privacy Counsel and/or Privacy Officer (where applicable to the extent this is also a privacy incident).

2. EOHHS IT Operations must designate appropriate points of contact who are able to direct and implement on-the-ground identification, containment, and remediation efforts who should include the following:

   - IT Site Manager and/or Regional Operations Manager,
   - Server Administrators, and
   - Network Administrators.

   The SIRT has numerous purposes with respect to resolution of an incident. The SIRT can:

   a. effectively coordinate and communicate required actions for incident response and remediation,
   b. keep Agency and IT leadership updated about status of investigation and resolution of an incident,
   c. quickly course-correct management of investigation and remediation of an incident, and
   d. ensure all stakeholders are able to quickly and effectively remove any barriers to remediation of an incident.

   Within 30 days after the start of a state fiscal year, Agencies must designate the individuals who will participate in the Agency SIRT. Additionally, within 30 days after the start of a state fiscal year, EOHHS must designate the individuals who will participate in an EOHHS SIRT, should the need arise. EOHHS need not identify the IT Operations staff that will participate in a SIRT as the regional and/or office staff will assist with Incident response and remediation. The SIRT lists will be attached hereto as Attachment 9.

v. *Reportable Event Handling – Overview*

After the System and Support Desk opens a ticket and assigns it to the ENT.SEC.CSO queue:

1. The Incident Response Lead will review the ticket, contact the reporting employee and gather additional information to determine if a Reportable Event has, in fact, occurred. (Section XI(c)(vi)(1))
2. If it is not an incident and not a Reportable Event, the ticket is closed by the Incident Response Lead or sent back to the System and Support Desk to be addressed as not a Reportable Event, but an issue that needs to be addressed. If the ticket is closed, the requester will be notified by email.

3. If it is not an incident, but is a Reportable Event, the Incident Response Lead will perform appropriate follow-up with respect to investigation and data gathering, as described in Sections XI(c)(vi)(2) and XI(c)(vii) below.
4. If it is an incident, the Incident Response Lead will determine if it can be handled by the Security Office or if the SIRT must be assembled. The incident will then be managed as outlined further below.
5. The Security Office and/or SIRT investigates and gathers the data for the Reportable Event or incident. Forensics is performed if necessary to determine how the Reportable Event or incident started, has spread, and how best to contain the incident. There will also be a determination if the authorities need to be contacted (if not already contacted) and if additional legal action is required. (Section XI(c)(vii)(1))
    a. Because of the potential for further legal action, the utmost care must be maintained for documenting and preserving the chain of custody of materials to be used as evidence. The Security Office and SIRT should be observing and kept up to date with each transfer of custody of materials.
6. Once the path to remediation is determined, even if the start and spread of the incident has not been identified, the Security Office or SIRT will work towards remediation as expeditiously as possible while being mindful of the identification efforts. (Section XI(c)(vi)(2))
7. Once the Incident is remediated the SIRT will work towards supporting restoration of operations. (Section X.c.viii)
8. Additionally, once the incident is remediated, the SIRT will gather all supporting evidence and document its findings with respect to the incident response and management. The Security Office will maintain the document of record with respect to the incident. (Section X.c.viii)
    a. If the Incident is deemed HIGH IMPACT the report will be provided to the Risk Governance Committee.
    b. The Security Office shall use the documented findings to work towards remediating the identified vulnerabilities, improve its incident detection capabilities, and improve its response.

vi. *Reportable Event Handling – Triaging, Identifying, and Investigating Attack Vector of the Reportable Event*

Related Documents: *EOHHS Incident Chain of Custody Form, EOHHS Incident Evidence Form*

1. The Incident Response Lead will contact the individual who reported the Reportable Event or incident to gather additional details. Those details will be input into the EOHHS Incident Evidence Form and will include foundational information like:

    a. Affected application/website/hardware/software/business process.
    b. Is there any hardware/software affected? Servers or desktops as well as IP addresses should be recorded if this is a DDOS attack.

c. Attack vector, if known – for example, is this a phishing email that triggered the incident?
   A copy of the email should be procured and analyzed in a sandbox environment, if possible. All pertinent details about the email (sender, recipient, external link, etc.) should be recorded.
d. Necessary forensics tools should be identified (a list should be gathered of what is available for use)
e. Affected users. Who is affected by the incident? Internal and external staff? Is the public affected?
f. What environments are affected by the attack?

2. After verifying the details of the Reportable Event or incident the Incident Response Lead, in consultation with other members of the Security Office, will make a determination if the Reportable Event is an incident and if the SIRT should be assembled.

    a. In the event the incident can be managed internally by the Security Office or a slightly broader group of resources, the Incident Response Lead will continue to manage the incident as outlined herein without the SIRT.
    b. In the event the incident is HIGH IMPACT and requires significantly broader management, the Incident Response Lead will contact the SIRT to identify the incident and perform any follow-up with respect to the incident. The SIRT will meet periodically throughout the duration of the incident until resolution of the incident.
    c. The Incident Response Lead will contact the appropriate staff with access to the affected components to continue investigation of the incident:

        i. Application Subject Matter Expert (SME) - In the event the application is compromised (integrity is in question) access to it should be cutoff/read only and business continuity should be evoked
        ii. System Admin – Logs may need to be gathered for the affected system or access frozen
        iii. Network Admin – Logs may need to be gathered. Network traffic monitoring may need to be done. DDOS attack may need to involve a third party such as Akamai for assistance. The Net Admin should be able to provide some information on what protections are in place if any
        iv. Account Operations – if an account is compromised it must be disabled. The manager of the employee will be informed
        v. ITSM – if a desktop/device/server is compromised, the ITSM may need to implement on-the-ground remediation of the desktop/device/server. In the event they are directed to turn over a desktop/device/server for additional review (even in-place), the EOHHS Chain of Custody Form should be utilized. As equipment is shut down and retrieved for

handover for forensic review, the form must be completed by each person involved in moving and/or transferring control of the hardware

d. While the SMEs investigate, the Incident Response Lead will coordinate the investigation effort by ensuring and coordinating that the SMEs have the appropriate access and equipment to investigate. As time is of the essence to appropriately address and remediate an incident, any impediments to investigating the incident must be escalated through the SIRT to the Chief Security Officer and corresponding IT and programmatic management immediately to eliminate the impediment.
e. Once a path to remediation has been identified, remediation should begin. In the event the investigation of the incident and any spread is not completed, remediation should take priority to first contain the incident and minimize any damage from the incident.

vii. *Remediating an Incident*

Incident remediation will be dependent on the findings from the investigation. Below are potential scenarios for this, but each Incident may be handled differently. What is important to note is that the goal of remediation is to prevent the further compromise of the confidentiality, integrity and availability of an Information Resource or location and ensuring that future compromises should not occur due to the same cause.

Incidents and/or Reportable Events will typically fall into one of the following categories and should generally be handled as outlined:

1. Account and/or Location Compromise:

    a. This occurs when an individual(s) steal a legitimate set of credentials for access to an Information Resource or location and use that to access the Information Resource or location. Alternatively, an individual may spoof or hack an Information Resource or location using fraudulent credentials or by taking advantage of latent vulnerabilities.
    b. Any logs or other relevant records related to the access should be reviewed.
    c. Any potential violations of HIPAA or other legal compliance source should be reported to the Agency Privacy Office or equivalent immediately.
    d. Any improper access should be terminated and the source of improper access should be closed such that improper access cannot continue (e.g.: by resetting passwords). Any improper activity should be reversed, to the extent possible, and the proper state of operations should be restored to the extent feasible.

2. Suspicious employee behavior:

    a. This occurs when an employee exceeds the legitimate extent of their access or engages in behavior that will compromise the confidentiality, integrity, or availability of any EOHHS Information Resource.
    b. The Incident Response Lead should ensure that Agency Human Resources and the Legal Department are notified of the inappropriate behavior.
    c. The Incident Response Lead should work with Forensic Analysts to monitor the employee's aberrant behavior and collect evidence with respect to that behavior.
    d. In the event the employee's behavior will lead to an imminent loss of the confidentiality, integrity, or availability of Information Resources, the Incident Response Lead should act to prevent such loss.

3. Application compromise:

    a. This occurs when an individual gains access to an application (including websites) and makes material changes to the operations of that resource.
    b. Application teams may be required to place the application in read only mode in order to preserve integrity or freeze access.
    c. The intrusion vector should be identified and patched, to the extent feasible, to stop continued access.
    d. The application's backups should be reviewed to ensure the backups are verified as good. This is especially critical where, for example, there is a ransomware infection where the infection could be present in backups for days or weeks. The application should then be restored from a verified good backup. In the event a backup cannot be verified as good, then the application should be reconstructed to restore operations to the greatest extent possible.
    e. Application teams should implement business continuity plans with respect to impacted or unavailable service.

4. Information Spillage:

    a. This occurs when an Information Resource transfers information to an individual, group, or other Information Resource without authorization.
    b. The Incident Response Lead will work with Information Resource teams to identify the information involved in the information spill, the scope of the downstream spillage, and any comingling or other impact by the information spill.

c. The Incident Response Lead will work with Information Resource teams to isolate access to impacted Information Resources to prevent unauthorized access to the information spill and additional transmission to other Information Resources.
d. The Information Resource team will work to "scrub" all spilled data from the system to eliminate, to the maximum feasible extent, the presence of spilled data in any application databases (including in backups).
e. The Incident Response Lead will then work with Information Resource teams to verify that the information has been scrubbed and verify the Information Resource is "clean" prior to restoring full access to the Information Resource.

5. Virus Outbreak or Social Engineering Attack

    a. This occurs when malicious code is knowingly or unknowingly deployed in the EOHHS Environment and may range from a single instance of the malicious code to widespread dissemination of the malicious code. This may also occur where someone disseminates information as a result of a seemingly legitimate request for information which is in fact an illegitimate request or from an illegitimate source.
        i. Note that single desktop virus infections will follow the current process that EOHHS IT Site Managers ("ITSMs") have in place to initiate a virus scan and follow its recommendations for remediation unless additional assistance is needed.
    b. These are predominantly isolated incidents which can be handled internally by the Security Office with assistance by ITSMs. Occasionally, the impact will be more widespread, impacting a number of Information Resources. If that occurs, the Incident Response Lead may require the assistance of a broader group of individuals to remediate the incident.

6. Physical Disturbance/Act of God

    a. This occurs when a natural event renders inaccessible some or all of EOHHS's or an Agency's operations and Information Resources.
    b. The impacted Agency or portion of EOHHS should implement their continuity of operations plan.
    c. The Security Office will assist with coordination of the maintenance of the confidentiality, integrity, and availability of impacted Information Resources.

7. The EOHHS Security Office will maintain desk level procedures for handling each category of incident. EOHHS and its Agencies are responsible for and must individually maintain continuity of operations plans in whatever form

they deem appropriate, which outline how operations will continue in the event of the occurrence of any of the aforementioned classes of Incidents.

viii. *Restoring Operations*

EOHHS SIRT Response Form, EOHHS SIRT Incident form, EOHHS SIRT Lessons Learned form

1. Once the incident has been contained, there should be a focus on restoration of business operations

    a. Access to websites, applications, and other Information Resources should be restored from read only.
    b. Equipment should be returned as is or from a new image.
    c. A notice may need to be submitted to the public depending on the incident. A summary SIRT Response Form is attached to this Document as Attachment 6 which can provide guidance on how to respond or what information should be provided.
    d. The Incident Response Lead or their designee should complete the SIRT Incident form to close out reporting on the incident.

2. In conjunction with a restoration of business operations, the Incident Response Lead should work with Agency counsel, privacy counsel, and/or Privacy Officers to:

    a. make a determination about what privacy and security reporting is required as a result of the incident (in accordance with law and contract—outlined pursuant to *Section VIII, Inventory and Classification* and Attachment 2),
    b. complete all required privacy and security reporting, and
    c. make a determination about any remediative or corrective action necessary to satisfy legal or contractual obligations with respect to security and privacy.

3. Scheduling of Lessons Learned should be arranged with all participating and impacted Agencies and staff invited. The minutes from those Lessons Learned meeting(s) should be recorded and kept with the Incident Form for reference. Any changes to any processes, procedures, or Information Resources as a result of the Lessons Learned should be documented, tracked, and followed-up with a future meeting to ensure the change has been implemented as discussed.

d. Testing the Incident Response Plan

On an annual basis, the Incident Response Lead will coordinate with EOHHS and each Agency a tabletop exercise testing the effectiveness of this Incident Response Plan and the continuity of operations plans. Such tabletop exercise will generally include one or more scenarios designed by the Security Office to test the responsiveness of EOHHS and the

Agency with respect to an incident. The process for testing will generally adhere to the following process:

i. At the beginning of the fiscal year (July 1), the EOHHS Security Office will generate a number of incident scenarios ranging from minor to worst-case-impact. Those scenarios will be crafted to maximize testing of the incident response process and business continuity process with an eye towards intentionally stressing the processes and revealing gaps in the processes.

ii. The list of incident scenarios will be provided to the Agency SIRT by August 1. The Agency SIRT should work with other personnel at the Agency to determine an appropriate response path for the scenarios.

iii. Beginning on September 1 and ending on December 31 of that fiscal year, the Incident Response Lead will schedule times to meet with Agency SIRTs. At those meetings, the Incident Response Lead will pick a random subset of the incident scenarios and run through them with the Agency. At the Incident Response Lead's discretion, the Incident Response Lead may modify the scenario, within reason, to make it easier or more difficult. After the conclusion of the meeting, the Incident Response Lead will draft a memorandum outlining the strengths and weaknesses of the incident response and business continuity implementation and provide recommendations for improvement (if any).

iv. Beginning on January 1 of that fiscal year, the Incident Response Lead will schedule follow-up meetings with the Agency SIRTs to distribute the incident response memorandum findings and recommendations and work with the SIRTs to implement the recommendations by the end of the fiscal year.

e. Forms for Reporting on the Incident

Per EOTSS Standard IS.009, the following forms must be filled out during the investigation:

i. EOHHS SIRT Chain of Custody Form – Attachment 4
ii. EOHHS SIRT Evidence Form – Attachment 5
iii. EOHHS SIRT Response Form – Attachment 6
iv. EOHHS Lessons Learned Form – Attachment 7
v. EOHHS SIRT Incident Form – Attachment 8

XII. CONTINGENCY PLANNING

a. Purpose

Contingency Planning, in the broadest sense, deals with the planning and management of continued access to critical EOHHS Information Resources and business functions in the event of impact to the data contained within or the inability to access such data. This may result from infrastructure failure, natural disasters, or other events that compromise continued EOHHS operations.

b. Policy

All Agencies and critical EOHHS Information Resources and business functions must have a contingency plan in place. This contingency plan must consider how service provision will continue during the event giving rise to implementation of the contingency plan. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

c. Contingency Planning Standards

All Agencies and critical EOHHS Information Resources and business functions must define and document the processes that are critical to continued service provision. Once identified, it is the responsibility of those groups to determine how operations will continue in the event of an event giving rise to deploying the contingency plan.

i. Agency leadership and Owners are responsible for ensuring the critical business functions and access to data can continue in the event of an event giving rise to deploying the contingency plan.

ii. The contingency plan must document the scenarios in which it will be activated and the mission critical assets/data/functions it will cover.

iii. The contingency plan must also include information with respect to continued operation including:

1. scenarios where access to the data is not possible such as network or power outage,
2. any manual processes that may be enacted for processes that were previously performed via an electronic means,
3. defining the roles needed and the people assigned to lead in performing those processes,
4. a list of contacts for notification of the outage and those responsible for performing any potential disaster recovery operations,
5. any connectivity to other processes or departments that would be impacted by the enactment of the contingency plan,
6. any notifications to the public of the enactment of the contingency plan,
7. timeframes of acceptable recovery as well as timeframes for enacting the various portions of the contingency plan,
8. recovery objectives should include minimizing the amount of work duplicated and data lost, and
9. details on the resumption of operations once the event has concluded.

iv. The contingency plan should further identify what failover sites exist to continue operations, even if the failover is for staff to work from home. Staff contact information should be readily accessible and available for management and other

staff to support continued operations.

d. Contingency Plan Auditing, Training and Testing

Annual testing of the plan must be conducted in order to ensure that the information in the document is correct and kept up to date. This testing should be conducted in order to maximize training of the plan with staff. When possible, a full failover test should be scheduled. The testing may also be conducted in concert with the testing outlined in *Section XI, Incident Response and Security Incident Response Team*. In addition, at least one staff member should review the efficacy of the contingency plan and make recommendations for improvement or at least identify deficiencies in the current contingency plan.

e. Contingency Planning Standards Specific to Information Systems

Owners must determine whether or not they should have a geographically distinct backup and processing site such that during an event giving rise to implementation of the contingency plan that there is no impact to service. This is deemed met if the Information System is using EOTSS's preferred or provided hosting services, which includes geographically distinct backup services. In the event an Information System is not hosted with EOTSS's preferred or provided hosting service, that Information System's Owner should determine whether or not that is appropriate based on the impact to critical Agency operations from downtime.

XIII. CONFIGURATION MANAGEMENT

a. Purpose

Configuration management, in the broadest sense, deals with changes to the configuration of Information Resources which could impact the overall security posture of the EOHHS Environment. Proper recording of the approved changes will allow environmental consistency, assist in business continuity and disaster recovery, and assist in troubleshooting problems. It also allows Owners to monitor and audit against the baseline to ensure that changes were implemented as presented and that unapproved changes were not performed.

Appropriate management of configurations allow quick and easy deployment of resources and reconstituting/rebuilding from scratch for business continuity and disaster recovery purposes. It also provides consistency across environments. In the Information System space, for example, each lower level will need to be clones of the previous (development, test, staging, and production) in order to ensure the integrity of the work being done in the Information System.

b. Policy

All EOHHS Information Resources must have a recorded Baseline. Configuration Management will include any aspect of hardware, software, settings and processes needed to enable expected and planned functionality and comply with any required regulations. Documentation shall include the architecture, any connections to other environments, and

processes captured on usage. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Configuration Management Standards

Owners must maintain a Baseline for operations, Information Systems, and other Information Resources under their purview. While the requirements outlined in this *Section XIII, Configuration Management* are focused on Information Systems, all Information Resources and processes must have prepared Baselines to support resumption of operations as expeditiously as possible.

Baselines must include, at a minimum and as applicable, the following considerations:

i. Description of the Information Resource and the intended functionality
ii. Architecture of the Information Resource
iii. Information Resource hardware components
iv. Information Resource software components
v. Configuration changes made to the installation of software and hardware aside from vendor recommendations
vi. Name, title, and contact information for Owners
vii. Location of hardware (server rack, desktop, etc.)
viii. Location of media files for installation along with any additional components that have been added
ix. Location of associated documentation for business continuity and disaster recovery
x. Configurations for creating and monitoring alerts
xi. Documentation for required configurations based on law or contract
xii. Any linkage to other Information Resources and details on how they are connected
xiii. Secure configurations for the system:

    1. Accounts with details of access to the system including groups such as system administrators and service accounts
    2. Reference to the hardened template used for the operating system
        a. Included should be any ports or services that have been enabled for the Information Resource to function and why it was necessary to deviate from the standard
    3. Audit, authentication and access controls
    4. Approved methods of accessing the system for maintenance (VPN only, SSL, physical location, etc.)
    5. Protections in place such as HIPS, endpoint protection, firewall, etc.
    6. Firewall settings
    7. Operational Risk Assessment sign off documentation, if applicable, generated pursuant to the process outlined in *Section X, Authorization to Operate and Operational Risk Assessment*

Baselines must be reviewed at least once annually and updated as appropriate. Baselines must also be reviewed upon significant and material changes to the Information Resource that render the prior Baseline obsolete.

d. Change Control Committee and Change Process

Owners should work to expeditiously implement change control committees to verify and approve a Baseline. The size and formality of these groups will vary from Information Resource to Information Resource and Agency to Agency. At a minimum, all change control committees must be structured to ensure the division of labor such that the individual or group approving of changes is competent to approve of such changes and is distinct from the person implementing changes. The change control committee should include the Information Resource Owners or report to such Owners.

Any changes to the Baseline must be submitted for approval to Owners for review. The change must be documented with detailed implementation steps, settings and software/hardware necessary to adequately implement the change in the development environment. Change documentation should also include the expected outcome(s) from the change and if there are any known security risks/vulnerabilities being introduced or remediated because of the change. If there are known security risks/vulnerabilities being introduced, the process outlined in *Section X, Authorization to Operate and Operational Risk Assessment* must be followed expeditiously to not impact deployment of changes to Production. Changes should be distributed and accessed on a need-to-know basis.

A rollback plan should also be included in the event the change does not function as expected. The rollback plan should also include the exact steps for the return to the previous Baseline. Any processes that will also change as a result should be documented and either updated in the current procedures or an addendum should be included.

Once the Owner approves of the Baseline change, it should be tested for compatibility and security impact. When testing is successfully completed and the changes are ready to be moved into the Production or business operations environment, it will need to be submitted to the change control committee for review and approval. Members of the committee will be able to ask questions to the submitter regarding the change as well as scheduling resource availability for implementation. The change control committee should review the expected time to implement the change, any rollback plans, and any authorization to operate or operational risk assessment. If approved, the change should be placed onto a change calendar managed by the change control committee. If the change is not approved, feedback should be provided to the submitter including comments for remediation for resubmission.

During implementation, the implementation team should be available to answer questions posed by the change control committee, to troubleshoot if issues arise, or to implement the rollback plan. Once the implementation is completed it will need to be verified and approved by the change control committee. Relevant stakeholders should also be notified of the completion of the change or implementation of the rollback plan. All associated documentation should be updated before the change is closed. That documentation should be maintained to support operationalization of the change. Software should be filed in a predefined and accessible media library and materials saved in a designated documentation retention area.

XIV. IDENTITY AND AUTHENTICATION

a. Purpose

The standards outlined in this *Section XIV, Identity and Authentication* address the processes, procedures, and systems used to verify the identity of individuals and accounts that may request access to Information Resources and to make authorization decisions granting or denying access.

b. Policy

All Information Systems must have appropriate administrative and technical controls in place to ensure accurate identification of individuals and accounts, and proper authorization prior to granting access to Information Systems and to functions that read, create, modify, and reporting on Information Resources. User, account, and system access shall be affirmatively managed throughout account and system lifecycles, including identification of users; disabling of known- or suspected-compromised accounts; modification of account rights and privileges when roles change, when individuals start and end service, and at otherwise appropriate times; and revocation of access when it is no longer needed to fulfill an authorized business function. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Identity and Authentication Standards

i. **Unique Identification:** Information Systems must uniquely identify and authenticate both (a) organizational users (employees, contractors, researchers, etc.); and (b) non-organizational users (vendors, external support staff); for all processes and accounts acting on their behalf, before providing access to, establishing a connection to, or executing a function on, any Information Resources.

ii. **Multi-factor authentication:** Information Systems must require multi-factor authentication for remote and network access to all user accounts, privileged and unprivileged, and for local access to privileged accounts. All authentication mechanisms must include hardening in design or implementation to resist session-replay (traffic sniffing or traffic replay) attacks. Multi-factor authentication for remote access to privileged and non-privileged accounts must include at least one factor provided by an approved smartphone app or hardware token. All Information Systems must accept and electronically verify Personal Identity Verification (PIV) credentials for identification and authentication.

iii. **Credentialing process:** The registration process to receive passwords, certificates, hardware tokens, and other authenticators must be conducted **in person** by an individual authorized to distribute such credentials. Passwords may not be sent by email or text message/SMS (except that: (i) self-serve password-reset links may be sent electronically, as long as they expire after no more than 24 hours; and (ii) one-time use PINs may be sent electronically, as long as they expire after no more than 5 minutes).

iv. **Identifiers (usernames/account names):** Owners are responsible for ensuring their Information Systems and associated processes perform all of the following requirements with respect to identifiers (usernames, account names, security badge numbers, Globally Unique Identifiers ("GUID"), etc.:

1. Receiving prior, written authorization from business process Owners before assigning an individual, group, role, or device identifier;
2. Selecting and assigning an identifier for the relevant individual, group, role, or device;
3. Preventing reuse of identifiers for at least ten years;
4. Disabling the identifier after a defined period of inactivity (60 days for user accounts; 1 year for application or system accounts; 1 year for groups with no active accounts);

v. **Authenticators (passwords, PINs, tokens):** Owners are responsible for ensuring their Information Systems and associated processes perform all of the following with respect to authenticators (passwords, PINs, biometrics, etc.):

1. Verifying the identity of the individual, group, or device receiving the authenticator before distributing it;
2. Ensuring that authenticators have sufficient strength of mechanism for their intended use;
3. Establishing and implementing procedures for initial authenticator distribution, initial authenticator content, changing default content of authenticators prior to Information System installation, changing or revoking lost/compromised or damaged authenticators; and for revoking authenticators;
4. Changing/refreshing authenticators on a regular schedule appropriate to the authenticator type (60 days for passwords, 5 minutes for one-time PINs in apps or hardware tokens; 5 years for access cards such as PIVs and other identification cards, etc.)
5. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; protecting authenticators and authenticator content from unauthorized disclosure and modification, and requiring that individuals take steps and are trained to do the same;
6. Never using shared authenticators (e.g. password shared with multiple individuals) unless it is technically impossible to operate the Information System without doing so, and changing shared authenticators whenever there are membership changes in groups with access to a shared authenticator.
7. For hardware token-based authentication, the token and authentication system must satisfy FIPS 140-2 requirements.
8. If an Information System accepts third-party credentials, they must be FICAM-approved, and the Information System must conform to FICAM-issued profiles.

vi. **Password standards:** All password-based authentication must meet the following requirements:

1. **Complexity:** Enforce minimum password complexity of at least:
    a. Character Count:
        i. 8 characters for public user accounts,
        ii. 12 characters for all other non-administrator accounts,
        iii. 15 characters for administrator accounts,
    b. And including:
        i. 1 lower case letter,
        ii. 1 upper case letter,
        iii. 1 number,
        iv. and 1 special character.
2. **Not recently used:** Any new passwords must be different from the last 24 passwords used for that individual or account
3. **Changes must be non-trivial:** All changes must modify at least 2 characters from all stored previous passwords.
4. **Minimum and maximum age:** passwords must be changed regularly (every 60 days for user accounts; annually for service and application account), and may not be changed within 1 day of the previous change (unless a written exception justifying an earlier change is documented).
5. **Temporary/Initial Passwords:** Information Systems may allow the use of a temporary password for initial logons or password resets, as long as: (1) the initial password is randomly set; (2) it is unique to the account to which it is assigned; and (3) the system requires an immediate password change upon first login. Password resets must require re-identification of the individual whose account is being reset.
6. **Password encryption required; salt preferred:** Passwords and other authenticating credentials may not be stored or transmitted in plaintext; they must always be cryptographically protected in transit (e.g., session encryption, HTTPS) and at rest (e.g., hashed) using Acceptable Encryption Suites, and, if available, a site- or system-specific salt prior to hash.

vii. **Certificate-based authentication recommended:** Although PKI/certificate-based authentication is difficult to set up, once it has been initialized, it is more secure and arguably easier to use than passwords. For this reason, Owners are strongly encouraged to use certificate-based authentication instead of (or in addition to) password-based authentication. All cryptographic authentication mechanisms must use Acceptable Encryption Suites.

viii. **Certificate authentication requirements:** All PKI/certificate-based authentication must:

1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor;
2. Check certificate status information (including revocation lists via Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP), and against a Certificate Transparency chain if one exists for the relevant domain);
3. Enforce authorized access to the corresponding private key;

4. Map the authenticated identity to the account of the individual or group; and
5. Implement a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

d. Additional Design and Configuration Hardening Requirements

i. **No hardcoded credentials**: Owners must ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. Hardcoded passwords and hardcoded certificates are not permitted. If authenticators are used in the manner stored, then those representations are considered unencrypted authenticators, irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

ii. **Do not display secret authenticators:** All Information Systems must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals (for example, displaying asterisks (*s) at a login prompt instead of the password itself, which reduces the risk of shoulder-surfing).

iii. **Impede account enumeration attacks:** Authentication denials must behave the same whether an identifier exists and the authenticator was incorrect, or there was no matching identifier found (to prevent account-enumeration attacks). Similarly, for password reset requests by email, Information Systems must not indicate whether an account was found or not. Instead, they should indicate that if an account with that identifier (username or email address) was found, reset information was sent to its registered email address.

XV. MEDIA PROTECTION

a. Policy

All EOHHS personnel must secure media in any form in the EOHHS Environment so that Information Resources contained on those media are secured. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

b. Media Protection Standards

Staff are not restricted in the kinds of media they may use in the EOHHS Environment and all digital (e.g.: USB flash drive) and non-digital media (paper) are permitted. Staff, however, must not store Sensitive Information on unencrypted digital media or in an unencrypted format if the digital media cannot be encrypted itself. Additionally, staff may not store Sensitive Information on unsecured non-digital media. To that end:

i. All non-digital media containing Sensitive Information must be locked in a container (e.g.: filing cabinet) or secured within a locked room (e.g.: a locked office) when not in use. Non-digital media should not be left unsecured while unattended.

ii. All information resources stored on digital media must be encrypted. That encryption may be container-based (e.g.: an encrypted file) or device-based. If relying on device-level encryption, the media must meet the standards outlined in FIPS 140-2 Level 2 for secure devices.

Digital media must have an owner and devices without a specific owner must not be used in the EOHHS Environment.

All media containing Sensitive Information that leaves the EOHHS Environment must be marked on the media that it contains Sensitive Information. This may be done by marking the media as confidential, sensitive, or with some other similar marking or indication. Movements of media containing Sensitive Information outside of the EOHHS Environment should be documented such that access to the media and custody of the media can be attested to throughout transit.

When media containing Sensitive Information is at the end of its lifecycle, it must be destroyed or sanitized pursuant to the requirements of NIST 800-88. These requirements assure that information is removed from media such that the information cannot be retrieved or reconstructed.

XVI. SYSTEM AND COMMUNICATIONS

a. Policy

All Information Systems must have appropriate administrative and technical controls in place to ensure the protection of systems, components, subcomponents, and communications among them. Owners are responsible for designing and configuring their Information Systems to ensure the confidentiality, integrity, and availability of Information Systems and information resources. Generally, Information Systems shall be inventoried, affirmatively managed, configured according to industry best practices, patched with security updates, and used only so long as they are supported by the vendor or provider (or, in the case of open-source software, the project is releasing security updates, even if not formally contracted for support as with COTS or vendor-developed software). Generally, communications shall be encrypted and authenticated, and shall take place through functions that include security checks, rather than direct access to data or memory. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

b. System and Communications Standards

i. All Information Systems must:

1. Separate user functionality (including user interface services) from information system management functionality.
2. Prevent unauthorized and unintended information transfer via shared system resources.

3. Protect against or limit the effects of denial-of-service attacks, including network- and application-level flooding, DDoS, reflected DDoS, ransomware, and physical damage, by:

    a. Hardening all system configurations according to vendor recommendations and industry best practice
    b. Using protective technologies where the cost of doing so is less than the risk appropriate (which may include intrusion prevention systems, firewalls, router access control lists, proxies, reverse proxies, web application firewalls, and sinkholing/blackholing services)
    c. Allocate sufficient technical and logical resources (bandwidth, compute/CPU, memory, sessions, etc.) to handle the highest normal expected load, where appropriate partitioning such resources using priority queues and/or quotas
4. Maintain a separate execution domain for each executing process (i.e., processes may only interact through APIs, not shared memory).
5. Log system and resource loads over time, which Owners must periodically review, adjusting assigned resources to handle projected loads

ii. For each Information System, Owners must:

1. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system (e.g. between services, components, and subcomponents within the system).
2. Implement controls, where practicable, to verify the source and format of data passed between systems or between components or subcomponents within a system, ensuring that malformed requests are logged and denied.
3. Implement subnetworks for all publicly accessible system components that are physically or logically separated from internal organizational networks.
4. Design and configure their Information Systems on the assumption that interfacing systems, components, and data flows may be compromised, and develop and implement their own Information Systems with boundaries designed to stop or impede that compromise from spreading (defense-in-depth). Information Systems must avoid blindly trusting the format of data streams just because they are internal or from a known external partner; instead, their format and well-formedness must be checked at each boundary before the information is processed or passed on.

iii. For all connections to external networks or resources, Information Systems must:

1. Connect to external networks, services, or 3rd-party information systems, only through managed interfaces that include boundary-protection devices (firewalls, proxies, etc.)
2. Limit the number of external network connections
3. Implement a separate managed interface for each external service or system

4. Establish and periodically review traffic flow policies for each managed interface, with a default-deny policy (deny all, permit by exception)
5. Document any exceptions to traffic flow policies with a supporting business need, duration of such need, and approval thereof (reviewing all such exceptions at least annually, and removing any which are no longer supported by a business need)
6. Protect the confidentiality and integrity of the information being transmitted across each interface (i.e., with encryption and authentication)
7. Prevent, by policy and configuration, remote devices from simultaneously establishing non-remote connections with the Information System and communicating via some other connection to resources in external networks (i.e., split tunneling is disabled, and users are prevented from enabling it)
8. Employ authenticated proxy servers at managed interfaces for all transmissions of regulated data to any external networks, services, or 3rd-party information systems, logging metadata for all such traffic to a central logging platform

iv. Within each Information system, Owners must ensure:

1. Implementation of host-based firewalls on all servers, workstations, mobile devices, and other Information System components (or external or virtual firewalls at the immediate next network hop – e.g. a Layer 3 switch with built-in firewall)
2. Isolation of systems providing user authentication, user authorization, network management, configuration management, vulnerability scanning/management, and other high-risk services from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system
3. The Information System fails securely in the event of an operational failure of a boundary protection device (e.g., if a firewall fails, no traffic flows; if a router with ACLs cannot process the traffic load, it defaults to dropping unprocessed packets, etc.)
4. The Information System protects the confidentiality and integrity of transmitted information, within Information Systems (between components), between Information Systems, and transmissions to 3rd-party or other external systems, using Acceptable Encryption Suites during transmission to (a) prevent unauthorized disclosure of information; and (b) detect changes to information in-transit. The information system must also maintain the confidentiality and integrity of information during preparation for transmission and during reception
5. The Information System terminates the network connection associated with a communications session at the end of the session or after a policy-defined period of inactivity (not to exceed 15 minutes for applications and 4 hours for VPN/tunneling connections)

c. Key Management Standards

Owners must ensure that their Information Systems and all business processes manage the cryptographic keys for required cryptography in accordance with FIPS 140-2 Level 2; HIPAA; NIST SP-800-53r4; and other applicable laws, regulations, and directives.

All public key certificates must be issued in accordance with these same requirements, or obtained from an approved service provider that meets these requirements.

d. Mobile and Collaboration Devices Standards

Owners must ensure that collaborative computing devices (VOIP and traditional telephones, teleconference equipment, microphones, cameras (except security cameras), electronic white boards, etc.): (a) prohibit remote activation, unless (i) authorized by the relevant EOHHS Risk Governance Team, or (ii) required by law; and (b) provides an explicit indication of use to users physically present at the devices (unless (i) or (ii) above applies).

Owners must authorize, monitor, and control mobile devices that connect to Information Systems or access Information Resources, ensuring adherence to all applicable mobile device policies, and use only vetted & approved mobile devices, code, and technologies. Owners whose Information Resources contain FTI must work to prohibit access to FTI with that mobile device. Per IRS requirements, mobile devices are not authorized to be used to access FTI.

Owners must authorize, monitor, and control the use of VOIP technologies in their environments and by their employees above and beyond the EOHHS telephony system. Such Owners' authorization must be a risk-based assessment, taking into account the risk to Information Systems, Information Resources, and information itself, of potential misuse, including employee misuse (intentional or accidental) as well as malicious use (intentional eavesdropping, interference with other Information Systems, etc.).

e. Name and Address Resolution (lookup services and authoritative DNS)

Information Systems that provide name-to-address resolution (DNS, WINS, etc.), must provide additional data-origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to name or address resolution queries (e.g., DNSSEC). Where such an Information System is part of a distributed or hierarchical namespace, it must provide the means to indicate the security status of child zones and, if the child supports secure resolution services, to enable verification of a chain of trust among parent and child domains.

Information Systems that make name- or address-resolution requests must perform data-origin authentication and data-integrity verification on name and address resolution responses.

Information Systems that collectively provide authoritative name or address resolution services for an agency, organization, location, or subnetwork (e.g., authoritative DNS servers) must be fault-tolerant (i.e., at least two active systems in at least two different

physical locations, one primary and one secondary) to eliminate a single point of failure and to minimize the risk of name-resolution outages. They must also implement internal/external role separation: separate Information Systems must be used for internal-only namespaces, such that Systems with internal roles only process name and address resolution requests from within organizations (i.e., from internal clients), while those with external roles only process name and address resolution information requests from clients external to organizations (i.e., on external networks including the Internet). Access to all internal namespace resolution services must be restricted (e.g., by address range, client lists, certificates, etc.) to internal systems, with any exceptions documented and specifically authorized.

f. Encrypting Sensitive Data in Transit

Information Systems must protect the authenticity of communications sessions (in addition to data packets) carrying Sensitive Information, using Acceptable Encryption Suites (including for confidentiality and authentication) that provides assurance of all communication parties' identities, ensures data is not modified in transit, and protects against session hijacking, session replay, XSRF, and other man-in-the-middle and session attacks. This should include data transmissions within MAGNet, as well as transmissions to and from external parties/services, and all wireless data transmissions.

Encryption and authentication should be the default choice for data transmission. In addition to required encryption, Owners are strongly encouraged to encrypt all data in transit. Wherever possible, Owners are strongly encouraged to configure their Information Systems to check certificates against the certificate revocation list, and to disallow connection if offered a revoked certificate or if the CRL cannot be reached.

g. Encrypting Sensitive Information in Email

Whenever sending sensitive information via email, Owners must ensure that their employees and Information Systems send only encrypted email, such that the authorized recipient can only receive the sensitive information over an encrypted channel. Acceptable methods include encrypting an attachment in the normal email stream, as long as the passphrase or key is shared via a separate, authenticated communications method, a plaintext email containing a link to an authentication-protected download portal, etc.

Information Systems sending or receiving email (inbound and outbound mail relays, inbox servers, etc.) must support encrypted transit using an Acceptable Encryption Suite, and must use such encryption if the other system (either sending or receiving the mail) supports it. Information Systems should log the number of emails sent to each domain, and record whether that domain supports SMTP over TLS (or other encrypted channel) or not.

h. Encrypting Sensitive Information at Rest

Information Systems must protect the confidentiality and integrity of data at rest. For all Sensitive Information, Owners must ensure either (i) physical control of access to the media storing and the Information Systems processing that information or (ii) encryption of the data with an Acceptable Encryption Suite. File, row/application, folder, and/or disk-level

encryption may be appropriate based on the system architecture and the types of risks it faces. When data is encrypted, its encryption key must be securely stored, such that the level of access required to read the encrypted data does not automatically include access to the key (e.g., encrypted .zip files may not be sent over email if the key is also shared via email); an encrypted laptop or portable hard drive does not count as "encrypted" under this Document if the passphrase or key required to decrypt it is affixed to or stored with the device.

i. Data and Process Partitioning

Where appropriate, Information Systems must be partitioned into separate physical domains or environments based on the data classification of the Information Resources and data they contain.

Highly sensitive information may only be stored in tighter-controlled environments (i.e., NIST 800-53r4 High; FedRAMP High, etc.). Highly sensitive information will be defined on an as-needed basis by each Agency maintaining the data. At a minimum, this information includes CJIS data maintained in the EOHHS Environment.

j. Sensitive Information in Fax Transmissions

For any Information Systems authorized to send or receive PHI in fax transmissions, the recipient must be authorized, the fax-capable machine located in a locked room or other secure Facility, fax preset/speed-dial numbers must be checked for accuracy at least annually and whenever cause to believe the number is inaccurate or no longer accurate arises. Outgoing fax transmissions must use a cover sheet that explicitly provides guidance to the recipient that includes a notification of the sensitivity of the data and the need for protection, and a notice to unintended recipients to telephone or reply to the sender (collect if necessary) to report the disclosure and confirm destruction of the information.

XVII. PHYSICAL AND ENVIRONMENTAL PROTECTIONS

a. Purpose

Physical and environmental protections controls address physical safeguards and procedures that grant or deny access to Facilities and Supporting Infrastructure, as well as their design and operation. For access controls for Information Resources or Systems themselves, including decisions about how such permission is granted, modified, and revoked, see *Section VI, Access Control*.

b. Policy

All Facilities must have appropriate physical and environmental controls in place (considering data classification levels and operational criticality) to protect against unauthorized access, interruption of service, interception or modification of traffic, and to detect, respond to, and review incidents that arise. Compliance with these standards must

be achieved within twenty-four (24) months of publication of this Document.

c. Physical and Environmental Protections Standards

i. *Restrict Access to Authorized Individuals*

Managers must adopt, disseminate, provide training on, and periodically review and update (at least annually) policy and procedures to ensure implementation of the following requirements:

1. Managers must identify the Facilities for which they are responsible and any Supporting Infrastructure, determine the physical boundaries, controlled areas, and access points of each, and enforce physical access authorizations at each access point, including all of the following:
    a. Authorizing individual access according to the principle of least privilege, so that individuals only have the lowest level of access necessary to perform their (current) job
    b. Implementing technical, operational, and administrative controls to maintain separation and adhere to the principle of least privilege where authorized individuals have physical access to logically separated data, applications, databases, or virtual hosts
    c. Verifying individual access authorization before granting access to the Facility or Supporting Infrastructure
    d. Controlling ingress to and egress from the Facility using locked doors, keys, PIN entry pads, badge readers, access control vestibules (man-traps), guards, and/or other appropriate physical access controls
    e. Maintaining physical access audit logs for each access point (written and/or automated)
    f. For areas of a Facility designated as publicly accessible (e.g. lobbies, delivery areas, etc.), providing physical separation from controlled-access areas and any security safeguards necessary to support the controls applied to the controlled-access areas of the Facility (e.g., guards, cameras, motion detectors, etc.)
        i. Components of Information Systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible, as long as access to these components is effectively controlled using technical or administrative safeguards
    g. Escorting all visitors to controlled-access areas in Facilities, monitoring their activities, and logging their identity, entry and exit times, and the reason for the visit
    h. Securing all keys, key cards, identification badges, security tokens, and other physical access devices, and inventorying and accounting for them at least annually
    i. Changing combinations and keys (i) periodically (at least once every 5 years); and (ii) whenever keys are lost, combinations are compromised, or individuals are transferred or terminated (and

such individual had access to combinations, or had keys and failed to return them, or had keys and was known or suspected to have made copies)

j. Ensuring that output devices (including but not limited to printers, fax machines, and display devices that show output without requiring authentication) are appropriately located, or otherwise protected, so as to prevent unauthorized individuals from viewing or obtaining the output
k. Locating Information Systems within Facilities, and designating and designing any new Facilities, so as to minimize the opportunity for unauthorized access (considering the type of physical access controls applied, lines of sight, physical distance between Information Systems and points of access for controlled areas)
l. Designing and operating Facilities and Information Systems so as to minimize the potential for unauthorized interception, recording, and modification of wireless traffic
m. Authorizing, monitoring, and controlling the movement of all devices entering, exiting, or within a Facility (including hard drives, flash drives, CDs/DVDs, and other storage media; computers, computer parts or other components of an Information System; mobile devices, including mobile phones, tablets, and wearable devices; cameras, voice recorders, or other recording devices; in short any device which can record or store information, or connect to an Information System—including wirelessly, over WiFi, Bluetooth, Zigbee, Z-Wave, proprietary protocol, or otherwise)
n. Securely removing any sensitive data, regulated information, and licensed software from media/devices exiting a Facility, unless there is a specific business need for, and regulations and applicable Third Party Agreements allow, removal to an off-site facility
o. Ensuring any off-site facilities which handle equipment from an EOHHS Facility, where the device/equipment has not been securely erased (i.e., overwritten: standard deletion and drive formatting are not sufficient) is required to adhere to these same controls

2. Managers must maintain and approve a list of individuals with authorized access to each Facility, based on position or Role; issue authorization credentials for Facility access; periodically review their access lists; approve any visitors to the Facility; and remove individuals from access lists when access is no longer required. They must also ensure that:
    a. Physical access to Facilities is monitored to detect and respond to apparent, suspected, and reported security incidents, including break-ins, the presence of unauthorized individuals, and misplaced or stolen access credentials
    b. All individuals, including visitors, who enter access-controlled areas are included in the physical access logs
    c. Physical access logs are reviewed at least annually (sampling is permitted for periodic reviews), and reviewed in detail whenever unauthorized access is apparent, suspected, or reported

d. The results of reviews and investigations are shared with the organizational incident response capability
e. Physical intrusion alarms and other surveillance equipment are monitored
f. Staff are trained to avoid piggy-backing (using one individual's entry authorization to allow multiple people through an access point), even among colleagues
g. Staff are trained to report the presence of anyone not carrying a badge (and whom they do not recognize) to appropriate security personnel

3. Managers must ensure that contractors, vendors, and other third-parties performing work or providing goods to or services in Facilities adhere to these requirements. Managers must notify such persons or organizations that failure to do so may be grounds for termination of existing agreements and may be considered in evaluation and negotiation of future agreements.
4. Managers must ensure that procedures are in place to facilitate controlled access for emergency responders in the event of a medical, fire, or security event.

ii. *Protect Facilities and Supporting Infrastructure*

Managers are responsible for maintaining a stable, safe operating environment at each Facility, by:

1. Maintaining and updating Facility equipment and Supporting Infrastructure according to manufacturer recommendations, ensuring that maintenance, troubleshooting, and repair are conducted by authorized personnel, and keeping current documentation and maintenance/repair logs on all such equipment
2. Protecting from damage and destruction each Information System's power equipment, power cabling, network cabling, network devices, and other Supporting Infrastructure
3. Ensuring the ability to shut off power to each Information System (and/or individual components) in emergency situations
4. Placing emergency power shutoff switches in appropriate locations to facilitate safe and easy access for personnel
5. Protecting emergency power shutoff capability from unauthorized activation
6. Locating Information Systems within Facilities, and designating and designing any new Facilities, so as to minimize potential damage from fire, flood, wind, rain, lightning, tornado, snow, ice, falling trees/limbs, and other hazards of the weather (including at least a consideration of incoming electromagnetic radiation from EMP bursts and solar flares, even if the response is acceptance of the risk), as well as intentional sabotage (e.g., terrorism, burglary, vandalism) and foreseeable accidents (e.g., vehicular traffic on adjacent roadways, windows that may break, etc.)
7. Protecting the Information Systems from damage resulting from water leakage by:

a. Providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel
b. Using water-leak-detection devices that alert appropriate personnel

8. Providing a short-term uninterruptible power supply, to facilitate either an orderly shutdown or a transition to long-term alternate power for all Information Systems within the Facility, in the event of loss of power from the primary power-source
9. Employing and maintaining automatic emergency lighting for the Information Systems, which activates in the event of a power outage/disruption and covers emergency exits and evacuation routes within the Facility
10. Installing and maintaining fire suppression and detection devices/systems for Facilities and Information Systems that:

    a. Are supported by an independent energy source
    b. Activate detection mechanisms automatically
    c. Notify appropriate personnel in the event of a fire or activation of the device/system (including Facility personnel and emergency responders)
    d. Deploy fire-suppression capabilities automatically (for any Facility not staffed on a continuous basis)

11. Defining acceptable temperature and humidity levels based on manufacturer recommendations of Information Resource components, maintaining those levels within the Facility, and monitoring them continuously or periodically (at least hourly).

iii. *Backup Facilities and Alternate Sites*

1. During normal operation, all redundant, failover (whether automatic or manual), and backup Facilities must use the same controls required at the primary Facility, unless each such deviation is documented in writing and approved by the relevant EOHHS Risk Governance Team.
2. In case of emergency as designated by relevant EOHHS Risk Governance Team, alternate work sites may be used (such as other government property, or employees' homes if voluntarily provided) which do not meet all of these physical and environmental security controls, without written documentation of each deviation (although the deviation still must be, in fact, authorized by the relevant EOHHS Risk Governance Team).
3. Managers for each Facility and Information System must document and disseminate a means for employees to communicate with Managers and with information security personnel in case of security incidents, problems with the Facility, or emergency.

XVIII. PERSONNEL SECURITY

a. Purpose

Personnel Security, in the broadest sense, deals with how staff are vetted during the hiring process, monitored during employment, and appropriately offboarded when their employment ends.

b. Policy

All EOHHS staff must be appropriately vetted, provided the minimum necessary access to perform their work, be monitored on an ongoing basis, and be completely offboarded at the conclusion of employment. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

c. Personnel Security Standards

Every Information Resource must have clearly defined and readily identifiable roles and responsibilities corresponding to the work that staff perform with respect to the Information Resource. Every Information Resource must also have an Access Coordinator. EOHHS should support Access Coordinators by providing straightforward and accessible processes for providing and revoking staff access to facilities and Information Resources.

i. *Role Definition*

1. All EOHHS staff positions must be classified based on their risk designation to the organization. The classifications must be consistent and supportable both within an Information Resource group and across the Agency. Some examples of how risk designation should be assigned are as follows:

- Low Risk:
    - the employee poses no or low risk to the organization for exfiltration or loss of sensitive information through mistake or intentional wrongdoing;
    - the employee's access credentials do not provide the ability for an external attacker to modify or gain access to sensitive network resources; or
    - the employee does not have decision-making authority with respect to sensitive matters or resources in the EOHHS Environment.
- Moderate Risk:
    - the employee poses some risk to the organization for exfiltration or loss of sensitive information through mistake or intentional wrongdoing;
    - the employee's access credentials provide the ability for an external attacker to modify or gain access to some sensitive network resources, but the scope and extent of that access is somehow limited; or

- the employee has decision-making authority with respect to some sensitive matters or resources in the EOHHS Environment, but their authority or scope of authority is limited.

- High Risk:
  - the employee poses significant risk to the organization for exfiltration or loss of sensitive information through mistake or intentional wrongdoing;
  - the employee's access credentials provide the ability for an external attacker to modify or gain access to most or all sensitive network resources and there are few or no effective limitations on that access; or
  - the employee has decision-making authority with respect to sensitive matters or resources in the EOHHS Environment and there are few or no limits with respect to that authority.

Risk designations must be reviewed by the end of the calendar year and updated based on good faith assessments of staff impact to Information Resources. All new positions must be classified within thirty (30) days of creation. Positions existing at the time of drafting this policy must be classified within a year of the effective date of version 1.0 of these *EOHHS Enterprise Information Security Standards*.

ii. *Working for the Organization*

1. The Access Coordinator must establish screening criteria commensurate with the risk level of the position to appropriately vet and train a new staff member. Depending on the severity of risk assigned to the role, such screening may include calling references, criminal or other background checks, role or position-based training, privacy or confidentiality agreements, or other means of safeguarding Information Resources. Screening would preferably occur before staff are provided access to Information Resources, but may occur after, however must not occur more than thirty (30) days after hire.

   Low and Moderate Risk staff are only required to be screened upon hire (but must receive training annually, pursuant to *Section V, Acceptable Use and Information Security Training*). High Risk staff must be screened once annually to include, at a minimum, position-based information security training.
2. The Access Coordinator must explicitly request staff access prior to the commencement of employment, pursuant to the relevant EOHHS, Agency, and/or Information Resource requirements for access. Access must not be granted outside of the scope of those requirements. The Access Coordinator should be mindful of appropriate processes and timelines for requesting access.
3. The Access Coordinator is responsible for monitoring and appropriately updating staff access to Information Resources and the facility in which they are located.

4. When staff are transferred, the Access Coordinator for their current Information Resources and the Access Coordinator for their new Information Resources must coordinate the appropriate access and timeline for the old and new Information Resources and ensure that access is appropriately terminated and created. Both Access Coordinators are responsible for ensuring that their current and former staff have appropriate access.

   Staff access to resources in the event of a transfer should be modified effective as of the date of the transfer. Staff access to resources in the event of a transfer must not occur later than thirty (30) days after the transfer.

iii. *Termination of Access*

1. When a staff member's employment with EOHHS ends, the Access Coordinator for their Information Resources is responsible for ensuring that access to Information Resources and any facilities to which the staff had access is terminated pursuant to the relevant EOHHS, Agency, and/or Information Resource requirements for access. Access to Information Resources and facilities must be terminated as soon as reasonably practicable. Access Coordinators must ensure that access to the EOHHS network and facilities are terminated as of the last day of the staff member's employment.
2. Access Coordinators must also ensure retrieval of all Commonwealth property including, but not limited to, identification cards, laptop computers, and mobile devices.
3. Access Coordinators must take steps to preserve business continuity such that they can access files and email for the staff member and continue to fulfill the business operation conducted by that staff.

iv. *External Access*

1. External access to EOHHS Information Resources must be classified and categorized similarly to the standards outlined in this *Section XVIII, Personnel Security*. Access Coordinators should work with Owners and the relevant EOHHS Risk Governance Team to determine external access to those Information Resources. Vendor Access should further be assessed pursuant to *Section XIX, System and Services Acquisition*.

v. *Special Provisions for Access to FTI*

1. Agencies must initiate and complete a background investigation for all employees and contractors prior to permitting access to FTI. This is required not only by IRS Publication 1075, but also by MGL c. 6A § 18Z. Per the requirements of IRS-1075, background investigations for any individual granted access to FTI must include, at a minimum:

a. FBI fingerprinting (FD-258) - review of Federal Bureau of Investigation (FBI) fingerprint results conducted to identify possible suitability issues. (Contact the appropriate state identification bureau for the correct procedures to follow.) A listing of state identification bureaus can be found at: https://www.fbi.gov/about-us/cjis/identity-history-summary-checks/state-identification-bureau-listing. This national agency check is the key to evaluating the history of a prospective candidate for access to FTI. It allows the Agency to check the applicant's criminal history in all 50 states, not only current or known past residences.
b. Check of local law enforcement agencies where the subject has lived, worked, and/or attended school within the last 5 years, and if applicable, of the appropriate agency for any identified arrests. The local law enforcement check will assist agencies in identifying trends of misbehavior that may not rise to the criteria for reporting to the FBI database but is a good source of information regarding an applicant.
c. Citizenship/residency – Validate the subject's eligibility to legally work in the United States (e.g., a United States citizen or foreign citizen with the necessary authorization).

Any employees or contractors who fail to pass a background check or refuse to undergo a background check may not access FTI and if they are currently accessing FTI must have their access to FTI revoked immediately. All employees and contractors accessing FTI must undergo a background investigation complying with the requirements herein every five years.

vi. *Sanctions for Failure to Comply*

1. Relevant EOHHS Risk Governance Teams must create and enforce sanctions for:

a. Failure of staff to comply with appropriate access requirements, and
b. Failure of Access Coordinators to supervise staff access and abide by the requirements outlined herein.

XIX. SYSTEM AND SERVICES ACQUISITION

a. Policy

All externally provided Information Systems and services must be appropriately evaluated and information security standards appropriately enforced. Compliance with these standards must be achieved within twelve (12) months of publication of this Document.

b. System and Services Acquisition Standards

i. All Information Systems and services must be procured and contracted for with explicit consideration of information security requirements including criteria for:

1. Evaluation, which require an explicit description of information security functionality and at least a high-level security architecture description, and acceptance of Information Systems and services,
2. Enforcement provisions including a description of interconnection requirements (e.g.: ports, protocols, services, etc.),
3. Legal and contractual requirements for data sources that will be used in connection with the Information System or services, and
4. Detailed documentation of all information security functions and mechanisms and privileged Information System functions so that EOHHS can fully and independently implement and operate the Information System.
5. Configuration and change management to ensure that only EOHHS-approved configurations and changes are implemented.
6. Security flaw testing (including code testing using analysis tools), tracking, remediation, and resolution.

Within twelve (12) months of publication of Version 1.0 of these *EOHHS Enterprise Information Security Standards*, the EOHHS Security Office will promulgate standard language to incorporate in procurement and contract documents. That standard language will, to the extent feasible, require external entities providing Information Systems or services to abide by the requirements outlined herein. Owners must ensure that appropriate resources are allocated to ensure information security standards can be appropriately implemented. Such standards will be crafted in accordance with appropriate legal and contractual drivers, identified pursuant to *Section VIII, Inventory and Classification* and Attachment 2.

ii. Owners must adopt a system development lifecycle methodology that appropriately accounts for information security considerations and permits identification of responsible parties for information security, testing of information security measures, and integrates information security risk management principles into the development lifecycle.

iii. At EOHHS's option, all externally provided Information Systems and services must be assessed, either by EOHHS or by an external auditor. No externally provides services should be further subcontracted without EOHHS's express approval and review.

iv. All Sensitive Information must be hosted within the United States. Sensitive Information must only be accessed from within the United States or via secure VPN connections into the United States.

v. When an Information System component is no longer supported by the vendor, developer, or manufacturer, that component must:

1. Be replaced with a component that is in support, or
2. Continue in place with express written justification, approved pursuant to the process outlined in *Section X, Authorization to Operate and Operational Risk Assessment*.

XX. SYSTEM AND INFORMATION INTEGRITY

a. Purpose

System and Information Integrity addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance, with respect to the integrity of Information Systems, the code running on them, and the Information Records they contain.

EHS must handle and retain information in and output from Information Resources in accordance with applicable federal and state laws, executive orders, directives, policies, regulations, standards, contractual obligations, and operational requirements. Generally, Information Systems must protect against malicious code running in firmware, kernel, and user-space; protect memory from unauthorized disclosure and alteration; provide facilities for vulnerability remediation and patching (and reporting); make use of logging and monitoring facilities; support security alerts, advisories, and directives; handle errors securely; and validate/sanitize information flowing into and out of the Information System and between system components. Information that is particularly important or sensitive shall be protected from unauthorized alteration and removal with the use of secure APIs (preferred over direct access), log entries for changes, cryptographic hashes, cryptographically signed modifications (e.g., PKI certificates), or through other suitable mechanism, policy, or process.

b. Policy

All Information Systems must have appropriate administrative, technical, and physical controls in place to ensure the integrity of Information Systems, code that runs on such systems, Information Records stored on such systems, guarding against improper or unauthorized modification or destruction. Owners are responsible for designing and implementing integrity controls that ensure information non-repudiation and authenticity. Compliance with these standards must be achieved within twenty-four (24) months of publication of this Document.

c. System and Information Integrity Standards

For each Information System, Owners must:

i. Identify, report on, and correct any vulnerabilities (whether publicly known or known to the Owner or any EOHHS staff) within 90 days of release of vulnerability information to the public (or release privately to EOHHS).
ii. Fully test software and firmware updates related to vulnerability remediation for effectiveness and potential side effects before installation, incorporating flaw remediation into the organizational configuration management process.
iii. Complete the installation and testing of all security-relevant software and firmware updates within 90 days of release of such update.
iv. Centrally manage the vulnerability remediation process, employing automated mechanisms (reporting, etc.), at least monthly, to determine the state of Information System component with respect to security vulnerabilities

Owners must also ensure the following physical, technical and administrative controls are in place for the following kinds of issues:

i. *Malware*:

Information Systems must:

1. Employ malware protection mechanisms (e.g., antivirus, executable whitelisting, etc.) at the System's entry and exit points to detect and eradicate malicious code.
2. Update malware protection mechanisms whenever new releases are available (automatically if possible, and in no case more than 30 days for signatures/definitions and 90 days for agent software) in accordance with organizational configuration management policy and procedures.
3. Run periodic scans using malware protection mechanisms (at least quarterly).
4. Perform real-time malware scans of files as they are downloaded, opened, or executed, on endpoint machines (in memory or in local storage), upon saving to or reading from shared storage (e.g., shared drives), and at network entry/exit points.
5. Block or quarantine malware where reasonably possible, alerting appropriate staff in response to detection of malware (e.g., through central logging and alerting on central log repository).

Owners must:

1. Address false positives during malicious code detection and eradication and contain and manage the potential impact on the Information System.
2. Centrally manage deployment, configuration, logging, and reporting of malware protection mechanisms/software.

ii. *System and Log Monitoring*:

1. Information Systems must be monitored to detect attacks, potential attacks, and indicators of compromise, identifying unauthorized, suspicious, and unusual activity. Every Information System must have designated individuals responsible for such monitoring, which group may comprise Owners, system administrators, agency staff, EOHHS staff, EOTSS staff, contractors, or other authorized parties. They must identify and analyze unauthorized and unusual activity/conditions using audits, log review, event correlation engines (e.g., SEIM), user behavior analytics, or other methodology, and initiate the incident response process when appropriate. Monitoring must cover activity on local systems, over the local network, via remote connections, and over connections to vendors/contractors/other third parties (including inbound and outbound traffic).

2. In addition to monitoring capabilities within Information Systems, Owners must ensure that independent monitoring devices (intrusion detection systems, web application firewalls, etc.) are deployed (i) strategically throughout the infrastructure (alongside Information Systems) to collect essential information such as authentication and authorization metadata; (ii) ad-hoc at appropriate locations to track transactions and information flows for highly sensitive information; and (iii) where wireless networks are deployed, to detect rogue wireless devices and attempts to eavesdrop on or inject traffic.

3. Log information, whether collected from an Information System or an independent monitoring device, must be protected from unauthorized access, modification, and deletion, including in-transit to the log collection facility and in storage once saved there. If an Information System is unable to either save its log information locally or reach a log-collection device (via a stateful, error-reporting protocol such as TCP), it must stop processing information and/or shut down.

   Owners must implement mechanisms to coordinate the access and protection of log information among external organizations when audit information is transmitted outside of EOHHS, such as with outsourced data centers or cloud providers. Those providers must be held accountable to protect and share audit information with EOHHS though mechanisms including, but not limited to, contract.

4. Owners are responsible for ensuring that Information Systems and monitoring devices send log information to a central log-management facility (centralizing at the Agency, EOHHS, or commonwealth-wide level, depending on the type of Information Resource and the application or Information System in which it resides). Owners are responsible for ensuring that their designated reviewers have access to the log, audit, correlation, and threat information necessary to perform this monitoring and analysis. Owners, Agencies, and EOHHS shall, to the extent practicable, ensure automated methods and tools are used to support near real-time analysis of events.

5. Users and services must have unique accounts, account metadata, or other identifying information, enabling those monitoring to identify the individual, service, account, or other party on whose behalf the Information System is acting, and the location or system where the activity is taking place.

6. Monitoring activity must be heightened whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, the Commonwealth, or the United States, based on information from law enforcement, intelligence, industry threat exchanges, or other credible sources of information. Owners, agency CIOs, and EOHHS are responsible for coordinating and implementing appropriate monitoring

activities and for configuring Information Systems to provide notice sufficient to allow such monitoring.

iii. *Receiving and Processing Security Alerts from External Entities*:

EOHHS shall (working with EOTSS as appropriate) designate appropriate personnel to receive information security alerts on an ongoing basis from reliable external partners to be identified by the EOHHS Security Office as regards specific information security threats and known indicators of compromise. EOHHS shall coordinate responses to these alerts, engaging the incident response process and notifying Owners and other agency staff as appropriate. Patch management will be managed separately: Owners shall designate appropriate personnel from among their system administrators to receive routine patching alerts for their Information Systems (usually from vendors). Incident response and patch management shall be tracked and measured against established SLA targets for each process, and the reason for and POAM for resolving any SLA overages shall be documented.

iv. *Security Function Testing*:

Information Systems must verify that security functions (such as access control, authentication/authorization, etc.) are operating correctly. This verification must be performed: (i) at system startup (or resume/wake from suspend); (ii) upon command by user with the appropriate privilege; and (iii) routinely at least monthly. The Information System must generate an alert for appropriate personnel, and then shut down or restart, when anomalies in security functions are detected. Failed tests or anomalous results must be treated as potential incidents and proceed through the incident response process.

v. *Integrity Checks for Core Components*:

Information Systems must use integrity verification tools (whitelists, tripwires, file hash comparisons, etc.) to detect unauthorized changes to core system components, such as operating system software, security functions, and any applications or programs running with root/administrator/full control permissions. These checks must occur: (i) at system startup; (ii) when new versions of core system components are installed; (iii) when new instances of core systems components are spawned or run; (iv) periodically (at least monthly, and at least weekly for systems containing highly sensitive information). Failed integrity checks or anomalous results must be treated as potential incidents and proceed through the incident response process.

vi. *Spam and Anti-Phishing Protection*:

Every Information System that sends or receives email must use anti-spam and anti-phishing protection mechanisms at entry and exit points, enabling detection of and incident response to unsolicited messages, spoofed or fraudulent email messages, and especially email soliciting usernames, passwords, or other authenticating information (e.g., account numbers, authorization codes, etc.). These protection

mechanisms must be (i) centrally managed by agency, EOHHS, or EOTSS, and connected to log-collection facilities and incident management processes; and (ii) automatically updated when new releases are available in accordance with organizational configuration management policy and procedures.

The EOHHS incident response process shall include responses to known or suspected phishing attacks, and EOHHS shall provide a facility for users to report suspected phishing. EOHHS may "phish" users at any time to determine risk posture and may require users who submit information in such a phishing audit to complete additional information security training.

vii. *Data/Input Validation*:

Information Systems must implement controls to verify the source and format of data passed from users to Information Systems, from third-party systems to Information Systems, or between Information Systems, ensuring that malformed requests (including user inputs) are logged and denied. Where practicable, such controls should also be applied to transmissions or between components or subcomponents within a System.

viii. *Prevent Data Leakage in Error Messages*:

Information Systems must generate error messages that provide no more information than necessary for corrective actions, and must not reveal information that could be exploited by adversaries. This includes such measures as ensuring that the system response is the same for situations with valid usernames with invalid passwords and for situations with invalid usernames (i.e., "invalid username or password" rather than "username recognized, but invalid password").

Error messages should not reveal instance-configuration information. For example a web application that cannot connect to its database server should report "unable to connect to database" instead of "database at IP address 1.2.3.4 could not be reached," and a caching proxy or web application firewall should not reveal the name or address of the system it sits in front of. If this kind of information is required for troubleshooting, it may be written to the application/system log, but not shown directly to the user or interfacing system. The information in the system log should be tagged with a unique error identifier, and then the user presented with that error identifier, so that issues can still be traced and resolved, but only by personnel authorized to do so.

ix. *Memory Protection*:

Every Information System must implement protections for its memory, to prevent unauthorized code execution (or minimize the chances of successful exploitation). These protections can range from administratively choosing programming languages (or choosing products based on programming language/platform) that do not allow direct memory access or enforce strict bounds checking, to buffer overflow protection (e.g., Data Execution Prevention or DEP), stack canaries, the NX (No-

Execute) bit, and/or Address Space Layout Randomization (ASLR).

XXI. DEFINITIONS

TERM	DEFINITION
Acceptable Encryption Suites	means encryption that meets all of the following requirements: (a) complies with applicable federal, state, and local laws, federal and state Executive Orders, directives, policies, regulations, and standards of industry best-practice; (b) is approved under FIPS 140-2 for use in government; (c) capable of providing authentication assurance according to a certificate trust chain; and (d) is not currently known to be vulnerable to feasible attacks. The category of Acceptable Encryption Suites specifically excludes proprietary (non-public or non-peer-reviewed) encryption, as well as any cipher suite or key length that has been deprecated according to industry best practice or current web browser standards (i.e., Firefox, Chrome, Internet Explorer/Edge). Note that support for Acceptable Encryption Suites is not by itself sufficient: fallback to unacceptable encryption suites must also be explicitly disabled. In particular, as of the drafting of this document, the following algorithms/ciphers are **deprecated and not permitted**: SHA-1, DES, 3DES, RC4, MD5, SSLv2, SSLv3, and TLS-1.0. Acceptable Encryption Suites as of this drafting **include** TLS 1.2 (as long as any weak ciphers are disabled) and TLS 1.3.
Acceptable Use	means a set of rules applied by the owner of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.
Access Coordinator	means the individual identified as being responsible for managing staff access to Information Resources
Access Log	means a list of all requests for individual files that people or bots have requested from a Web site.
ACIO	means Assistant Chief Information Officer.
ACLs	Means Access Control List. It is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges.
Active Directory	means the directory used by the Commonwealth to maintain the identities of users within its network
Active Monitoring	means injecting test traffic into a network and then measuring its performance. These tests can either be one-way or round trip
Agency	means one of the constituent offices, departments, hospitals and Soldiers' Homes defined as being within EOHHS and included in Attachment 9.
Aggregated Logging System	means a system that gathers up disparate log files for the purposes of organizing the data in them and making them searchable.

TERM	DEFINITION
Aggregate Report	means a report that collects data within a selected criteria and aggregates it into totals.
APD	means Advanced Planning Document.
ATO	Means Authorization to Operate. This is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations, including mission, functions, image, organizational assets, etc.
Attack Vector	means the method or type of attack used against a computer system or network.
Audit Finding	means the items identified and reported resulting from a process that evaluates audit evidence and compares it against audit criteria.
Audit Log	means a digital record that is created to document when a change is made to a system.
Baseline	means the secure settings and configuration necessary for the protection of the Information Resource. These settings will be modified as updates, patches, code changes, or process changes are incorporated into the Information Resource.
BCP	means Business Continuity Plan. This is a plan to help ensure that business processes can continue during a time of emergency, disaster or any other case where business is not able to occur under normal conditions.
CIO	means Chief Information Officer.
Collaborative Tools	means software tools or applications that support groups of individuals to accomplish a common goal or objective.
Commonwealth	means the Commonwealth of Massachusetts.
Commonwealth Data	means the information created, maintained, or stored by or on behalf of the Commonwealth in whatever form such data is created, maintained, or stored. For purposes of clarification, Commonwealth Data includes Sensitive Information, but may also include information freely available to the public.
Commonwealth Enterprise	means the interconnected system infrastructure, networks, and information systems used within EOHHS.
Compensating Controls	means mechanisms put in place to satisfy a security requirement that are not explicitly as stated, due to legitimate technical or documented business constraints, but still sufficiently mitigate the risk associated with the requirement.

TERM	DEFINITION
Compliance	means evidence of having met a specific set of policies, standards, laws, frameworks regulations, etc.
Concurrent sessions	means when there is more than one user accessing the same computer resource at the same time or in the same predefined period of time
Configuration	means any arrangements to code, updates, patches and processes to an Information Resource.
COOP	means Continuity of Operations Plan. This is a federally-established policy to ensure that critical functions continue and that personnel and resources are relocated to an alternate facility in case of emergencies.
COTS	means commercial off-the-shelf. These are the products packaged solutions which are then adapted to satisfy the needs of the purchasing organization, rather than the commissioning of custom-made, or bespoke, solutions.
CRLs	means Certificate Revocation Lists. It is a list of digital certificates that have been revoked by the issuing Certificate Authority (CA) before their scheduled expiration date and should no longer be trusted.
CSRF	also known as CSRF, Cross-site request forgery. It is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts.
Data Flows	means the movement of data through a system comprised of software, hardware or a combination of both.
Data Mining	means The process of finding anomalies, patterns and correlations within large data sets for the purpose of discovering connections and predicting outcomes.
Development	means a System is in an environment where the structure or operation of that System is being developed or modified in such a way to not impact Production and/or the data contained therein.
Document	means this EOHHS Enterprise Information Security Standards
EMP	means Electromagnetic Pulse. It is considered a short burst of electromagnetic radiation. This kind of burst can come from a variety of sources, including our own sun, but in this case refers to a concentrated pulse from an event like a nuclear detonation that occurs at an extremely high altitude.
Encrypted	means data that has been translated into another form or code to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks.
Endpoints	means remote computing devices such as laptops, desktops, tablets or phones that communicate back and forth with a network

TERM	DEFINITION
EOHHS or the **Secretariat**	means the Commonwealth of Massachusetts Executive Office of Health and Human Services as defined by MGL c. 6A §16 and composed of the Agencies.
EOHHS Environment	means the facilities and information systems under EOHHS control that store, process, or use EOHHS data in any format and for any purpose.
EOHHS Information Resource or **Information Resource**	Information Resources include both technical and non-technical methods of storing, accessing, and processing information. Technical Information Resources include, without limitation: computers (including laptops), servers, printers and other peripherals, smartphones and other mobile devices (including tablets), storage media, network locations or information systems, that are either: 1) developed and/or provided by EOHHS; 2) connected to the EOHHS network, programs, applications, databases, or network shares managed by the Commonwealth or EOHHS; or 3) used to process Commonwealth Data or other Sensitive Information. Non-Technical Information Resources include, without limitation: any printed, handwritten, or other physical forms of Commonwealth Data or other Sensitive Information, such as paper documents and files, microfilm, physical photographs, as well as methods of storing them, such as filing cabinets, desk drawers, and storage rooms.
EOHHS Risk Governance Team	means a group composed of Agency leadership and EOHHS subject matter experts who are able to make determinations and recommendations with respect to risk acceptance for systems with an excessive amount of Risk. Where a System is escalated to the EOHHS Risk Governance Team, the team shall be composed of 1) key leadership from the impacted agencies whose data and environments may be impacted by the Risks which should include the following individuals or their assigns: Commissioner, Chief Financial Officer, Chief Operating Officer, Agency Chief Information Officer, and General Counsel and 2) key subject matter experts from EOHHS IT including the Security Office, IT Operations, and the EOHHS architecture team.
EOTSS	means the Executive Office of Technology Services and Security.
Event	means anything that occurs that impacts operations at EOHHS. Events that are within the scope of *Section X, Incident Response and Security Incident Response Team*, are Reportable Events.
Facility	means any facilities housing EOHHS Information Resources or Information Systems, whether or not owned by an Agency or a third-party, and whether or not operated or staffed by Agency or third-party personnel.
FICAM	means the Federal Identity, Credential, and Access Management (FICAM) Trust Framework Solutions initiative, which is run by the GSA and certifies products and services as FIPS-compliant.

TERM	DEFINITION
Forensic Analyst	is a member of the Security Office generally tasked with assisting with collection of electronic information for forensic matters at EOHHS. With respect to operationalization of this Document, Forensic Analysts are responsible for providing support to the Security Office and to assist with identification of the cause of a Reportable Event and management of tools throughout the Reportable Event to ensure remediation of a Reportable Event.
Form	means the Agency-appropriate identification and classification form an Information System. An example identification and classification form is attached here as Attachment 2.
FTI	means Federal Tax Information. It is a Public Key Certification - A digital certificate containing a public key for an entity and a name for that entity, together with some other information that is rendered un-forgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard.
Gap Analysis	means the comparison of a system or organization's current performance with desired performance or future state.
HIPAA	means the Health Insurance Portability and Accountability Act of 1996. This rule created by The U.S. Department of Health and Human Services established set of national standards for the protection of certain health information. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being.
IDM	means Integrated Data Management. This is the process of bringing many data sources together to aid the daily functions of a business.
Incident Response Lead	is the member of the Security Office tasked with managing implementation and operationalization of *Section X, Incident Response and Security Incident Response Team*.
Information Resources	means the data and information used by an organization.

TERM	DEFINITION
Information Resource Owner or **Owner**	means the individual or group who has the authority to make decisions about an Information Resource. Typically Information Resources will have at least one "owner" who manages or is responsible for the data contained in the Information Resource. Information Systems have two owners: the IT manager for that Information System and the business or programmatic manager who manages the program or data that the Information System supports or uses, respectively.
Information Security Incident or **Incident**	means any situation due to any action or inaction, internally or externally, that does or could lead to an situation including, but not limited to, compromising the confidentiality, availability, or integrity of: 1) the Commonwealth or EOHHS network and/or environment, 2) Commonwealth Data, 3) EOHHS Information Resources, or 4) an EOHHS location.
Information System or **System**	means any application, system, process, database, or other mechanism for using, processing, manipulating, accessing, and/or storing data. Additionally, while the focus of Information System is for electronic data, Information System need not be limited to electronic data and may include non-technical versions of technical processes (e.g.: a paper database of files stored in a filing cabinet).
Information System Classification	means a process in which organizations assess the data that they hold and the level of protection it should be given. A typical system will include four levels of confidentiality: • Confidential (only senior management have access) • Restricted (most employees have access) • Internal (all employees have access) • Public (everyone has access)
ISA	means Information Sharing Agreement. This is a common set of documented principles that organizations have agreed to follow when sharing information with each other.
ITSM	means It Service Management all the activities involved in designing, creating, delivering, supporting and managing the lifecycle of IT services.

TERM	DEFINITION
Key Account Management practices	means a process of tracking and managing accounts critical to an organization
LDAP	means Lightweight Directory Access. This is a client/server protocol used to access and manage directory information.
Linux	means a type of open source operating system. Linux is software that sits underneath all of the other software on a computer, receiving requests from those programs and relaying these requests to the computer's hardware.
Log Correlation Services	means tools that take data from either application logs or host logs and then analyzes the data to identify relationships.
Logical Separation	means maintaining local and virtual connections separately within a network computing environment in order to optimize information security
MAGnet	means Massachusetts Access to Government network. This is the Commonwealth's WAN, or wide area network.
Malware	means malicious code, such as viruses, trojans, worms, spyware, adware, ransomware, scareware, logic bombs, and the like, regardless of how packaged, delivered, or executed (macros, scripts, executables, in-memory exploitation, etc.).
Manager	a designated point of contact responsible for controlling access to a Facility, identifying the individuals authorized to access a Facility, granting physical access to those individuals, and denying access to all others.

TERM	DEFINITION
Memorandum	means an Authority to Operate memorandum or an Operational Risk Assessment memorandum, as applicable, following the form attached here as Attachment 3.
Non-conformance	means instances in which information assets do not meet specifications, standards or requirements in some manner
OCSP	means Online Certificate Status Protocol. It is the Internet protocol used by web browsers to determine the revocation status of SSL/TLS certificates supplied by HTTPS websites.
PACE	the Commonwealth of Massachusetts Human Resources training application and repository.
Personal Identity Verification credential or **PIV credential**	refers to a US Federal government-wide credential used to access government facilities and systems, and has the meaning and requirements given to it under NIST publication FIPS 201-2 (commonly referred to as the "Common Access Card" or "CAC").
PHI	Means Protected Health Information. This is the term given to health data created, received, stored, or transmitted by HIPAA-covered entities and their business associates in relation to the provision of healthcare, healthcare operations and payment for healthcare services.
Phishing	means a fraudulent attempt to obtain sensitive information such as usernames, passwords, financial information, or other sensitive information by disguising the communication as one from a trusted entity such as a bank, helpdesk, or software/hardware vendor. Phishing is often, though not always, conducted over email.
PII	Means Personally Identifiable Information. This is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Examples of PII may include name, date of birth, place of residence, credit card information, phone number, race, gender, criminal record, age, and medical records
POA&M	means Plan of Actions and Milestones.
Privacy Incident	means any situation due to any action or inaction, internally or externally, that leads to an exfiltration of Sensitive Information as further defined in Agency privacy policy and procedures.
Production	means a System is in an environment that is in use for business operations that typically contains live and not test data.
Project Intake Form	means the document utilized by EOHHS to initiate or request a project within the Enterprise

TERM	DEFINITION
Public-facing	means any free or paid application or system that the public can access. Public-facing systems often comprise a public-facing component as well as a private side that is available only to internal staff.
Reportable Event	means any Event that impacts EOHHS Information Resources and which is reportable under *Section XI, Incident Response and Security Incident Response Team* as described further in Section XI.a.ii. All Incidents are Reportable Events and are a subset of Reportable Events.
Respondent	the group of application staff, facility staff, and Agency operations staff that respond to an assessment questionnaire.
Risk	A Risk is comprised of the following equation: Threat x Vulnerability = Risk. There is no Risk if a Threat or Vulnerability does not exist. Likewise, a minor Threat or Vulnerability might accompany a high level of Risk depending on the corresponding factor in the equation. NIST 800-30 defines Risk as, "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."
Risk Assessment	means an assessment identifies the various information assets that could be affected by a cyber attack (such as hardware, systems, laptops, customer data, and intellectual property), and then identifies the various risks that could affect those assets.
Risk Governance Team	means cybersecurity governance team whose activities involve the development, institutionalization, assessment and improvement of an organization's enterprise risk management and security policies
Role	means the standard business function performed by the individual with respect to the Information Resource.
SCIO	means the Secretariat Chief Information Officer.
Secretariat Security Liaison	is a member of the Security Office generally responsible for interfacing with Agencies to respond to information security questions and issues. With respect to operationalization of *Section X, Incident Response and Security Incident Response Team*, Secretariat Security Liaisons are responsible for providing support to the Security Office and to work with Agencies to ensure remediation of a Reportable Event.
Security Office	means the EOHHS Security Office.
SEIM	means Security Event & Incident Monitoring system, a database-driven event correlation tool.

TERM	DEFINITION
Sensitive Information	means any Commonwealth Data not made freely available for public consumption whether written, electronic, or otherwise stored, which may include: Protected Health Information, as that term is defined under HIPAA (45 CFR Parts 160 to 164); "personal data," as defined in M.G.L. c. 66A; "personal information," as defined in M.G.L. c. 93H; "personally identifiable information," as used in 45 CFR §155.260; "patient identifying information," as defined in 42 CFR Part 2; and any other individually identifiable information that is treated as confidential under applicable law regulation or other legal obligation to which EOHHS or an Agency is subject (including, for example, any state and federal tax return information or Social Security Administration information) in whatever form such data is created, maintained, or stored.
Sensitive Information, High or **Highly Sensitive Information**	includes, but is not limited to, federal "secret" clearance level materials (and above), personally identifiably AIDS and other infectious disease data, nuclear materials databases, and CJIS data.
Service and Support Desk	means the EOHHS Service and Support Desk, available at (617) 994-5050 or at the email addresses available at http://eohhs-web.EOHHS.govt.state.ma.us/IT/agency-email-addresses.asp.
Session Hijacking	also known as cookie hijacking and it is the exploitation of a valid computer session. It is to gain unauthorized access to information or services in a computer system.
Session replay	it is the ability to replay a visitor's journey on a web site or within a mobile application or web application. Replay can include the user's view (browser or screen output), user input (keyboard and mouse inputs), and logs of network events or console logs.
Shared Drives	means drives that let users quickly share files from computer-to-computer, allowing all users on the network drive to access stored files and share files with one another.
SIRT	Means Security Incident Response Team. This is a group within EOHHS tasked with responding to an Incident.
SLA	means service-level agreement. It is a commitment between a service provider and a client. Particular aspects of the service – quality, availability, responsibilities – are agreed between the service provider and the service user.

TERM	DEFINITION
SMTP	means Simple Mail Transfer Protocol. It is a TCP/IP protocol used in sending and receiving e-mail. is a communication protocol for electronic mail transmission.
Social Engineering Attack	means an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain
Supporting Infrastructure	means electricity, data/voice transmission lines (such as fiber, coaxial, twisted-pair, POTS, or otherwise), wireless (including WiFi, GSM, CDMA, LTE, LMDS, WiMax, point-to-point radio, etc.), and any other telecommunications infrastructure providing service to or otherwise supporting a Facility or Information System. Supporting Infrastructure includes redundant infrastructure, if that redundancy is relied upon to satisfy any controls or requirements outlined in this Document.
Test	means a System is in an environment where the structure and operation of the System may be tested in such a way to not impact Production and/or the data contained therein.
Third Party	means a party external to EOHHS who provides or received data from EOHHS. This could include vendors who receive, process, or use EOHHS information. It could also include federal and state teaming partners who provide us information, such as the Centers for Medicare & Medicaid Services, the Social Security Administration, the Internal Revenue Service, the Department of Revenue, and others.
Third Party Agreement	means an agreement with a third party for the transfer of our data and/or the provision of services. Depending on context, this may mean an agreement with a vendor who is receiving, processing, or using our data or an agreement with a trading partner providing us data. As required by these Standards, we may have imposed on us or will need to impose specific privacy and security obligations.
Threat	A Threat is defined as any natural or man-made circumstance that could have an adverse impact on an organizational asset. This includes Threats like building a data center in an earthquake prone area to allowing data entry into a form field without validating, sanitizing or filtering that entry first. NIST 800-30 defines Threat as “Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.”

TERM	DEFINITION
TLS	means Transport Layer Security. It is a protocol that provides authentication, privacy, and data integrity between two communicating computer applications. It's the most widely-deployed security protocol used today and is used for web browsers and other applications that require data to be securely exchanged over a network, such as web browsing sessions, file transfers, VPN connections, remote desktop sessions, and voice over IP (VoIP).
Unix	means an open source, portable, multiuser operating system originally developed in 1969
Virus	A Virus is defined as a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.
VoIP	Means Voice Over Internet protocol. It is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.
Vulnerability	A Vulnerability is defined as the absence or weakness of a safeguard in an asset that makes a Threat potentially more likely to occur, or likely to occur more frequently. Common Vulnerabilities are poor coding practices or not changing the default admin password in a System once acquired. NIST 800-30 defines Vulnerability as “Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.”

Changelog			
Date	**Version**	**Author**	**Change Summary**
12/9/2019	1.0	EOHHS Security Office	Effective Date – Approved by Secretary Sudders

ATTACHMENT 1: EOHHS ACCEPTABLE USE POLICY

Commonwealth of Massachusetts
Executive Office of Health and Human Services

INTRODUCTION

This Policy applies to all Users of EOHHS Information Resources. In furtherance of your job duties, you may be required or requested to access EOHHS Information Resources and only for the purpose of completing such duties. Your use of EOHHS Information Resources may be monitored, recorded, and audited. EOHHS has the right to review your files and emails at any time and for any reason without your prior consent. **Especially when using Technical EOHHS Information Resources (as defined below), you should have no expectation of privacy.** Unauthorized or improper use of EOHHS Information Resources may result in disciplinary action, as well as civil and criminal penalties.

You are responsible for using EOHHS Information Resources responsibly, in accordance with your job duties, and for protecting these resources against unauthorized or unpermitted use.

This Policy updates and supersedes the EOHHS Acceptable Use Policy, Version 1.0, dated 11/17/2015.

This Policy covers the following subjects:

1. Acceptable Use
2. Passwords
3. Equipment
4. Data Handling
5. Communications
6. Incident Reporting

By using an EOHHS Information Resource, you agree to the terms of this Policy.

DEFINITIONS

"Agency" means one of the offices, departments, hospitals and Soldiers' Homes defined as being within EOHHS pursuant to MGL c. 6A §16.

"Commonwealth" means the Commonwealth of Massachusetts.

"Commonwealth Data" means the information created, maintained, or stored by or on behalf of the Commonwealth in whatever form such data is created, maintained, or stored. For purposes of clarification, Commonwealth Data includes Sensitive Information, but may also include information freely available to the public.

"Devices" means a subset of EOHHS Information Resources which includes, without limitation: computers (including laptops), peripherals such as printers and monitors, desk phones, headsets, smartphones, cell phones, portable storage media and other equipment capable of utilizing, accessing, or storing Commonwealth Data or EOHHS Information Resources.

"EOHHS" means the Commonwealth of Massachusetts Executive Office of Health and Human Services as defined by MGL c. 6A §16.

"EOHHS Information Resource" EOHHS Information Resources include both technical and non-technical methods of access to, processing, and storing information. Technical EOHHS Information Resources

include, without limitation: computers (including laptops), servers, printers and other peripherals, smartphones and other mobile devices (including tablets), storage media, network locations or information systems 1) developed and/or provided by EOHHS; 2) connected to the EOHHS network, programs, applications, databases, and network shares managed by the Commonwealth or EOHHS; or 3) used to process Commonwealth Data or other Sensitive Information. Non-Technical EOHHS Information Resources include, without limitation: any printed forms of Commonwealth Data or other Sensitive Information, such as paper documents and files and methods of storing them, such as filing cabinets.

"Policy" means this Acceptable Use Policy.

"Portable Device" means laptops, smartphones, cell phones, tablets, flash drives and other portable devices.

"Sensitive Information". Any Commonwealth Data not made freely available for public consumption which may include Protected Health Information, as that term is defined under HIPAA (45 CFR Parts 160 to 164); "personal data," as defined in M.G.L. c. 66A; "personal information," as defined in M.G.L. c. 93H; "personally identifiable information," as used in 45 CFR §155.260; "patient identifying information," as defined in 42 CFR Part 2; and any other individually identifiable information that is treated as confidential under Applicable Law (including, for example, any state and federal tax return information) in whatever form such data is created, maintained, or stored.

"System and Support Desk" means the EOHHS System and Support Desk, available at (617) 994-5050 or at the email addresses available at http://eohhs-web.EOHHS.govt.state.ma.us/IT/agency-email-addresses.asp.

"User" means any individual who, in the course of doing business, accesses EOHHS Information Resources. Users include all EOHHS employees, workforce contractors, and third party contractors or vendors performing work with or on behalf of EOHHS. Where a member of the public access an EOHHS Information Resource under the direction of or while being attended by a User (even if not permitted to access such EOHHS Information Resource) then that User is responsible for the member of the public's actions.

ACCEPTABLE USE

This section describes the general "do's" and "don'ts" with respect to EOHHS Information Resources and what constitutes generally acceptable and unacceptable use of EOHHS Information Resources.

You should use the EOHHS Information Resources provided to you in furtherance of performing your job duties. In using EOHHS Information Resources, you must comply with all related federal and state laws, policies, and processes for use of EOHHS Information Resources including, but not limited to, compliance with Privacy Act of 1974. In order to do so, you should understand and comply with EOHHS annual training and education requirements and complete Security Awareness, Privacy, and other necessary training modules upon hire and annually thereafter, or on a schedule otherwise required by EOHHS. Those trainings will provide the background and information necessary to abide by precepts of acceptable use. You are required to comply with the guidelines provided in those trainings regarding use of EOHHS Information Resources. If in doubt about a specific activity, you are advised to consult with your manager and/or contact the System and Support Desk to be put in contact with the EOHHS Security Office.

Access to EOHHS Information Resources may only be granted to you if you have a job-related need. Additionally, access may only be granted to you to the extent necessary to complete the scope of your job duties. Accounts to access EOHHS Information Resources are provided to you only for your use of the information system. **Under no circumstances may you share your account information, including passwords, or allow another individual to access EOHHS IT Resources with your account. You are responsible for all actions taken using your accounts.** Additionally, you should not independently grant access to EOHHS Information Systems, unless within the scope of your job duties. In the event you are required to grant access to someone else for EOHHS Information Resources, you should ensure that you are doing so as required by law or based on programmatic need and only to the extent necessary for legal compliance or to fulfill that programmatic need.

Unless expressly part of your job duties, regardless of the type of access you have, you must never attempt to bypass access control measures or view, modify, or delete or destroy parts of any EOHHS Information Resource. If your job duties or responsibilities change, your need to access EOHHS Information Resources may change. Your manager is responsible for communicating those access changes to the System and Support Desk ***immediately.*** To that effect, any new employee access or terminated employee access must also be communicated to the System and Support Desk ***immediately***. If you discover that you have access beyond what is allowed, you must notify your manager and the System and Support Desk ***immediately*** so that your access may be adjusted appropriately.

EOHHS Information Resources are the property of EOHHS and the Commonwealth. EOHHS owns the data created or stored on these systems, including all email messages and the information they contain. **You do not own Information Resources on the EOHHS Network and should have no expectation of privacy in those Information Resources—including your MassMail emails.** If any data must be accessed or reviewed by the EOHHS Security Office during the course of a vulnerability assessment, investigation, or otherwise, the EOHHS Security Office will access such data as needed. Accessing that data will be coordinated—if feasible—through the respective EOHHS ACIO and program or project manager.

Any activity that you take on the network or with respect to EOHHS Information Resources that violates State and Federal law is prohibited. Those activities include using EOHHS Information Resources to copy, distribute, utilize, or install unauthorized copyrighted materials or any activity that might violate law and policy related to information protection (e.g., hacking, spamming, etc.). Furthermore, any activity such as viewing, creating, storing, and/or processing pornographic or other offensive or graphic content on EOHHS Information Resources is prohibited.

In addition, you may be disciplined for undertaking certain activities both within and outside of the workplace that relate to your employment at EOHHS. Activities that will adversely impact the workplace by causing the agency to not operate efficiently or effectively and/or create a hostile work environment include, but are not limited to:

- Sending harassing, threatening or offensive communications to other Users or members of the public; or
- Sending communications, including social media posts, that are disparaging towards or reflect poorly on other Users, the populations served by EOHHS, your Agency, EOHHS, or the Commonwealth.

You may not use EOHHS Information Resources for the purpose of utilizing, creating, storing, and/or processing your personal data, such as music, videos, family photographs, and personal documentation. This includes accessing your personal email accounts and connecting to social media (unless a function of your job duty). Streaming music and videos over Commonwealth networks, unless explicitly required as a function of your work for EOHHS, is also prohibited.

When not using EOHHS Information Resources, you must log off, lock, or terminate your session with those EOHHS Information Resources. You must also ensure that your computer or Portable Device automatically logs off or locks when not in use such that a password is needed to log in to the device. You may not install on any Device an automated sign-on system, password, or access phone numbers; a password must be required to be input by you each time an EOHHS Information Resource is accessed. Failure to abide by these log-on requirements could permit unauthorized access with your credentials.

You are accountable and responsible for all actions you take or which are undertaken with your account credentials while using EOHHS Information Resources. Failure to comply with the requirements set forth in this Policy may result in suspension of your access and/or disciplinary action, up to and including termination of employment or removal from a contract for contractor personnel. In some cases, violations may be grounds for civil action or criminal prosecution, **including fines and/or jail time**. Sanctions for non- compliance will be handled in accordance with applicable laws and regulations, collective bargaining agreements, civil service rules, and/or contractual agreements relating to third-party workforce.

You may seek exceptions to specific requirements in this Policy if absolutely necessary to fulfil your job duties. In order to do so, you must make a request in writing to your Agency's ACIO and corresponding business contact explaining in detail: 1) the acceptable use provision sought for exception, 2) the form of the exception, 3) the business justification for the exception, and 4) why the User cannot perform their job duties without the exception. The exception will be treated as a "Critical" level Risk pursuant to the Authorization to Operate and Operational Risk Assessment Policy and Process. If you are denied an exception, you may not attempt to implement the exception through a workaround or "self-help."

PASSWORDS

All Device passwords (provided by EOHHS or used to access EOHHS Information Resources) must meet the following minimum requirements:

- Be twelve (12) characters in length at minimum; and
- Contain one of the following characteristics:
    - One (1) upper-case letter,
    - One (1) lower-case letter,
    - One (1) number, and
    - One (1) special character (! @ # $ % ^ & * ( ) _ + = [ ] \ | ‘ “ : ;< > ? / .).

The security office recommends that Users try to make longer passphrases. The more seemingly random the passphrase (to others), the better. For example, "P4ssword!" is much less secure than "Mytruckbatterydied!" which is much less secure than "Badtrucknopower!".

Passwords must be changed a minimum of every sixty (60) days and may not be repeated for twenty five (25) iterations. If you have multiple accounts to access EOHHS Information Resources, you must not

use the same password for those accounts. Compromised passwords must be changed immediately. If you believe that one of your Information System accounts has been compromised, even if you are unsure of that, err on the side of caution and change your password, even if not directed to do so.

Passwords or any other authentication mechanism must never be stored in printed or written form in any easily accessible place. If passwords are stored digitally, they must not be stored in a clear-text or human-readable format. The Security Office recommends that you never store passwords in an unsecured fashion. Ideally, you should memorize your passwords. If you cannot memorize your passwords, write them down in a place where they will not be easily found (e.g.: store them in a locked drawer, cabinet, or your wallet) or store them digitally in an encrypted format.

Passwords must not be shared or disclosed with anyone, including other EOHHS employees. System and Support Desk staff will never ask you for your password and you should not share your password with System and Support Desk staff. Do not allow web browsers or applications to store passwords and login information. If possible, you should shield keyboards from view when passwords are being entered.

EQUIPMENT

You may use EOHHS-provided Devices to access and store Commonwealth Data and other EOHHS Information Resources. You may sometimes use personally-owned Devices to access Commonwealth Data and other EOHHS Information Resources. The conditions under which you may use a personally-owned Device are described further in this Section. Some Commonwealth Data and EOHHS Information Resources may require special configurations or may be limited in how or where they may be accessed. You must consult with the "owners" or managers of those EOHHS Information Resources to ensure that access is being conducted appropriately.

You must abide by all policies and procedures related to the use of Devices and other office equipment. The most current versions of any policies and procedures will be posted on the Security Office Intranet site, at http://eohhs-web.EOHHS.govt.state.ma.us/wp/informationsecurity.aspx. Devices and other office equipment are provided by EOHHS for official use only and in furtherance of your job duties. EOHHS does not condone personal use of EOHHS-provided Devices. Any Device that uses, accesses, or stores Commonwealth Data, including personal Devices, may be monitored, recorded, and audited. EOHHS has the right to review any information accessed, stored, printed, copied, or otherwise utilized on Devices at any time and for any reason.

Any Device used to access or process EOHHS Information Resources must be password protected. You must also ensure any Device used to access or process EOHHS Information Resources automatically locks after a time period consistent with EOHHS requirements and that a password is required to unlock the Device. Consistent with this, you must not program any Devices with automated sign-on sequences, automated password completion, or remote access phone numbers; you must enter a password each time you access a Device.

Downloading and installation of software applications onto EOHHS-provided Devices is prohibited without prior approval. You must not circumvent administrative lockouts or permissions in an attempt to install such software applications. Altering code, introducing malicious content, tampering with another person's account, denying service, port mapping, or engaging a network sniffer outside of the scope of your explicit job duties is prohibited. Even if you have a legitimate job-related reason to engage in these activities, you must seek approval as required by EOHHS.

In order to use a personally-owned Device to access EOHHS Information Resources, you must: 1) receive permission from your supervisor to use personally-owned equipment and 2) present the personally-owned equipment to the EOHHS Security Office for inspection and certification to use the personally-owned equipment. The Security Office or your supervisor may determine that access to EOHHS Information Resources may need to be conducted through VPN. Additionally:

a) EOHHS may monitor, record, and audit use of personally-owned Devices when accessing EOHHS Information Resources. You should not have an expectation of privacy when using the personally-owned Device to access EOHHS Information Resources.
b) EOHHS may require specific encryption, virus protection, anti-spyware, firewall/intrusion detection, and other software or settings to be installed on the personally-owned Device prior to that Device accessing EOHHS Information Resources. EOHHS may also require that such software is configured to meet EOHHS configuration requirements prior to connection to EOHHS networks. EOHHS may further require that certain software or certain kinds of software not be installed on a personally-owned Device due to the security vulnerabilities that may be introduced. You must implement those requirements and may not modify or deviate from requirements.

You may not use personally-owned Devices to store Commonwealth Data or EOHHS Information Resources. You should only store Commonwealth Data or EOHHS Information Resources on the appropriate network drive (individual or shared) to which you have access or EOHHS-provided portable media which has been provided for the purpose of storing specific Commonwealth Data or EOHHS Information Resources. Any removable or portable media used to store such information must be encrypted and password protected. When not in use, portable media must be secured in a desk or filing cabinet which can lock or be carried with you securely at all times.

The foregoing requirements related to Devices also apply Portable Devices. However, there are a number of additional requirements specific to Portable Devices.

Portable Devices, to the extent technically possible, must have disk-level encryption installed and enabled. Portable Devices should never be used to store sensitive Commonwealth Data, including PII or PHI. You are ultimately responsible for the Portable Devices and will be responsible for the loss of stored data on a Portable Device if the Portable Device is lost or stolen. The Security Office recommends that you keep devices under your physical control at all times and take all necessary precautions to protect Portable Devices against loss, theft, damage, abuse, or unauthorized use.

When traveling, you must keep Portable Devices under your physical control at all times. Consequently, you must not place any Devices in checked luggage. Additionally, you must not store any Devices in a publically accessible locker or storage space (such as at an airport, a train or bus station). At security checkpoints, such as airport security, you must place any Devices on the conveyor belt only after the belongings of the person ahead of you have cleared the scanner. If delayed, you must visually monitor the Devices to the extent possible until you can retrieve the Devices.

You must avoid leaving any Devices in in a hotel room. If you must leave a Device in a hotel room, you must lock it inside a safe provided by the hotel. If a safe is not available, you must keep the Device with you. You must never leave a Device unattended in an automobile, even if the vehicle is locked. Public or

shared computers (e.g. hotel business computers, library computers, etc.) should not be used to access EOHHS Information Resources or Webmail access.

Portable Devices must not be simultaneously connected to the EOHHS network and any kind of non-EOHHS network connection (including physical, wireless, or other connection). The exception to this is where a Portable Device is a smartphone and is required to connect to both a cellular network to function and an EOHHS wireless network.

You may be asked to return or hand-over Portable Devices to EOHHS for security-related repairs and inspections. Users must comply with these requests promptly and make the device completely available to EOHHS. Failure to do so may result in the loss of privileges to keep the Device (if an EOHHS provided Device) or access the EOHHS network with it (if a personally-owned Device). In the course of an inspection or update, EOHHS may need to make modifications to the Device, including software updates, which may delete all data on the Device. EOHHS has no responsibility for data improperly stored on a Device. If, during the course of an inspection, the Security Office finds software EOHHS determines should not be on a device, that software is subject to deletion without notice. This includes screen savers, games, software downloaded from the Internet, software brought from home, and software provided by other state agencies.

Unsecured wireless communication protocols (like Bluetooth and Infrared transmission) must not be used at an EOHHS location or when accessing EOHHS Information Resources. Wireless communication protocols, including the EOHHS Public Access Wi-Fi, must not be used to transmit PII, PHI, SSA and FTI data, or similarly sensitive data.

DATA HANDLING

You must ensure the proper handling of Sensitive Information according to applicable requirements, including but not limited to federal and state law, third party agreements, Commonwealth Executive Orders, and EOHHS policy and process. Your Agency may also have additional specific data privacy requirements with respect to Sensitive Information you may access. You must abide by those requirements at all times.

You must not divulge any Sensitive Information obtained through or in connection with your employment with the Commonwealth to any unauthorized person or organization or in violation of applicable requirements including, but not limited to federal and state law, third party agreements, Commonwealth Executive Orders, and EOHHS policy and process.

You may only use Sensitive Information in furtherance of and consistent with your job duties. You must not use, or permit others to use, any Sensitive Information that is not available to the general public for private purposes or personal use. You may only modify Sensitive Information in furtherance of and consistent with your job duties. You must not remove official documents or records from files or otherwise alter Sensitive Information for personal or inappropriate reasons. Falsification, concealment, mutilation, or unauthorized modification of Sensitive Information is prohibited and, in many cases, may subject you to criminal and civil penalties.

If you must dispose of Sensitive Information, you must do so properly. EOHHS requires that information be disposed of pursuant to the requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88. This means that:

(a) Non-technical EOHHS Information Resources (e.g.: paper documents) must be appropriately shredded such that the information they contain cannot be reconstructed. If your location has EOHHS-provided shredder bins, you must dispose of Sensitive Information there.
(b) Technical EOHHS Information resources must be completely wiped prior to disposal such that the data once stored on them is practically unrecoverable. You must contact your local IT Site Owner or the EOHHS Security Office to assist you with such destruction.

Prior to any data deletion or destruction, ensure you are in compliance with records retention guidelines pursuant to the Massachusetts Statewide Records Retention Schedule.

COMMUNICATIONS

Internet activities that may impact the confidentiality, integrity or availability of EOHHS information and information systems, or cause degradation of network services, are prohibited unless otherwise expressly permitted for official duties. You should not use EOHHS Information Resources to browse the internet for personal use. In no event may you host, set up, administer, or operate any type of public-facing server on any EOHHS network. Additionally, the use peer-to-peer (P2P) file sharing over the EOHHS network or on EOHHS Information Resources is prohibited. This includes any storage platforms such as Dropbox and Google Drive.

You may only use your MassMail email address in furtherance of your job duties and must not use it for personal matters. Most emails transmitted over MassMail are considered public records and may be disclosed if requested. Except for limited personal use, you must not transmit or distribute via EOHHS email any non-work related information about another employee. Improper use includes, but is not limited to broadcasting inappropriate messages (e.g., unsolicited personal views on social, political, religious, or other non-business matters; email chain letters; etc.) to Commonwealth mailing lists or other Users.

You may not transmit or store Commonwealth Data to or from personal email accounts (e.g. Yahoo, Gmail, Comcast, etc.). You must also not transmit Commonwealth Data to third parties via email outside of the scope of your job duties. You should not forward e-mail messages received through MassMail to addresses outside of MassMail unless required by your job duties.

MassMail email addresses are never to be sold or otherwise shared, disseminated, or used in any unofficial manner. You are encouraged to use your MassMail addresses to sign up for third-party work-related electronically distributed newsletters or magazines. You are, however, prohibited from using your MassMail address to sign up for third-party non-work-related electronically distributed newsletter or magazine.

If you receive an email message from any source requesting personal or organizational information or asking to verify accounts or security settings (a phishing email), you must treat the receipt of the email as a “Security Incident.” Similarly, you should treat emails that you receive from an unknown third party that implore you to click a third party link or download an attachment as “Security Incidents.” Do not click the link, download the attachment, or open the attachment. You should follow the incident reporting process outlined in the “Incident Reporting” section below in all of those cases. Additionally, you should also delete the message after forwarding it.

All official Commonwealth email communications must be conducted through a MassMail email account. Personal or private email addresses should not be used for business purposes. Use of personal or private email addresses may make the contents of those email accounts subject to disclosure and review by the Commonwealth and/or adverse third parties in a claim or cause of action against the Commonwealth.

EOHHS reserves the right to log and monitor all traffic that enters or leaves Commonwealth managed networks. Access and use of email via a technical EOHHS Information Resource should not be considered private.

Users who are identified as being a source of unauthorized intrusion or otherwise conducting prohibited activities on the network may be disconnected from the network. Re-establishing connection will be at the discretion of the EOHHS Security Office in consultation with the User's senior management.

All electronic messages created or received by state employees using the Commonwealth's information technology resources are public record under the Commonwealth's Public Records Law, M.G.L. c. 66, § 10, and most are therefore subject to public scrutiny. All such electronic messages are also records subject to the Commonwealth's Records Conservation Law, M.G.L. c. 30, § 42, and must be disposed of, or retained according to the agency's disposition schedule and the records retention guidelines pursuant to the Massachusetts Statewide Records Retention Schedule. The majority of such messages are also potentially discoverable communications for purposes of litigation. Agency heads and organization authorities must ensure that all electronic communications, are retained, disposed of, and disclosed, in compliance with the Public Records Law, the Massachusetts Statewide Records Retention Schedule, and the relevant discovery rules.

The Commonwealth VPN Solution provides remote access to a wide variety of technical EOHHS Information Resources for authorized users from any personal computer with a web browser that supports 128 bit encryption. The Commonwealth VPN Solution also provides the ability to telework remotely in emergency, contingency, or COOP situations.

When working at an alternate workplace (including from home), you must follow security practices that are at least as restrictive as those required at your primary workplace. Users who use VPN must protect the privacy and security of all EOHHS data and equipment in the same manner as required when working at an EOHHS location.

INCIDENT REPORTING

All incidents must be reported to the System and Support Desk immediately. An incident may include, but is not limited to, one of the following events:

- Loss or theft of a Device,
- Compromise of your account credentials,
- Loss of Commonwealth Data,
- Inappropriate or misdirected transmission of Sensitive Information,
- Presence of a virus on a Device,
- Suspicious email; and

- Anomalous System performance.

If in doubt, err on the side of caution and report an event as an incident. Failure to report an incident may lead to the impact, extent, or effect of the incident being exacerbated. If you fail to report an incident and it gets worse, you are responsible for the expanded scope of the incident and may be held accountable for such expanded scope.

If you report an incident, you may be contacted by the Security Office to provide additional information or be directed to take steps to resolve the incident. You must comply with such Security Office requests and direction to resolve an incident.

ATTACHMENT 2: INFORMATION RESOURCE INVENTORY FORM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

Application Name: _____

Date: _____

Application Inventory Instructions

This questionnaire is being sent to all application managers in order to inventory all applications within the EOHHS Environment. For purposes of this review "application" is a generic term intended to cover systems, applications, databases, or other mechanisms that hold, transmit, or otherwise process data. The term should be interpreted as broadly and liberally as possible.

The following clarifications and explanations have been included to assist with completing the questionnaire. If you have additional questions, please contact Aaron Weismann at (617) 689-2844 or Aaron.Weismann@State.MA.US.

- Question 1: please provide the name of the application, spelling out any acronyms.
- Question 2: please provide a high-level explanation of your application functionality. We recommend keeping this to a paragraph in length, but more text could be appropriate based on the complexity and functionality of your application.
- Question 3: additional details and explanation have been provided for MassHealth functions/activities
    - Member/consumer assistance – does your application support or is your application involved in activities related to providing assistance to MassHealth applicants or members?
    - Eligibility determinations – does your application support determinations of eligibility for benefits offered by MassHealth?
    - Eligibility appeals – does your application support or is your application involved in appeals for denials of eligibility?
    - Premium billing/co-payment – does your application support or is your application involved in premium billing or co-payments?
    - Managed care/plan enrollment – does your application support or is your application involved in enrollment activities for managed care or healthcare plans supported by MassHealth or otherwise?
    - CAC program – does your application support or is your application involved in activities related to the Certified Application Coordinator program, which is to assist individuals with applying for MassHealth membership?
    - Estate recovery – does your application support or is your application involved in activities related to the MassHealth estate recovery program, which is to reimburse MassHealth from a decedent's estate under certain circumstances for care provided to them by MassHealth?
    - Casualty recovery –does your application support or is your application involved in activities related to the MassHealth casualty recovery program, which is to recover the cost of medical services provided to MassHealth members with respect to an accident or injury, to the extent such costs are reimbursed or otherwise covered by a third party (such as the person or organization that caused the accident or injury, workers' compensation or other insurance)?
    - Premium assistance – does your application support or is your application involved in activities related to the MassHealth premium assistance program, which helps individuals pay for healthcare when they are not eligible for MassHealth coverage, but are eligible for a credit towards private healthcare premiums?
    - Other third party liability (TPL) – does your application support or is your application involved in activities related to the determination of third party healthcare coverage?

  - Oversight/financial integrity – does your application support or is your application involved in activities related to the MassHealth oversight and financial integrity group for activities like fraud prevention?
  - Quality improvement – does your application support or is your application involved in activities related to improvement of benefits and care delivery?
  - Reporting to CMS – to your knowledge, is your application directly or involved with any data reporting to CMS?
- Question 4: please provide a narrative explanation of the architecture/operation of your application.
- Question 5: what kinds of data does your application interact with? The data in the chart is organized as follows:

First Name/Initial	☐	Last Name	☐
Home Address	☐	Home Zip Code	☐
Work Address	☐	Work Zip Code	☐
Provider Number	☐	Employee ID	☐
Drivers License/State ID No.	☐	Financial Account #	☐
Tax ID	☐	SSN	☐
Credit/Debit Card #	☐	FTI	☐
Commonwealth Data	☐	MassHealth Number	☐
Hub Data	☐	MassHealth claims/encounter data	☐
MassHealth eligibility information	☐	MassHealth enrollment information	☐
Other Confidential Information (please specify):_____	☐	Health information (please specify):_____	☐

Key

Personal Information
Financial Information
Health / Claims Information
Federal Tax Information
Federal Hub (HIX) Data – also considered health information
Data generated by the Commonwealth
Other misc. confidential data

Additional details and explanation for each data point have been provided below:

  - First Name/Initial – does your application interact with first names or initials (MassHealth Members, Providers, etc.)
  - Last Name – does your application interact with last names (MassHealth Members, Providers, etc.)
  - Home Address – does your application interact with home addresses (MassHealth Members, Providers, etc.)
  - Home Zip Code – does your application interact with home zip codes (MassHealth Members, Providers, etc.)
  - Work Address – does your application interact with work addresses (MassHealth Members, Providers, etc.)
  - Work Zip Code – does your application interact with work zip codes (MassHealth Members, Providers, etc.)

  - Provider Number – does your application interact with provider numbers (NPIs, etc.)
  - Employee ID – does your application interact with employee IDs (EOHHS employee ID numbers, EINs, etc.)
  - Driver's License/State ID No. – does your application interact with driver's license or other legal state identification numbers?
  - Financial Account # - does your application interact with financial account numbers (bank account, etc.) other than credit and debit card numbers?
  - Tax ID – does your application interact with state or federal tax identification numbers?
  - SSN – does your application interact with social security numbers?
  - Credit/Debit Card # - does your application interact with credit or debit card numbers?
  - FTI – does your application interact with federal tax information, which is a specific kind of information provided by the IRS which contains information obtained from tax returns
  - Commonwealth Data – does your application interact with data generated by the Commonwealth?
  - MassHealth Number – does your application interact with MassHealth Member numbers?
  - Hub Data – does your application interact with data from the federal Hub (part of HIX)?
  - MassHealth claims/encounter data – does your application interact with claims or encounter data for treatment or other healthcare services provided to MassHealth Members?
  - MassHealth eligibility information – does your application interact with information about eligibility for MassHealth benefits?
  - MassHealth enrollment information – does your application interact with information about enrollment for MassHealth Membership?
  - Other Confidential Information – does your application interact with any other information that might be considered "confidential" which is not otherwise included in the above list? Please specify generally what that information is.
  - Health Information – does your application interact with other "health information" which is not otherwise included in the above list? Please specify generally what that information is.
- Question 6: please list the total number of users for your application broken down by internal and external user numbers.
- Question 7: please use the chart to explain what external connections your system has. This should be a comprehensive list of all external access to the system or transmission from the system. For non-EOHHS external connections, please feel free to use a high level of abstraction for the connection (e.g.: DOR, Providers, etc.). For internal systems, please list all systems and sub-systems to which you know your application connects. Please also include an explanation of any acronyms or system function (e.g.: AIMS is the "Account Information Management System" or is a system used for user account access management).
- Question 8: please list the vendors who access the application, whether that application is for development or ongoing access to or management of data. Please list the kinds of data accessible by each vendor. Also, please indicate whether or not (by answering "yes" or "no") there is data not accessible by your vendors.
- Question 9: please indicate whether or not your application is publicly accessible, the kinds of data that are publicly accessible, and whether or not there is data not accessible by the public.
- Question 10: please indicate whether or not your application is accessible by other third parties (including auditors, other agencies, and vendors not performing development or management activities of your application), who they are, what kinds of data is accessible by them, and whether or not there is data not accessible to those third parties.

- Question 11: please indicate all auditing that your application performs (manual or automatic).

Application Name: _____
Date: _____

1. What is the name of your application?
2. Please explain generally what your application does.
3. Please indicate if your application is involved with/supports any of the following MassHealth functions/activities:

Member/consumer assistance	☐	Estate recovery	☐
Eligibility determinations	☐	Casualty recovery	☐
Eligibility appeals	☐	Premium assistance	☐
Premium billing/co-payment	☐	Other third party liability (TPL)	☐
Managed care/plan enrollment	☐	Oversight/financial integrity	☐
CAC Program	☐	Quality improvement	☐
		Reporting to CMS	☐

4. Please describe, at a high level, the architecture of your application.
5. What kinds of data are transmitted, processed, manipulated, stored, collected, or otherwise pass through your application?

First Name/Initial	☐	Last Name	☐
Home Address	☐	Home Zip Code	☐
Work Address	☐	Work Zip Code	☐
Provider Number	☐	Employee ID	☐
Drivers License/State ID No.	☐	Financial Account #	☐
Tax ID	☐	SSN	☐
Credit/Debit Card #	☐	FTI	☐
Commonwealth Data	☐	MassHealth Number	☐
Hub Data	☐	MassHealth claims/encounter data	☐
MassHealth eligibility information	☐	MassHealth enrollment information	☐
Other Confidential Information (please specify):_____	☐	Health information (please specify):_____	

Other data (please specify) _____

6. Approximately how many other users (internal and external) have access to your application?
7. Does your Application interface with other systems? Y ☐ N ☐ (If you respond "Y", please fill out the remaining questions in this section; a chart has been provided for your convenience)

    a. What systems does your Application interface with?
    b. Does your application send or receive data?
    c. For each system with which your application interfaces, please describe how your application interfaces with them (e.g.: one or two-way connections, type of connection, persistence of connection, etc.).
    d. For each system with which your application interfaces, please describe what kind of data is transmitted to and from your Application into the other system. *Please use data types referenced in section 5 of this form*.

Application Name: _____

Date: _____

Interfacing System Name	Program Contact for Interfacing System	Send or Receive Data (or both)	Type of connection (e.g.: interchange, SFTP, etc.)	What data transmitted (Please indicate, where possible, if specially protected data like Federal Hub or data received from the SSA is transmitted)

8. Is your application directly accessible by a third party vendor (e.g.: does a non-EOHHS entity do work in your application)? Y ☐ N ☐

    a. Which vendor(s)?
    b. What data is accessible by the vendor(s)?
    c. Is there data that is not accessible by the vendor(s)?

9. Is your Application publicly accessible? Y ☐ N ☐

    a. What data is accessible by the public?
    b. Is there data that is not accessible by the public?

10. Is your application accessible by other third parties (e.g.: auditors, MCOs, EHS constituent agencies, other agencies, etc.)? Y ☐ N ☐
    a. Accessible by whom?
    b. What data is accessible?
    c. Is there data inaccessible to these parties?

11. How does auditing of your application take place, including what logs are maintained, what information is captured in those logs, how long those logs are maintained and how/how often logs are reviewed or analyzed for abnormalities? (A chart has been provided for your convenience)]

Log	Information captured	Length of time log is maintained	Review/analysis method and frequency

Application Name: _____
Date: _____

12. What legal and contractual compliance does your application require? (A chart has been provided for your convenience)

Information Resource:	**BSAS DataMart**
Applicable laws	• MGL c. 66A
Applicable contracts	•
Data Types	• Application logs • Metadata •
Requirements	•

Application Name: _____

Date: _____

Based on the foregoing information, the Security Office has made the following assessment with respect to impact level:

Impact Area	Impact Level	Justification
Confidentiality		
Integrity		
Availability		

Using the high watermark principle, the aggregate impact level for this Application is:

_____.

ATTACHMENT 3: AUTHORITY TO OPERATE/ OPERATIONAL RISK ASSESSMENT MEMORANDUM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

[Authority to Operate/Operational Risk Assessment] Memorandum
for the
Executive Office of Health and Human Services
[Agency]
[Program]
[System]

TO: [Agency ACIO and corresponding business contact]

CC: [EOHHS Risk Governance Team]

FROM: EOHHS Security Office

RE: [System Name] (System)

DATE: [DATE]

I. Introduction

This Memorandum is being transmitted on behalf of the Executive Office of Health and Human Services' (EOHHS) Security Office to identify issues with the named information system and raise awareness of the issues its vulnerabilities pose to the data it contains and the broader EOHHS Environment. The ultimate goal of this Memorandum is to request signoff by the recipients for continued operation of the System. The Security Office recommends that the vulnerabilities not be accepted in their current state and that the issues be remediated within [timeline]. The Security Office further recommends [further recommendations].

[Populate System and program background, including any other considerations for the System]

II. Overview of the Vulnerability/Risks

A. How Risk is Rated

Table 1: Risk Rating in Aggregate

Residual Risk		Likelihood			
		Highly Likely (4)	Likely (3)	Possible (2)	Unlikely (1)
Impact	Critical (4)	Critical (16)	Critical (12)	High (8)	Moderate (4)
	High (3)	Critical (12)	High (9)	Moderate (6)	Low (3)
	Moderate (2)	High (8)	Moderate (6)	Moderate (4)	Low (2)
	Low (1)	Moderate (4)	Low (3)	Low (2)	Low (1)

In order to calculate the risk rating, as outlined in Table 1, above, multiple considerations are taken into account to provide an aggregate rating of the impact of a vulnerability and the likelihood of the vulnerability occurring. The impact is determined by looking at the different kinds of results of a vulnerability being exploited, as outlined in Table 2, below. Once an Impact is identified, it is provided a two numerical ratings. First, it is provided a rating based on the severity of the impact on low to critical scale numerically measured between one and four, respectively. Second, it is provided a rating based on the ease or likelihood of an impact occurring. Again, this is based on the likelihood from low to critical numerically measured between one and four, respectively. By multiplying the two numbers together, the Security Office is able to determine the overall risk rating of a vulnerability.

Table 2: Impact Categories

Impact Categories	Definition
Financial	Financial impact to the Commonwealth based upon a risk being realized.
Reputational	Impact of a loss of confidence from its personnel, constituents, business partners and regulators, which would degrade the Commonwealth's reputation.
Legal and regulatory	Impact could result in observations, recommendations and/or comments from other state entities and/or federal oversight agencies and/or regulators
Operational	The operational impact to processes, people and technology in which Commonwealth employs to achieve its strategy and normal business operations.

Impact Rating	Impact Measurement
Critical	4
High	3
Moderate	2
Low	1

B. System Risks

The following vulnerabilities have been identified for the System:

Finding Group	NIST Control/Policy Impacted	Key Observation	Suggested Remedies from Architecture and Security Teams	Review comment Project	Estimated Fix Date	Risk Rating
Application						

1						
Database						
Quality Assurance						

III. Identification of Risk

A. Breakdown of Vulnerabilities by Risk Level:

Critical		
High		
Moderate		
Low		
		Total Vulnerabilities

Aggregate Risk Level:

B. Next Steps

[Identify recommendations for System, including escalating to the EOHHS Risk Management Team]

IV. Security Office Comments

[Observations, recommendations, other relevant information, etc.]

To Be Executed After Meeting with the EOHHS Risk Governance Team:

After the conclusion of the EOHHS Risk Governance Team Meeting(s) for the System, we have determined:

	To resolve the vulnerabilities in full prior to promoting the System to production

	To accept that the System has potentially significant vulnerabilities that may result in a loss of confidentiality, integrity, or availability of data in the System; to permit the System to operate "as-is" and resolve the vulnerabilities within the next [(1-12) months/(1-3) years]; and develop a remediation plan to be submitted to the EOHHS Security Office within the next 60 days for review and recommendation.

By signing below, we will ensure appropriate remediation of the System. We understand that the Security Office may be required to take additional action based on the contents of the Memorandum, including providing a copy of this Memorandum to EOTSS and other oversight agencies as required by law or policy.

Signed:

[Name, Title ACIO]	Date
[Name, Title Business Contact]	Date

ATTACHMENT 4: CHAIN OF CUSTODY FORM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

Name Of Affected	
Name of Submitter	
Date/Time	
Location	
Incident #	

Description of Evidence	
Item # (mark evidence)	**Description (Model, Serial, Condition)**

Chain of Custody				
Item #	**Date/Time**	**Released By (Signature)**	**Received By (Signature)**	**Comments/Location**

Authorization for Disposal

Evidence recorded and stored for incident # ____ may be destroyed or released to the released to the rightful owners

☐Evidence will be destroyed

- Items to be destroyed
- Signature of person releasing evidence _____
- Signature of person destroying evidence _____
- Signature of person witnessing destruction _____

☐Evidence will be released to owner

- Items to be released
- Signature of person releasing evidence _____
- Signature of person receiving evidence _____

ATTACHMENT 5: SIRT EVIDENCE FORM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

Incident Response Lead

Summary of Details		
Date/Time		
Name of affected application(s)	•	
Servers, Desktops, hardware affected (include IPs)	•	
External IPs (if applicable)	•	
Attack Vectors (if known)		
Forensic tools being used	•	
Affected Users		
Environment(s) Affected	☐Development ☐QA	☐Test ☐Production

Checklist items

Logs gathered and secured?	☐Yes	☐No
Was the attack occurring prior to being reported?	☐Yes	☐No
• If so, is there evidence available?	☐Yes	☐No
Does evidence need to be preserved for prosecution?	☐Yes	☐No

Analysis

Recommendations for Containment and/or Eradication

Recommendations for Remediation	
Staff Needed for Remediation	
Name	**Role**
Resources needed for Remediation (software patch, tool purchase, etc.)	

Next Steps

Priority	
Business Impact	
Information Impact	
Recovery Impact	
Contact Information for Response Team	
Name and phone number	**Role**

Are external organizations required to assist? ☐Yes ☐No

Contact Information for External Organizations	
Name and phone number	**Role**

Policies and Procedures for Response (if available)
•

Response (internal, external)

Additional SIRT members needed

Name	Role

Information Security Rating

Impact	Characteristics
High	• Threat to human safety. • Adverse impact on a "Critical" or "High" risk rated information asset, including infrastructure, applications and services (see Asset Management Standard). • Financial or legal liability equal to $1m and above to the Commonwealth. • Potential compromise of information classified as confidential information, including PII and other regulated information.
Medium	• Adverse impact on a "Medium" risk rated information asset, including infrastructure, applications and services (see Asset Management Standard). • Financial or legal liability between $1m and $100,000. • Potential compromise of information not intended for public disclosure.
Low	• Adverse impact on a "Low" risk rated information asset, including infrastructure, applications and services (see Asset Management Standard). • Financial or legal liability of less than $100,000.

ATTACHMENT 6: SIRT RESPONSE FORM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

The following form should be filled out by the designated team member(s) who will be providing a response to the public or internally to the organization

Name of Responders	Contact Information

Impact

Business Impact	
Information Impact	
Recovery Impact	
Summary of Details	
Audience to be Notified	Public, Colleges, Hospitals, Internal Users
Method of Communication	Email, Telephone, Television, Letter
Time and Date of Incident	
Affected Clients/Business	Internal Users, Website visitors, Payroll
Details on Information Impact	Proprietary information, PHI, Website defacement
Current Status of Incident	Ongoing investigation, Contained, Stopped
What is Being Done	Vendor contacted for patch, Police looking to make arrest, Anti-virus updates being made
Who is Involved	Police, CISO, CIO, FBI

Information Security Impact Rating

Impact	Characteristics
High	• Threat to human safety. • Adverse impact on a "Critical" or "High" risk rated information asset, including infrastructure, applications and services *(see Asset Management Standard).* • Financial or legal liability equal to $1m and above to the Commonwealth. • Potential compromise of information classified as ***confidential information,*** including PII and other regulated information.
Medium	• Adverse impact on a "Medium" risk rated information asset, including infrastructure, applications and services *(see Asset Management Standard).* • Financial or legal liability between $1m and $100,000. • Potential compromise of information not intended for public disclosure.
Low	• Adverse impact on a "Low" risk rated information asset, including infrastructure, applications and services *(see Asset Management Standard).* • Financial or legal liability of less than $100,000.

ATTACHMENT 7: SIRT LESSONS LEARNED FORM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

Lessons Learned	
Date	
Time	
Location	
Coordinator	
Incident #	
Attendees	

Summary of Incident
What was done right?
What could be done better?
Recommendations for improvement
Create/Update Policies, Procedures or Training?

Action Items	Person Responsible	Deadline

ATTACHMENT 8: SIRT INCIDENT FORM

Commonwealth of Massachusetts
Executive Office of Health and Human Services

Incident Response Lead

Name	
Date	
Department and Role	
Email Address	
Location	
Phone	

Incident Reporter

Name	
Date	
Department and Role	
Email Address	
Location	
Phone	

Incident Details

Time and Date of Incident	**Location**
Incident #	
Description of Incident and Type	
Current Status of Incident	
List of Affected Resources (include applications, servers, users, groups, etc)	
Does this appear to require forensics? Explain why	

Does this appear to have legal, criminal or litigation ramifications? Explain why

Recovery Time Expectations
Stakeholders that need to be notified
Associated forms filled out for investigation and data collections
Containment Measures
Evidence Collected
Next Steps

ATTACHMENT 9: SIRT TEAM COMPOSITION BY AENCY

Commonwealth of Massachusetts
Executive Office of Health and Human Services

EOHHS (including IT, HR, Finance, the Secretary's Office)	•
MassHealth (including HSN)	•
Department of Transitional Assistance	•
Department of Public Health	• Eileen Sullivan, Elizabeth Scurria Morgan, Lakeisha Applegate, Kelly Driscoll, Al Williams (DPH non-hospital), Jeanne Cannata (DPH hospitals)
BORIM	•
Department of Mental Health	•
Department of Developmental Services	•
Department of Children and Families	•
Department of Youth Services	•
Massachusetts Rehabilitation Commission	•
Massachusetts Commission for the Blind	•
Massachusetts Commission for the Deaf and Hard of Hearing	•
Executive Office of Elder Affairs	•
Veterans Affairs	•
Holyoke Soldiers' Home	•
Chelsea Soldiers' Home	•
Office of Refugees and Immigrants	•

Privacy Officers and/or Designated Legal Contact by Agency

EOHHS	• Sarah Ricardi
MassHealth	• Sarah Ricardi
Department of Transitional Assistance	•
Department of Public Health	• Lakeisha Applegate
BORIM	•
Department of Mental Health	•
Department of Developmental Services	•
Department of Children and Families	•
Department of Youth Services	•
Massachusetts Rehabilitation Commission	•
Massachusetts Commission for the Blind	•
Massachusetts Commission for the Deaf and Hard of Hearing	•
Executive Office of Elder Affairs	•
Veterans Affairs	•
Holyoke Soldiers' Home	•
Chelsea Soldiers' Home	•
Office of Refugees and Immigrants	•