EOHHS ACCEPTABLE USE POLICY (AUP)

EOHHS INFORMATION SECURITY OFFICE

Version 2.1 (03/31/2023)

Commonwealth of Massachusetts Executive Office of Health and Human Services

Table of Contents

Executive Summary

The EOHHS Acceptable Use Policy (AUP) outlines more specifically tailored requirements, in addition to the EOTSS Acceptable Use Policy. Compliance to both AUPs by all Users is mandatory.

Some of the key topics covered include, but are not limited to, the following:

Regulated Data – Use of third party regulated data must adhere to the requirements of the regulating third party.

No Expectation of Privacy – Users do not own EOHHS Information Resources and should have no expectation of privacy when using EOHHS Information Resources.

Use of EOHHS Information Resources – EOHHS prohibits Users from using EOHHS Information Resources in a manner that violates State or Federal law, Commonwealth Executive Orders, applicable regulatory or contractual obligations and/or agency-level, EOHHS or EOTSS policies, standards or processes.

Equipment – Use of a personally owned device to access EOHHS Information Resources while working remotely is expressly prohibited. The use of portable media is expressly prohibited without prior authorization.

User Access **–** Users are only permitted to access EOHHS Information Resources in furtherance of their job duties.

Incident Reporting – Security Incidents must be reported to EOHHS immediately whenever possible, or within thirty (30) minutes of discovery. See Section 7.14 for additional information, including whom to contact in the event of an actual or potential Security Incident.

Specific details for this topics, and additional topics, are included in the full policy below.

1. Purpose

The Executive Office of Health and Human Services (EOHHS) Acceptable Use Policy (the "AUP" or "Policy") documents the responsibilities necessary to protect and preserve the confidentiality, integrity, and availability of EOHHS Information Resources. EOHHS Information Resources include, but may not be limited to, Commonwealth Owned Data or information systems that process, store, or transmit Commonwealth Owned Data to support EOHHS's organizational operations. This Policy is an enhancement to, not a replacement for, the EOTSS AUP.

NOTE: All EOTSS security policies and standards are available at https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards

2. Impact

This AUP exists to protect EOHHS Information Resources. Inappropriate use of EOHHS Information Resources could lead to a Security Incident, the loss or theft of sensitive/regulated data, and/or legal action.

3. Scope

This Policy applies to the use of information, information systems, electronic and computing devices, applications, and network resources used to conduct business on behalf of EOHHS.

This Policy applies to all agencies within EOHHS and to all EOHHS employees, contractors and vendors, as well as any other authorized persons who access, use, or disclose EOHHS Information Resources (hereinafter referred to as "Users").

4. Definitions

"Agency" means any of the offices, departments, hospitals, Soldiers' Homes, or any entity within EOHHS, as defined under M.G.L. c. 6A, §16.

"Commonwealth" means the Commonwealth of Massachusetts

"Commonwealth Owned Data" means the information processed, stored, or transmitted by or on behalf of the Commonwealth or EOHHS in whatever form such data is processed, stored, or transmitted. For purposes of clarification, Commonwealth Owned Data includes information of all classifications.

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

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

"EOHHS Information Resources" means data and information assets used or owned by EOHHS, including, but not limited to: computers (including laptops and other Devices), emails, servers, printers and other peripherals (such as filing cabinets), smartphones and other mobile devices (including tablets), storage media, network locations or information systems that are developed or provided by EOHHS or connected to the EOHHS network, programs, applications, databases, and network shares managed by the Commonwealth or EOHHS or used to process Commonwealth Data or other Sensitive Information. EOHHS Information Resources are inclusive of Commonwealth Owned Data and Sensitive Information, in all formats (such as paper documents and electronic records).

"EOTSS Security Operations Center" means services including Security Information and Event Management (SIEM), vulnerability management, threat intelligence, and security incident response and reporting programs. EOTSS Security Operations Center is available at eotss-soc@mass.gov.

"Helpdesk" means the EOHHS Helpdesk, available at (617) 994-5050 (option 2) or at the email address systemssupporthelpdesk@mass.gov

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

"Security Incident" means any situation, due to any action or inaction, internally or externally, that does or could lead to a situation including, but not limited to, compromising the confidentiality, availability, or integrity of 1) the Commonwealth or EOHHS network and/or environment; 2) EOHHS Information Resources or; 3) an EOHHS location.

"Sensitive Information" The Commonwealth classifies data into three categories: Confidential, Internal Use Only, and Public. For the purpose of this Policy "Sensitive Information" collectively refers to all Confidential and/or Internal Use Only data as defined in the EOTSS Asset Management Standard document (available at mass.gov), unless otherwise explicitly stated. Sensitive Information may include Protected Health Information (PHI), Personally Identifiable Information (PII) and any other information classified as Confidential and/or Internal Use Only.

"User" Includes all EOHHS employees regardless of type (Ex. full-time, part-time, temporary, seasonal, intern), workforce contractors, and third-party contractors or vendors performing work with or on behalf of EOHHS and who 1) connect to the Commonwealth's network; 2) utilize EOHHS Information Resources or; 3) have access to Commonwealth Owned Data.

5. Compliance

Compliance with this AUP is mandatory for all Users. Failure to adhere to this AUP or any unauthorized or improper use of EOHHS Information Resources or Commonwealth Owned Data may result in disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including termination of employment and/or assignment with the Commonwealth. In some cases, violations may be grounds for civil action or criminal prosecution, **including fines and/or imprisonment**.

Exceptions to any part of this AUP must be requested via email to the Security Office. A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the EOHHS Chief Information Security Officer or their designee.

6. Responsibilities

6.1 EOHHS Security Office

EOHHS Security Office is responsible for the development and ongoing maintenance of this Policy as well as monitoring compliance. It may enlist other departments to assist with the enforcement of this AUP.

6.2 Users

Users are responsible for (1) reading, understanding and complying with this AUP and the EOTSS Acceptable Use Policy; (2) exercising reasonable judgement when interpreting this AUP; and (3) seeking clarification regarding the meaning or practical application of this Policy as needed from their manager. **Users of EOHHS Information Resources must comply with both the EOTSS Acceptable Use Policy and this Acceptable Use Policy**.

7. Policy Statements

7.1 General and Acceptable Use

Users must use EOHHS Information Resources only in furtherance of organizational goals, priorities, and in performance of job duties. Users must comply with relevant enterprise, Secretariat, and agency-level policies, as well as all relevant federal and state laws.

7.2 Regulated Data

Users within EOHHS agencies that have regulated data or receive third party regulated data must adhere to the requirements of the regulating third party (e.g., SSA, DOR, CMS, IRS, etc.). For clarification on the definition, use, and requirements of third party regulated data, refer to the regulations set by the respective regulating third party and any documented agreement between said third party and EOHHS agencies.

To further clarify, regulated data may not be accessed, used, stored, or transmitted by any method not explicitly approved by the regulating authority. This includes, but is not limited to, local storage, network storage, cloud storage (government cloud or otherwise), email, chat, virtual meetings and screenshares.

Users are responsible for communicating to their supervisor any questions or concerns related to their access, use, or transmission of regulated third party data.

7.3 Training and Awareness

7.3.1 Users must complete Security Awareness, Privacy, and other required IT or InfoSec training modules upon hire and thereafter as scheduled or required by EOHHS or EOTSS.

7.3.2 Users are required to comply with the guidelines provided in the trainings regarding use of EOHHS Information Resources. If in doubt about a specific activity, Users are advised to consult with their manager and/or contact the EOHHS Security Office.

7.4 No Expectation of Privacy

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.

7.4.1 Users do not own EOHHS Information Resources and should have no expectation of privacy when using EOHHS Information Resources. This includes communication resources such as Commonwealth email and other messaging tools such as Microsoft Teams regardless of who owns the device, the type of device, the circumstances of use, or method of connecting to EOHHS Information Resources.

7.4.2 The use of EOHHS Information Resources may be monitored, recorded, and audited.

7.4.3 EOHHS has the right to review any information accessed, stored, printed, copied, or otherwise utilized when using EOHHS Information Resources at any time and for any reason.

7.5 Use of EOHHS Information Resources

Users must act in a professional and ethical manner and comply with all policies, standards, and/or applicable contractual obligations.

EOHHS prohibits Users from using EOHHS Information Resources in a manner that violates State or Federal law, Commonwealth Executive Orders, applicable regulatory or contractual obligations and/or agency-level, EOHHS or EOTSS policies, standards or processes.

The prohibited activities include but are not limited to:

7.5.1 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.).

7.5.2 Viewing, creating, storing, and/or processing sexually explicit, obscene, or otherwise inappropriate materials on EOHHS Information Resources.

7.5.3 Using EOHHS Information Resources for personal, commercial, or non-work-related use.

7.5.4 Downloading and installation of software applications onto EOHHS Information Resources without prior approval.

7.5.5 Circumventing administrative lockouts or permissions to install, or attempting to install, such software applications.

7.5.6 Engaging in malicious activity, including but not limited to, altering code, port mapping, or engaging a network sniffer unless explicitly authorized to do so.

7.5.7 Accessing or using EOHHS Information Resources over unsecured/unencrypted Wi-Fi and/or unsecured wireless communication protocols.

7.5.8 Accessing EOHHS Information Resources while outside the United States without prior written authorization.

7.5.9 Accessing client or member-related information when not required by specific job tasks. ***Accessing client or member-related information of family or friends is expressly prohibited.***

7.6 Email Use

To avoid engaging in harmful email practices, Users should:

7.6.1 Only use Commonwealth email accounts for purposes related to Commonwealth business.

7.6.2 Not conduct Commonwealth business through or send Sensitive Information to a personal email account.

7.6.3 Only send Commonwealth Owned Information or Sensitive Information to recipients authorized to receive such information.

7.6.4 Only send Commonwealth Owned Information or Sensitive Information in a manner commensurate with the level of sensitivity of the data.

7.6.5 Not send Commonwealth Owned Information or Sensitive Information to an external e-mail address unless authorized to do so.

7.6.5.1 When sending Commonwealth Owned Information or Sensitive Information to an external e-mail address, ensure the recipient is authorized to receive such information and that the email is sent securely.

7.6.6 Not send Commonwealth Owned Information or Sensitive Information in violation of any federal or state law, third-party contract, or organizational or agency-level policy.

As stated above, **Users should have no expectation of privacy when using EOHHS Information Resources—including Commonwealth emails and email accounts.**

7.7 Equipment

Use of a personally owned device to access EOHHS Information Resources while working remotely is expressly prohibited. Exceptions can be made for 1) incidental or emergency situations or; 2) for interim use once a User has submitted a request for a Device and before the Device has been issued.

7.7.1 The use of portable media is expressly prohibited without prior authorization.

7.7.1.1 In no event may removable or portable media devices be used to transfer Commonwealth Owned Data without express authorization.

7.7.1.2 If authorized, the agency must provide an encrypted, password protected drive to be used only for the purpose of that specific job duty.

7.7.1.3 When not in use, portable media must be stored securely at all times.

7.8 Access Management

The following applies to any device used to access or process EOHHS Information Resources:

7.8.1 Devices must be password protected consistent with EOTSS requirements.

7.8.2 Devices must automatically lock after a time period consistent with EOTSS requirements.

7.8.3 A password must be required to unlock a device.

7.8.4 Devices must not be programmed with automated sign-on sequences, automated password completion, or remote access phone numbers.

7.8.5 A password must be entered each time a device is accessed.

7.8.6 When not using EOHHS Information Resources, Users must log off, lock, or terminate their session with those EOHHS Information Resources.

See also: EOTSS Access Management Standard IS.003-SDR Asset Management

7.9 User Access

Users are only permitted to access EOHHS Information Resources in furtherance of their job duties.

7.9.1 Users must not share authentication credentials (including passwords) or allow another individual to access EOHHS Information Resources with their authentication credentials. Each User is responsible for all actions taken using their accounts.

7.9.2 Users must request access to EOHHS Information Resources required for job responsibilities using EOHHS-approved access request tools and procedures. Authorized

access should be granted based on organizational need and only to the extent necessary to fulfill that organizational need.

7.9.3 Any attempt to gain unauthorized access to EOHHS Information Resources is strictly prohibited.

7.9.4 Any attempt to perform unauthorized actions that may modify, delete, or destroy any part of any EOHHS Information Resource is strictly prohibited.

7.9.5 If a User discovers they have access beyond what is required, they must notify their manager so that access may be adjusted appropriately.

7.10 Passwords

7.10.1 All Devices provided by EOHHS or any device used to access EOHHS Information Resources must have passwords that meet the minimum requirements set by EOTSS. *See EOTSS Access Management Standard IS.003*, Section 6.4 Password Management.

7.10.2 Passwords must never be stored in printed or written form in any easily accessible place. If passwords are stored digitally, they must be in an encrypted format.

7.10.3 Passwords must not be shared or disclosed with anyone, including other EOHHS Users. Helpdesk staff will never ask a User for their password.

7.11 Secure Workspace

7.11.1 Users must keep their assigned workspace secure. This includes locking Sensitive Information in drawers.

7.11.2 While telecommuting or working remotely, Devices must not be left unattended in public spaces, such as on public transportation, in a restaurant or coffee shop, or in a doctor's office.

7.11.3 When printing confidential information on a shared printer, it must be retrieved immediately to reduce the risk of unauthorized access.

7.12 Data Handling

7.12.1 Users must not divulge any Sensitive Information obtained through or in connection with their employment with the Commonwealth to any person or organization except those explicitly authorized to receive such information in support of EOHHS business.

7.12.2 Users must not use any Sensitive Information that is not available to the general public for private purposes or personal use.

7.13 Record Retention

Information storage and retention time frames shall be limited to what is required for legal, regulatory, and business purposes.

7.14 Security Incident Reporting

All Users must report Security Incidents that potentially or actually compromise the confidentiality, integrity, or availability of information systems, processes, or procedures.

All Security Incidents must be reported to the following contacts: EOHHS SCIO, CISO, Security, and EOHHS HelpDesk immediately whenever possible, or within thirty (30) minutes of discovery.

EOHHS SCIO: Mike.Guerin@mass.gov
EOHHS CISO: Anthony.Ristaino@mass.gov
EOHHS Security: EHS-DL-SecurityOperations@mass.gov
EOHHS HelpDesk: Systemssupporthelpdesk@mass.gov or (617)-994-5050

A Security Incident may include, but is not limited to, one of the following events:

- Loss or theft of a Device
- Loss or theft of Commonwealth Data
- Improper usage of Commonwealth Data or devices
- Misuse of legitimate access, intentionally or not
- Compromise of account credentials
- Inappropriate or misdirected transmission of Sensitive Information
- Presence of a virus or other malware on a device
- Any occurrence resulting in an investigation involving IT resources

If in doubt, err on the side of caution and notify the contacts above. Failure to report an incident may lead to a more serious impact on the system, data, or business operations.

Any deliberate attempt by a User to cause, create or worsen a Security Incident may result in disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth. In some cases, violations may be grounds for civil action or criminal prosecution, **including fines and/or imprisonment**.

Changelog			
Date	**Version**	**Author**	**Change Summary**
1/9/2018	0.5	Aaron Weismann	Finalized first draft of document
1/10/2018	0.6	Aliza Mon	Comments
1/11/2018	1.0	Aliza Mon, Meredith Shantz, Aaron Weismann	Finalized document for publication
11/15/2021		Anthony Ristaino	
1/20/2022	2.0	Anthony Ristaino and Jim Cusson	Rewrite/refresh draft
12/1/2022		Meredith Shantz and Donna Walsh	Update draft
3/31/2023	2.1	EHS Security Compliance	Updates to draft, corrections, clarifications, Executive Summary added