Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Privacy Office

Enterprise Data Privacy Policy

Document Name: Enterprise Data Privacy Policy	Effective Date: 9/1/2025
Document ID: EDP.01	Last Revised Date: 9/1/2025

Table of Contents

1. Purpose 2
2. Authority 3
3. Scope 3
4. Responsibility 4
5. Compliance 4
6. Information Privacy Objectives 5
7. Designation of Privacy Officer 5
8. Policy Statements 5
9. Privacy Notices 7
10. Privacy Impact Assessments 8
11. Privacy Awareness and Training 9
12. Data Breach Notifications 9
13. Document Change Control 10

1. Purpose

1.1. The Commonwealth of Massachusetts ("the Commonwealth") creates, collects, manages, and stores information on a regular basis to support its organizational operations and government functions. The Commonwealth aims to use and unlock its diverse technologies, data, and tools to their full potential to provide data-driven and people-centric decision-making, service evaluation, and operational improvement, while preserving the confidentiality, integrity, and availability of its information assets. The purpose of this policy is to establish core data privacy controls and related measures for data about or relating to individuals in, or interacting with, the Commonwealth.

1.2. The Commonwealth must respect the rights and obligations of individuals and organizations with the collection, use, retention, disclosure, and destruction of personal data. Personal data, as used in this policy, includes any of an individual's full name, partial name including first initial and surname, social security number, driver's license number, government-issued identification card number, financial account number, credit or debit card number, or biometric data, either alone or when combined with other data that is linked or linkable to the individual. Examples include:

- Personally Identifiable Information (PII), defined as any representation of information that permits identification of an individual to whom the information relates to be reasonably inferred by either direct or indirect means;
- Personal data as defined in Mass. Gen. Laws chapter 66A, § 1;
- Personal information as defined in Mass. Gen. Laws chapter 93H, § 1; and
- Health information regulated by Medicare (e.g., "beneficiary identifiable data" as defined in 42 C.F.R. § 401.703), HIPAA (e.g., "protected health information" or "PHI" as defined in 45 C.F.R. § 160.103), TEFCA (e.g., "electronic health information" as defined in 45 C.F.R. § 171.102), and other applicable laws and regulations.

1.3. Except as required by statute, personal data does not include data that is anonymized and cannot without undue effort be reassociated with any individual to whom the represented information relates. For example, personal data does not include information that was PHI and has been de-identified in accordance with 45 C.F.R. § 164.514.

1.4. Establishing robust data privacy measures fosters trust between the public and the Commonwealth. This trust is essential for enabling collaborative and effective data

sharing. Striking the right balance between safeguarding personal data and facilitating collaborative efforts allows the Commonwealth to use data on behalf of its residents and communities, such as in public health initiatives, urban planning, emergency response, and climate change. Upholding principles of privacy and individual rights, the Executive Office of Technology Services and Security ("EOTSS") has created this document, the Enterprise Data Privacy Policy (hereafter, "This Policy"), to reinforce the Commonwealth's commitment to a data privacy program and to assist agencies in complying with applicable state and federal laws governing the treatment of personal data. This policy outlines information privacy requirements to safeguard data and help the Commonwealth in achieving its data privacy and data enablement objectives.

2. Authority

2.1. Mass. Gen. Laws chapter 7D, § 2, provides that "there shall be an executive office of technology services and security that will be an executive office within the meaning of section 2 of chapter 6A. The office shall be administered by a secretary who shall be appointed by the governor and who shall supervise all activities concerning information technology of state agencies.… Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

2.2. Mass. Gen. Laws chapter 7D, § 4B, provides that "the [EOTSS] secretary may… appoint a qualified individual to serve as commonwealth chief privacy officer (CPO), who shall serve at the pleasure of the [EOTSS] secretary. The chief privacy officer shall promote privacy and security in the use and dissemination of sensitive data and shall serve as an ombudsperson to effectuate resolution of concerns regarding privacy and security in the use of data."

2.3. See also Mass. Gen. Laws chapter 4, § 7, clause 26; chapter 6A, § 7A; chapter 7D, § 10; chapter 66A, § 1; chapter 93H, § 1; and chapter 93I, § 1.

3. Scope

3.1. This policy applies to all executive department agencies required under Mass. Gen. Laws chapter 7D, § 2, to adhere to the policies, procedures, and objectives established by EOTSS with respect to activities concerning information technology, including all offices and agencies that use or participate in services provided by EOTSS. Offices and agencies who create, collect, store, use, share, disclose, or otherwise process data on behalf of the Commonwealth using services provided by EOTSS must agree to follow this policy as a condition of use. Such offices and agencies are referred to herein as "Participating agencies." Participating agencies may have additional privacy policies

that more specifically address that agency's particular legal and regulatory requirements consistent with this policy.

3.2. This policy exists to ensure appropriate handling of personal data. While the policy only applies to participating agencies, when personal data is shared with an entity that is not a participating agency, it is the responsibility of the participating agency sharing the personal data to ensure that the receiving entity handles the personal data in accordance with this policy and all other applicable legal requirements. The participating agency may determine how best to satisfy this requirement based on the categories of data being shared and the context of the sharing.

3.3. Exclusions: Independent, quasi, or constitutional agencies are excluded from this policy unless they voluntarily opt into using or participating in services provided by EOTSS. Other exclusions may be granted where agencies have privacy policies related to regulatory obligations; such exclusions must be properly documented in the same manner as any other policy exception as described by the EOTSS Enterprise Information Security Policies and Standards.

4. Responsibility

4.1. The Enterprise Privacy Office (EPO) within EOTSS, directed by the Commonwealth CPO, is responsible for the development and ongoing maintenance of this policy.

4.2. The EPO is empowered to monitor compliance with this policy and may enlist other offices to aid in the enforcement of this policy. Each participating agency is responsible for enforcing this policy within their agency.

4.3. Any inquiries or comments about this policy should be submitted to the EPO by sending an e-mail to EOTSS-privacy@mass.gov.

4.4. Other related policies and standards may be found at: https://www.mass.gov/cybersecurity/policies.

5. Compliance

5.1. Compliance with this policy is mandatory for all uses of services provided by EOTSS, as described above in section 3, "Scope." Agencies will be given a reasonable amount of time, not more than six months, to come into compliance with this policy after it is first adopted.

5.2. Violations by EOTSS employees are subject to disciplinary action per applicable employment and collective bargaining agreements, up to and including termination of employment and/or assignment with the Commonwealth.

5.3. Participating agencies are required to determine the approaches for enforcing this policy that are most effective for their agency.

5.4. Non-compliance may also violate applicable state or federal laws.

6. Information Privacy Objectives

6.1. This policy includes an information privacy program to manage risk within the Commonwealth and facilitate the data privacy goals of the Commonwealth through the establishment of supporting policies, standards, and guidelines. This policy can adapt to changes in the cybersecurity threat landscape and account for evolving organizational, legal, and regulatory requirements. The privacy goals of the Commonwealth are:

- Enable organizational strategy for the protection of Commonwealth data and non-public information;
- Follow applicable privacy laws, regulations, and contractual obligations;
- Establish a governance structure to manage information privacy effectively and efficiently;
- Manage identified privacy risks to an acceptable (i.e., risk tolerance based) level through design, implementation, and maintenance of risk remediation plans;
- Establish a culture of accountability and a high level of awareness by all personnel to meet information privacy requirements;
- Establish responsibility and accountability for information privacy policies and governance across the Commonwealth.

7. Designation of Privacy Officer

7.1. The EOTSS EPO needs to have a primary point of contact with each of the participating agencies, i.e., Commonwealth Agencies and Offices using or participating in EOTSS services. Accordingly, all such participating agencies must appoint at least one individual to serve as their primary Privacy Officer to facilitate compliance with the EPO privacy policies and standards, and to coordinate with the EOTSS EPO and the Commonwealth CPO on privacy initiatives. If an agency has more than one privacy officer, then it must appoint a primary point of contact for this policy. In the absence of a designee, the default Privacy Officer will be the agency General Counsel.

7.2. Privacy Officers of the participating agencies must support their agency's implementation of this policy and be responsive to the EOTSS EPO and the Commonwealth CPO.

8. Policy Statements

8.1. Privacy Program

8.1.1. Each participating agency must develop, support, and implement, as appropriate, policies, procedures, guidelines, and standards to establish and

govern the Commonwealth's data privacy program to safeguard the confidentiality, integrity, and availability of its information assets and data, considering the federal and state laws, regulations and policies that apply to the programs administered by the participating agency. All agency level privacy policies and standards must be reviewed and approved by the agency's Agency Head or designee and Privacy Officer or General Counsel. The Commonwealth CPO reserves the right to review agency level privacy policies. Agencies lacking adequate policies, procedures, guidelines, and standards will be given reasonable time, not more than six months, to remedy.

8.2. Notices

8.2.1. Participating agencies must inform constituents by providing timely notices, at least to the extent required by law, about what, how, and why the agency collects, uses, discloses, accesses, and retains personal data.

8.3. Choices and Consent

8.3.1. Where consent is required by law for specific data collection or other processing of personal data about a data subject, participating agencies must provide notice to the data subject and obtain appropriate consent prior to the collection or other processing of the personal data.

8.3.2. Where collected data may be shared with other entities (including other agencies, offices, or vendors), any required notice must disclose the potential for sharing and specify the other entities that may receive the data.

8.4. Monitoring

8.4.1. Participating agencies must monitor compliance with privacy policies and procedures and have procedures to address privacy related inquiries, complaints, and disputes.

8.4.2. Participating agencies must develop and implement remediation plans for any issues identified during privacy compliance reviews.

8.5. Data Minimization and Responsible Data Utilization

8.5.1. Participating agencies must employ data minimization techniques to limit data utilization, disclosure, access, and retention of personal data to only that which is necessary for legally permissible purposes, using only the minimum data elements necessary.

8.5.2. Participating agencies must restrict use of personal data to: (1) purposes consistent with the legally permissible purposes of originally collecting the data, (2) reasonable purposes disclosed to the individual at the time of collection, or (3) any additional purposes required or otherwise authorized

by applicable law. Data may be used to fulfill requests from or on behalf of the individual who is the subject of the data, to prevent fraud, and to maintain utilization statistics and analysis for service provisioning.

8.5.3. Personal data must be retained only as long as necessary for these purposes or as required by law. An agency holding personal data must ensure that the data is securely destroyed within a reasonable period of time after there is no longer a reasonable purpose for retaining the data.

8.6. Data Quality, Integrity, and Accuracy

8.6.1. Participating agencies must protect personal data and take reasonable steps to correct, update, or otherwise maintain accurate personal data as required by law.

8.7. Individual Access

8.7.1. Per Mass. Gen. Laws chapter 66A, § 2, and other applicable laws, agencies must implement a process to allow individuals to access and correct their personal data when appropriate.

8.8. Third Parties

8.8.1. Data disclosure to third parties must only be allowed in accordance with applicable law and regulation.

8.8.2. A participating agency sharing data with a third party is responsible for ensuring that the third party handles the received personal data in a manner consistent with this or the agency's own privacy policy and, where applicable, the EOTSS Enterprise Security Polices and Standards. This may be accomplished through proper enforcement of contract provisions.

8.9. Safeguards

8.9.1. Appropriate physical and digital safeguards must be implemented to protect personal data from threats and from unauthorized collection, use, disclosure, access, and retention, and must follow the EOTSS Enterprise Security Policies and Standards.

8.9.2. Agencies subject to other applicable laws and regulations must review and implement added security measures beyond this policy in compliance with those laws.

9. Privacy Notices

9.1. When collecting personal data, participating agencies must provide appropriate privacy notices, e.g., where required by laws applicable to a program they

administer, such as Mass. Gen. Laws chapter 66A or HIPAA. The privacy notices must include, at minimum, the following components:

- Identity of the agency;
- Descriptions of the categories of personal data that are collected;
- The purpose and scope for collection and use of the personal data collected, including how data is collected, used, shared, and otherwise processed;
- Identify how individual subjects of the data can exercise their rights, if any, including agency contact information.

9.2. The EOTSS EPO is responsible for creating and managing the Commonwealth Privacy Notices for mass.gov and systems that are managed by the Executive Office of Technology Services and Security.

9.3. Each agency is responsible for creating and managing privacy notices that address department specific data. Agency-level privacy notices must satisfy the standards defined by the EPO.

9.4. Written privacy notices must be in plain and simple language and posted conspicuously.

10. Privacy Impact Assessments

10.1. Participating agencies must conduct a Privacy Impact Assessment (PIA) for any new or substantially changed information technology project or system that creates, collects, stores, maintains, disseminates, discloses, or disposes of personal data, or any electronic information collection of personal data, where there is a substantial risk of harm to individuals who are the subjects of the data. PIAs must be completed prior to the project or system processing personal data. Agencies lacking a PIA for a project or system will be given reasonable time, not more than three months, to remedy.

10.2. The requirement for a PIA will be satisfied by any one of the following:

10.2.1. A description of the project, including a high-level catalog of data types involved, and a finding that the project does not process personal data;

10.2.2. A description of the project, including a high-level catalog of data types involved, and a finding that the project does not process personal data with a substantial risk of harm to individuals who are the subjects of the data, along with a determination of whether a filing is required under Mass. Gen. Laws chapter 30, § 63;

10.2.3. A description of the project, including a detailed catalog of data types involved, a description of the requirements for processing such data safely to mitigate potential risks of harm to individuals who are the subjects of the data, and a description of how those requirements are satisfied, along with a determination of whether a filing is required under Mass. Gen. Laws chapter 30, § 63; or

10.2.4. A document similar to those described here, with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections, e.g., as described at section 208(b)(2) of the Federal E-Government Act of 2002 or as described in the NIST Privacy Framework.

10.3. PIAs will be used:

- To identify risks, gaps, impacts, and remediation efforts associated with processing of personal data through information technology.
- To evaluate protections provided by the program or system, including controls implemented, design and process decisions made, and other mitigations for identified risks associated with the system.

10.4. Each participating agency will establish a structured PIA process, including scoping the assessment, identifying privacy risks and impacts, evaluating safeguards and mitigation measures, documenting findings, and involving relevant stakeholders. PIAs must be conducted early in each project lifecycle and regularly reviewed and updated, as necessary.

11. Privacy Awareness and Training

11.1. Participating agencies must ensure that all agency personnel complete the general privacy awareness training which is included with cybersecurity training at on-boarding and annually thereafter.

12. Data Breach Notifications

12.1. Commonwealth Agencies and Offices must follow all applicable laws and regulations regarding data breach notifications and timelines, including but not limited to, Mass. Gen. Laws chapter 93H.

12.2. Information security incidents involving data breaches with the potential to leak personal information regarding Commonwealth residents on Commonwealth systems must be reported to the Massachusetts Security Operations Center (SOC) for investigation as soon as practicable and without unreasonable delay.

13. Document Change Control

13.1. This policy is owned and controlled by the Enterprise Privacy Office. It is the responsibility of the policy owner to maintain, update, and communicate to implementing parties the content of this policy. Questions or suggestions for improvement must be submitted to the policy owner.

13.2. This Privacy Policy must be reviewed and updated by the policy owner on an annual basis or when significant policy or procedure changes necessitate an amendment.

Version No.	Revised By	Effective Date	Description of Changes
1.0	EOTSS	9/1/2025	Initial Document.