Commonwealth of Massachusetts

Executive Office of Technology Services and Security
Enterprise Risk Management Office

Enterprise Third Party Risk Management Policy

Document Name: Third Party Risk Management Policy	Effective Date: 1/1/2025
Document ID: ISP.009	Last Revised Date: 4/8/2025

Table of Contents

1. Purpose 2
2. Authority 2
3. Scope 2
4. Responsibilities 3
5. Compliance 3
6. Third Party Risk Management 4
7. Roles and Responsibilities 6
8. Control Mapping 7
9. Document Change Control 8

1. Purpose

1.1. The purpose of this ***policy*** is to establish the minimum security requirements that must be implemented to manage ***third-party*** vendors who provide any type of ***information*** technology goods and/or services, outsources ***applications***, cloud services, and/or network and security management to the Commonwealth. This ***policy*** reinforces the Commonwealth's commitment to an effective ***third-party risk*** management program and outlines the ***controls*** necessary to safeguard the Commonwealth's ***information assets*** and reduce ***risks*** posed by improper management of ***third-party*** relationships, from contract initiation through termination.

2. Authority

2.1. Pursuant to M.G.L. Ch. 7d, the Executive Office of Technology Services and Security (EOTSS), possess the authority to establish ***policies***, ***procedures***, and objectives with respect to activities concerning ***information*** technology. M.G.L. Ch. 7d provides in pertinent part: "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."

3. Scope

3.1. This document applies to the use of ***information***, ***information systems***, ***assets***, ***applications***, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, boards, commissions, ***agencies***, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security (EOTSS), by any form of contractual arrangement, are required to comply with this document as a condition of use. Commonwealth Agencies and Offices are required to implement ***procedures*** that ensure their ***personnel*** comply with the requirements herein to safeguard ***information***.

4. Responsibilities

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***policy***. The Enterprise Risk Management Office is responsible for this ***policy*** and may enlist other departments to assist in maintaining and monitoring compliance with this ***policy***. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this ***policy*** on an annual basis, or when significant ***policy*** or procedural changes necessitate an amendment. Questions regarding this document must be submitted to the ***document owner*** by sending an email to ERM@mass.gov.

4.2. Additional ***information*** regarding this ***policy*** and its related ***policies*** and ***standards*** may be found at https://www.mass.gov/cybersecurity/policies. Definitions of terms in bold may be found in the ***IS Glossary*** at https://www.mass.gov/cybersecurity/policies.

4.3. In the event of any conflict between the provisions contained in this ***policy*** and the provisions set forth in any of the Enterprise Information Security Standards, the provisions in the Enterprise Information Security Policies will govern.

4.4. Definitions of terms in bold may be found in the *IS.Glossary of Terms* at https://www.mass.gov/cybersecurity/policies.

5. Compliance

5.1. Compliance with this document is mandatory for the Executive Branch and all Commonwealth Agencies and Offices. Violations are subject to 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.

5.2. In the event any Commonwealth Agency or Office is unable to comply with any of the requirements of this document, the agency or office must submit an Information Security Policy Non-Compliance Report to the Enterprise Risk Management Office online through ServiceNow, https://www.mass.gov.service-now.com).

5.3. The Non-Compliance Report will:

5.3.1. Specifically state the reason/cause of the non-compliance

5.3.2. Identify and explain in detail the ***risks*** created due to the non-compliance

5.3.3. Provide a detailed explanation of the ***controls*** the agency, or office will implement to mitigate the ***risks*** to an acceptable level.

5.3.4. Specify the time-frame required to implement the ***controls*** and mitigate the identified ***risks***. All Risk Mitigation Plans (RMP) will be for a limited time.

5.3.5. The names and contact information for both the ***risk owner*** and the ***control owner*** designated by the agency to accept and manage the ***risks*** associated with the non-compliance and implement the ***controls*** that will effectively mitigate the identified ***risks***

6. Third Party Risk Management

6.1. Commonwealth Offices and Agencies must execute a contract with ***third-party*** vendors, prior to or engaging with the ***third-party***, or transferring any Commonwealth ***information*** to the ***third-party***.

6.2. Commonwealth Agencies and Offices must ensure that ***Information*** Security requirements are addressed and documented in any and all ***third-party*** contracts. Provisions must be established and must be clearly set forth in the contract to protect the security of the Commonwealth's ***information assets***.

6.3. Any and all ***third-party*** vendors who provide any type of ***data*** storage, including cloud-based ***data*** storage, ***information*** storage applications, or other cloud-based services, and/or network and ***information*** security management to the Commonwealth, must use servers located in the continental United States to perform these functions and for the storage of Commonwealth ***data***.

6.4. All ***third parties*** are required to comply with all Commonwealth ***Information*** Security ***Policies*** and ***Standards***, including but not limited to EOTSS ***information*** classification and protection requirements, and EOTSS Vulnerability Management Program.

6.5. All ***third-party personnel*** with access to any Commonwealth ***information*** system must adhere to all regulations and governance ***standards*** associated with the accessible ***data*** (e.g. PII, HIPAA, FTI, PCI, CJIS, etc.).

6.6. Commonwealth Agencies and Offices will evaluate all existing contracts with ***third parties*** prior to renewal, to determine the ***third-party's*** capability to maintain the confidentiality, integrity, and availability of Commonwealth ***information assets*** in accordance with EOTSS ***policies***.

6.7. During the on-boarding phase, Commonwealth Agencies and Offices will perform high-level ***risk*** assessments. As part of a ***risk*** assessment, ***third-party*** vendors will provide complete and timely ***information*** to the Commonwealth. The ***information*** that will be provided to the Commonwealth may include but will not be limited to ***third-party*** audit reports such as a SOC2 Type II, proof of Insurance, ***incident*** response plans, and disaster recovery plan.

6.8. During the on-boarding phase all ***third-party*** vendors will disclose to the Commonwealth whether they use, or plan to use of any form of artificial intelligence tools that may collect, process, and/or store any Commonwealth ***data***, or Commonwealth system ***information***.

6.9. During the contract life cycle, ***risk*** assessments will be performed for all significant changes involving privacy or ***information*** security, including but not limited to new ***software applications***, new ***software*** features, introduction of new system and ***software*** architecture or a significant modification to existing ***software application*** features or existing architecture.

6.10. All ***third-party*** vendors will immediately notify the Commonwealth prior to the use of any form of artificial intelligence tool that collects, processes and/or stores any Commonwealth ***data***, or Commonwealth system ***information***.

6.11. Following the initial on-boarding phase, the cadence of ***risk*** assessments will be determined based on business criticality, ***data*** sensitivity and StateRAMP membership.

6.12. Vendors who are StateRAMP authorized must provide the Commonwealth with access requested through StateRAMP. In lieu of StateRAMP access, the vendor will be required to complete the full length Commonwealth ***Risk*** Assessment ***process***.

6.13. In addition to any form of ***risk*** assessment performed by any Commonwealth Agency and/or Office, the ***Commonwealth CISO***, or his or her designee, reserves the right to require any and all ***third parties*** to complete the EOTSS Vendor Risk Management Program (VRM), and/or the EOTSS Vulnerability Management Program (VMP), prior to engaging with the Commonwealth.

6.14. All ***third-party*** vendors who sell or otherwise provide any form of ***software,*** and/or cloud based services, will upon notice from the ***Commonwealth CISO***, or his or her designee, complete the Application Security Center of Excellence (ASCOE) program, prior to engaging with the Commonwealth.

6.15. Commonwealth Agencies and Offices are required to manage ***third parties*** throughout the life cycle of the contract. Commonwealth Agencies and Offices will designate an ***application administrator***, or other contract

manager, to manage the ***third-party*** contract relationship, in collaboration with existing ***information*** security, procurement, and/or Legal Teams.

6.16. Commonwealth Agencies and Offices will establish and maintain an inventory of all ***third parties***. The inventory must include a description of the type, and version of the product provided by the ***third-party***, the type of Commonwealth ***data*** stored within the ***third-party's*** solution, the principal point of contact from the ***third-party,*** and the designated ***application administrator***, or contract manager, from the Commonwealth. Contact ***information*** must include, at a minimum, name, email, and/or phone number.

6.17. ***Third parties*** will provide the Commonwealth with complete and timely access to all Commonwealth ***information*** upon request, both during and after the ***third-party*** engagement.

6.18. ***Third parties*** must be securely decommissioned upon the expiration of a contract.

7. Roles and Responsibilities

Role	Responsibility
Commonwealth Chief Information Security Officer (CISO)/Chief Risk Officer (CRO)	The person responsible for ensuring compliance with this policy across all Commonwealth Agencies and Offices. The CISO leads the ERM Office and is responsible for aligning security initiatives with enterprise programs and business objectives. The CISO ensures that all of the Commonwealth's IT assets, communication systems, data and technologies are securely protected.
Manager of Vendor Risk Management	The person within the ERM Office, designated by the Commonwealth CISO to supervise the EOTSS Vendor Risk Management Program. As the designee of the Commonwealth CISO, the VRM Manager decides which third-party vendors must complete the EOTSS Vendor Risk Management Program, what information the third parties will provide for a particular risk assessment and approves the results of the assessments for vendors.

Enterprise Risk Management Office (ERM)	The office within EOTSS responsible for risk strategy, identification, assessment, analysis, monitoring, reporting and mitigation. Under the direction of the Commonwealth CISO/CRO, ERM establishes the Commonwealth's information security policies, standards, guidelines and directives to create an effective risk governance program that determines acceptable levels of risk tolerance and implements cybersecurity best practices to mitigate operational, reputational, security and financial risk.
Application Administrator/ Contract Manager	The person(s) within the Commonwealth Agency or Office responsible for managing the third-party contract relationship in collaboration with the agency's information security, procurement, and/or Legal Teams. Application Administrators/managers are responsible for establishing and maintaining the third-party inventory, including all data details and contact information required by this policy.
Commonwealth Agencies and Offices	Commonwealth Agencies and Offices are responsible to adhere to this policy and to comply with the requirements in this document in addition to any supporting documentation issued by the Secretary of EOTSS/Commonwealth CIO, the Commonwealth CISO/CRO, and/or the ERM office.

8. Control Mapping

Section	NIST SP 800-53	CIS 18	NIST CSF
Policy Statement	RA-01	-	GV.OC-01
Third Party Risk Management	PM-30,	13.1, 13.3, 17.2, 18.8	GV.SC-01, GV.SC-03, GV.SC-05, GV.SC-06, GV.SC-07
Decommissioning	-	15.7	-
Roles and Responsibilities	RA-01, PM-29		GV.OC-02, GV.RM-05, GV.SC-02, GV.RR-01, GV.RR-02, GV.RR-03

9. Document Change Control

Version No.	Revised By	Effective Date	Description of Changes
1.0	Vendor	5/6/2024	Initial Policy Draft
1.1	Thomas E. McDermott	12/23/2024	Revisions, Corrections and Formatting
1.2	Anthony J. O'Neill	1/1/2025	Final Review
1.3	Thomas E. McDermott	4/8/2025	Updates, Corrections and Formatting
1.3	Miklos Lavicska	4/22/2025	Corrections and Formatting
1.3	Anthony J. O'Neill	4/28/2025	Final Review