Commonwealth of Massachusetts
Executive Office of Technology Services and Security (EOTSS)
Enterprise Risk Management Office

Third-Party Information Security Standard

Document Name: Third-Party Information Security Standard	Effective Date: October 15th, 2018
Document ID: IS.026	Last Revised Date: March 21, 2025

Table of Contents

1. PURPOSE

1.1. This ***standard*** establishes security requirements for the use of ***third parties*** that handle Commonwealth ***confidential information***, either by storing, processing, transmitting, or receiving ***information***.

1.2. This ***standard*** outlines the following ***controls*** to reduce the ***information*** security ***risks*** associated with contracted services and staff:

1.2.1. Identification of ***risks*** related to ***third parties*** to ensure appropriate protection of Commonwealth ***information assets***

1.2.2. Definition of ***information*** security requirements for ***third-party*** agreements

1.2.3. ***Third-party information*** management oversight 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 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. RESPONSIBILITY

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***standard***. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in maintaining and monitoring compliance with this ***standard***. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this ***standard*** 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 ***standard*** and its related ***policies*** and ***standards*** may be found at https://www.mass.gov/cybersecurity/*policies*.

4.3. In the event of any conflict between the provisions contained in this ***standard*** and the provisions set forth in any of the Enterprise Information Security Policies, 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. STANDARD STATEMENTS

6.1. Third-Party Selection - During the ***third-party*** selection process, Commonwealth Agencies and Offices must ensure that the items listed below are evaluated from a security perspective during the sourcing and contracting phases:

6.1.1. Technical and industry experience

6.1.1.1. Identify areas where the Commonwealth may have to supplement the ***third-party***'s capabilities related to ***information*** management to fully manage ***risk*** to Commonwealth's ***information assets***.

6.1.1.2. Evaluate the ***third-party***'s use of other ***third parties***' (i.e., subcontracting relationships) technology to support the contracted operations.

6.1.1.3. Evaluate the experience of the ***third-party*** in providing services that include the handling of ***confidential information*** in the anticipated operating environment.

6.1.1.4. Evaluate the ***third-party***'s ability to respond to service disruptions (see *IS.020 Information Security Incident Management Standard and IS.016 Business Continuity and Disaster Recovery Standard*).

6.2. Operations and Control (as applicable)

6.2.1. Determine/review the adequacy of the ***third-party's policies*** and ***procedures*** relating to internal ***controls*** in accordance with Report on Controls of Service Organizations such as SOC1/SOC2 User/Client Control Considerations (e.g., parameters, logical access, event logs/audit trails), facilities management, privacy protections, maintenance of records, business resumption contingency planning, secure systems development, and maintenance and employee background checks.

6.2.2. Determine whether the ***third-party*** provides sufficient security precautions, including, when appropriate, firewalls, ***encryption***, and customer identity authentication, to protect Commonwealth ***information*** resources as well as detect and respond to intrusions.

6.2.3. Evaluate whether the Commonwealth has complete and timely access to its ***information*** maintained by the ***third-party*** both during and after any ***third-party*** engagement.

6.2.4. Evaluate the ***third-party***'s knowledge of regulations (e.g., FTI, PII, PHI, PCI) that are relevant to the services they will provide.

6.2.5. Obtain proof of the ***third-party***'s cybersecurity insurance coverage and assess the adequacy of the insurance coverage in consultation with ***risk*** management or procurement functions.

6.3. Contractual Security Risk Identification

6.3.1. All contracts by which a ***third-party*** provides services to the Commonwealth or allows a ***third-party*** to access, store, process, analyze or transmit Commonwealth ***confidential information*** must be assessed, prior to entering into an agreement, to determine the ***third-party***'s capability to maintain the confidentiality, integrity and availability of Commonwealth ***information assets*** consistent with *IS.001 Enterprise Information Security Governance Policy*. The following must be considered during ***third-party*** sourcing and/or contract negotiation:

6.3.2. ***Third-party*** sourcing and contract negotiation

6.3.2.1. Organizational objectives and requirements.

6.3.2.2. Transparency to evaluate and manage ***third-party*** relationships.

6.3.2.3. Importance and criticality of the services to the Commonwealth (*see IS.015 Asset Management Standard and IS.017 Communication and Network Security Standard)*.

6.3.2.4. Defined requirements for the contracting activity, including any potential regulatory requirements.

6.3.2.5. Necessary security ***controls***/reporting ***processes*** in Commonwealth Agencies and Offices.

6.3.2.6. Contractual obligations and requirements to be imposed on the ***third-party***

6.3.2.7. Contingency plans, including the availability of alternate ***third parties***, costs and resources required to switch ***third parties*** upon breach or termination (see *IS.005 Business Continuity and Disaster Recovery Standard*).

6.4. Contractual Security Provisions

6.4.1. Commonwealth Agencies and Offices must ensure that ***Information*** Security ***policies*** and requirements are addressed and documented in any contract with the ***third-party***.

6.4.2. Provisions must be established and must be clearly set forth in the contract to protect the security of the Commonwealth's ***information assets***.

6.4.3. ***Third-party*** contracts must address the following where applicable:

6.4.3.1. All parties involved with the agreement must be made aware of their privacy and security responsibilities and are required to sign confidentiality agreements (e.g., non-disclosure agreements).

6.4.3.2. ***Information*** classification requirements in accordance with the Commonwealth's ***Information*** Classification and ***Information*** Protection Requirements (*see IS.001 Enterprise Information Security Governance Policy and IS.015 Asset Management Standard*).

6.4.3.3. Relevant legal and regulatory requirements which may apply to ***information*** processed, stored, or transmitted.

6.4.3.4. Requirements governing the acceptable use of Commonwealth-owned or managed ***information***. (*see IS.002 Acceptable Use of Information Technology Policy*).

6.4.3.5. The means by which a ***third-party*** proposes to transfer ***information*** to other ***third parties*** and the means by which a third party will require written notice and agreement from the Commonwealth prior to any such transfer.

6.4.3.6. Adherence by the ***third-party*** to an ***information*** security program, including, but not limited to, password and access management requirements, physical security of facilities and servers containing Commonwealth ***information***, network protection, system and ***software*** protection, ***encryption***, and ***information*** security of ***data*** in transit and at rest, and intrusion-detection/prevention systems.

6.4.3.7. Training and awareness requirements for specific procedures and ***information*** security requirements (e.g., for ***incident*** response, authorization procedures).

6.4.3.8. Screening requirements, if any, for ***third-party personnel***, including responsibilities for conducting the screening and notification ***procedures*** if screening has not been completed or if the results give cause for concern.

6.4.3.9. The Commonwealth's explicitly reserved right to audit the performance of ***information*** security and other contractual responsibilities of the parties involved in the signed agreement. This will be done when deemed necessary by a Commonwealth organization, and doing so will incur no additional cost to any Commonwealth contract.

6.4.3.10. The ***third-party***'s obligation to periodically deliver an independent report on the effectiveness of ***controls*** (e.g., SOC1/SOC2, ***vulnerability*** testing results) and agreement on timely correction of relevant issues raised in the report.

6.4.3.11. ***Processes*** used by the ***third-party*** to report ***incidents*** in writing to the Commonwealth involving any type of ***security breach*** or unauthorized access to the Commonwealth's ***information assets*** within the appropriate timeframes (see *IS.005 Incident Response Policy and IS.020 Information Security Incident Management Standard*).

6.4.3.12. Upon termination of the contract, Commonwealth ***information*** will be transmitted to the Commonwealth or the Commonwealth's ***third-party*** of choice in a format defined by the Commonwealth at a cost specified to the mutual satisfaction of the Commonwealth and the ***third-party*** prior to termination.

6.4.3.13. ***Processes*** used to electronically erase, render unreadable or physically destroy all Commonwealth's ***information assets*** upon termination of the agreement (see *Information Disposal in IS.015 Asset Management Standard*).

6.4.3.14. Commonwealth's explicit reserved right to request, at any time, transfer or purging of some or all ***information*** stored on ***third-party*** systems under conditions and at a cost specified to the mutual satisfaction of the Commonwealth and the ***third-party*** prior to termination.

6.4.3.15. Maintenance and testing ***procedures*** for Business Continuity Planning as appropriate.

6.4.3.16. Enabling ***processes*** to provide for timely forensic investigation in the event of a compromise.

6.4.4. All contracts will be reviewed according to each agency's internal ***policy***. If the ***information*** being collected or exchanged is ***restricted*** or ***confidential***, a binding non-disclosure agreement must be in place between the Commonwealth and the ***third-party***, whether as part of the contract or a

separate non-disclosure agreement (required before any ***restricted information*** or ***confidential information*** is shared).

6.5. Third-Party Life Cycle Management

6.5.1. Commonwealth Agencies and Offices must ensure that all ***third parties*** are managed through the life cycle of the contract by the ***Information Owner*** in collaboration with the ***Information Security Team*** and Procurement/Legal.

6.5.2. The following must be considered throughout the ***third-party*** life cycle management process:

6.5.2.1. Inventory of ***third parties*** with assigned vendor ***risk*** rating.

6.5.2.2. Contractual performance criteria or service-level agreements.

6.5.2.3. Contractual, regulatory, or legal requirements.

6.5.2.4. Inventory of all relevant contractual deliverables.

6.5.2.5. ***Information*** classification of ***information*** entrusted to ***third parties***.

6.5.2.6. Enablement of accounts used by ***third parties*** for remote access only during the time period needed and monitor remote access accounts when in use.

6.5.2.7. Audit provisions to determine the ***third-party***'s compliance per defined requirements.

6.5.2.8. The frequency of audits, based on advice from teams such as Internal Audit, ***Information Security***, Risk and ***Legal***.

6.5.2.9. Communicate the need for transition or return of ***information*** at end of engagement/contract and obtain certification in writing from the ***third-party*** that all Commonwealth ***information*** has been permanently deleted if the contract so requires.

6.5.2.10. ***Risk*** assessment at the onset and at least annually thereafter and upon significant changes to the agreement or environment. The ***risk*** assessment will identify critical ***assets***, threats and ***vulnerabilities*** and result in a formal, documented analysis of ***risk*** (*see IS.010 Information Security Risk Management Standard).* Significant changes include:

6.5.2.10.1. Changes and enhancement to networks.

6.5.2.10.2. Use of new technologies.

6.5.2.10.3. Adoption of new products or newer versions or releases.

6.5.2.10.4. New development tools and environments.

6.5.2.10.5. Changes to the physical location of service facilities.

6.5.2.10.6. Subcontracting to another ***third-party.***

6.5.2.11. Awareness training for Commonwealth ***personnel*** that interact with ***third parties*** regarding appropriate rules of engagement based on the type of ***third-party*** and level of access to Commonwealth ***information assets***.

7. CONTROL MAPPING

Section	NIST SP800-53 R4 (1)	CIS 20 v6	NIST CSF
6.1 Third-party Selection	CA-2	CSC 4	ID.RA-1
	CA-3	CSC 1	ID.AM-3
	SA-9	-	ID.AM-4
	AC-1	-	ID.GV-1
	AU-1	-	ID.GV-1
	CA-1	-	ID.GV-1
	CM-1	-	ID.GV-1
6.2 Contractual Security Risk Identification	CP-1	-	ID.GV-1
	IR-1	-	ID.GV-1
	MA-1	-	ID.GV-1
	PE-1	-	ID.GV-1
	PL-1	-	ID.GV-1
	PM-1	-	ID.GV-1
6.3 Contractual Security Provisions	PS-1	-	ID.GV-1
	AT-1	-	ID.GV-1
	RA-1	-	ID.GV-1
	RA-2	-	ID.AM-5
	SA-1	-	ID.GV-1
	SA-6	-	-

6.4. Third-party Life Cycle	RA-3	CSC 4	ID.RA-1
	AT-1	-	ID.GV-1
	RA-1	-	ID.GV-1
	RA-2	-	ID.AM-5
		-	ID.AM-6
		-	ID.BE-1

8. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting.
0.92	John Merto	1/02/2018	Corrections
0.95	Sean Vinck	5/7/2018	Corrections and formatting.
0.97	Andrew Rudder	5/31/2018	Corrections and formatting
0.98	Anthony O'Neill	5/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	6/01/2018	Pre-publication review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Thomas E. McDermott	11/24/2023	Corrections, Formatting, Updating and Annual Review
1.3	Anthony O'Neill	11/24/2023	Final Review
1.4	Thomas E. McDermott	12/16/2024	Corrections, Formatting and Annual Review
1.4	Anthony O'Neill	12/16/2024	Final Review
1.5	Thomas E. McDermott	2/25/2025	Updates, Corrections and Formatting
1.5	Miklos Lavicska	3/14/2025	Corrections and Formatting
1.5	Anthony O'Neill	3/21/2025	Final Review