Commonwealth of Massachusetts

Executive Office of Technology Services and Security (EOTSS)

Enterprise Risk Management Office

Communication and Network Security Standard

Document Name: Communication and Network Security Standard	Effective Date: October 15th, 2018
Document ID: IS.017	Last Revised Date: March 13, 2025

Table of Contents

1. PURPOSE

1.1. This ***standard*** establishes the minimum security requirements for the Commonwealth's network infrastructure and connectivity, including:

1.1.1. Network architecture requirements to include redundancy, network segmentation, ***encryption***, and the documentation of network diagrams.

1.1.2. Use of network infrastructure protection such as firewalls, intrusion detection systems, web-proxies and ***data*** loss prevention.

1.1.3. ***Controls*** to protect ***endpoint*** computing systems.

1.1.4. Requirements for remote access.

1.1.5. Requirements for ***third-party*** business-to-business connections.

1.1.6. Requirements for secure file transfer.

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:

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

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

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

5.1.4. 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.

5.1.5. 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. Network Security Management

6.1.1. Commonwealth Agencies and Offices will follow best industry standards and practices and will provide network security capabilities that will protect ***data*** during transmission. Commonwealth Agencies and Offices must ensure that access to ***information assets*** is restricted to authorized ***personnel*** and protected at all times.

6.1.2. Network Architecture and Connectivity

6.1.2.1. The Commonwealth will establish ***controls*** to manage and mitigate the ***risks*** associated with network connections to ensure that ***users*** are only provided with access to the services that they have been specifically authorized to use. ***Controls*** will, at a minimum, include:

6.1.2.1.1. Network confidentiality: ***Controls*** will include the use of ***encryption*** and device authentication to protect the confidentiality of transmitted ***information*** (see *IS.002 Acceptable Use of Information Technology Policy and IS.019 Cryptographic Management Standards)*.

6.1.2.1.2. Network segmentation: Networks will be logically or physically separated into functional modules (e.g., internet/extranet, ***data*** center, WAN, access module) that are a grouping of infrastructure platforms, ***information systems*** and end-***user*** devices that play distinct roles within an architecture.

6.1.2.1.3. Functional modules will be further subdivided into security zones, an association of ***information systems*** and services with similar security ***controls***, policies and ***information*** classification.

6.1.2.1.4. Networking platforms and ***information systems*** associated with a particular security zone will have the same trust level and approval to interact with or process ***data*** of similar classification.

6.1.2.1.5. ***Information systems*** with direct connectivity or providing services to the Internet will be isolated in the appropriate security zone.

6.1.2.2. Egress points: limit the number of external connections to the Internet. Egress points must be controlled and monitored centrally (where possible).

6.1.2.3. Network redundancy: the Commonwealth will determine the degree of redundancy based on availability requirements for the affected ***data*** (see *IS.016 Business Continuity and Disaster Recovery Standard)*.

6.1.2.4. Network documentation: the Commonwealth's network architecture will be clearly documented.

6.1.2.4.1. Document internal and external network connections.

6.1.2.4.2. Review and update documentation annually or when major network or systems revisions are implemented.

6.1.2.4.3. Classify documentation such as network diagrams, routing tables and IP addresses as ***Confidential*** and protect accordingly.

6.1.3. Use of Firewalls

6.1.3.1. The Commonwealth will ensure that all access points into its networks from external connections (e.g., ***third-party*** connections, remote access) are protected with network boundary protections to adequately isolate systems and all internal and ***confidential information***.

6.1.3.2. Firewall and router configuration standards will be established by the Enterprise Security Office that includes the following:

6.1.3.2.1. A formal process for approving and testing all network connections and changes to the firewall and router configurations.

6.1.3.2.2. Network device hardening standards with minimum security baselines defined, including business justification for use of all services, protocols and ports allowed for system components, specifically security features implemented for those protocols considered to be insecure (e.g., FTP, Telnet, POP3, IMAP and SNMP).

6.1.3.2.3. All external connections must pass through an Enterprise Security Office managed firewall.

6.1.3.2.4. Access restriction requirements to specific source, destination, and protocols/services.

6.1.3.2.5. Network diagram details with all external connections, including any wireless networks, identified.

6.1.3.2.6. Requirements for a firewall (or similar network traffic filtering device) at each egress point and between security zones.

6.1.3.2.7. Description of groups, roles, and responsibilities for logical management of network components.

6.1.3.2.8. The process to track and monitor system and network configuration changes and resulting effects on the network (see *Change Management in IS.004 Asset Management Standard*). Changes will only be approved after the completion and review of a formal ***risk*** assessment.

6.1.3.3. Direct public access from the Internet to any internal system in the enterprise is prohibited. ***Controls*** will, at a minimum, include:

6.1.3.3.1. Perform inspection of unencrypted ingress traffic sourced from the Internet using signature and behavioral detection/prevention technologies.

6.1.3.3.2. Disclosure of private IP addresses and routing ***information*** to unauthorized entities is explicitly forbidden.

6.1.3.3.3. Restrict unauthorized outbound traffic from the internal network to the Internet. Outbound traffic must be authenticated and passed through a controlled system (like a proxy) for logging.

6.1.3.3.4. Implement firewalls that perform stateful inspection (i.e., dynamic packet filtering).

6.1.3.4. Review firewall and router rule set on a semiannual basis.

6.1.4. Intrusion Prevention and Detection Systems

6.1.4.1. The Enterprise Security Office will implement and maintain a network-based intrusion prevention system (IPS) or, alternatively, an intrusion detection system (IDS) with a higher degree of monitoring. The network-based IPS will be configured to perform real-time analysis on traffic patterns for:

6.1.4.1.1. Networks with direct connectivity to open or untrusted networks.

6.1.4.1.2. Monitor traffic at the perimeter and at critical points inside the Commonwealth's internal network zones.

6.1.4.1.3. Alert ***personnel*** of suspected compromises.

6.1.4.1.4. IPS/IDS prevention engines, baselines, and signatures (and behavioral heuristics where feasible) will be configured, maintained, and updated per vendor baseline instructions and the Commonwealth's security requirements to ensure optimal protection.

6.1.5. Denial of Service Protection

6.1.5.1. The Commonwealth will implement and maintain ***controls*** to prevent denial of service events.

6.1.5.2. ***Application***-layer flood denial of service attacks

6.1.5.3. Distributed denial of service attacks

6.1.5.4. Unintended denial of service attacks

6.1.6. Data Loss Prevention

6.1.6.1. The Commonwealth will implement and maintain ***controls*** to prevent the loss of ***confidential information*** within the boundaries of legal and regulatory requirements.

6.1.6.2. The DLP system will be configured to perform analysis on ***data***-at-rest, ***data***-in-motion, and ***data***-in-use (see *Information Labeling and Handling in IS.015 Asset Management Standard*).

6.1.6.3. The following guidance will be considered in the ***data*** monitoring strategy for ***data***-in-motion:

6.1.6.3.1. Egress points and common insecure services such as HTTP, SMTP and FTP will be monitored to ensure ***confidential information*** is not insecurely transmitted outside of the Commonwealth's networks.

6.1.7. Domain Name Services (DNS)

6.1.7.1. All internal hosts must register with the internal DNS and external hosts with external DNS.

6.1.7.2. Any external DNS query will be handled by Commonwealth registered DNS servers.

6.1.7.3. Use of externally provided DNS (e.g., Google) is prohibited.

6.1.7.4. The Commonwealth will implement ***controls*** to validate DNS queries and deny outbound connections for domains that are known to be untrusted.

6.1.7.5. The DNS will provide ***data*** origin authentication and integrity verification artifacts in response to external name/address resolution queries.

6.1.7.6. The DNS will request and perform ***data*** origination and ***data*** integrity verification on name/address resolution responses the system receives from authoritative sources.

6.1.7.7. A separate execution domain will be maintained for each executing system process.

6.1.8. Dynamic Host Communication Protocol (DHCP)

6.1.8.1. All ***information systems*** will be assigned a Commonwealth assigned IP.

6.1.8.2. All IP addresses will be centrally managed.

6.1.8.3. All IPs must resolve to a fully qualified domain name (FQDN).

6.1.8.4. All DHCP assignment ***logs*** will be collected and maintained for security monitoring purposes.

6.1.9. Web Proxy

6.1.9.1. Internal host addresses must be hidden from the Internet.

6.1.9.2. Unauthenticated outbound traffic from the Commonwealth network is prohibited.

6.1.9.3. All outgoing web traffic must go through a proxy server, and ***logs*** will be collected and maintained for security monitoring purposes.

6.1.10. Administrative Services Protection

6.1.10.1. Access to administrative services will be securely controlled.

6.1.10.2. Physical access to diagnostic and configuration ports will be controlled and monitored.

6.1.10.3. Technical standards will specify the network services and ports that may be opened for business operations.

6.1.10.4. All administrative access to any network device must use ***multi-factor authentication***.

6.1.10.5. The Commonwealth reserves the right to block ports and services if an event is identified that could adversely impact the network.

6.1.10.6. The Commonwealth will monitor and ensure that all opened ports and services for network devices are vetted through the change management system.

6.1.10.7. Prior to the implementation of a firewall change, Commonwealth Agencies and Offices must perform a ***risk*** assessment to assess the validity of the change request.

6.1.10.8. Firewall change requests must be reviewed and approved by the ***Information Security Team***.

6.1.11. Wireless Security

6.1.11.1. Authentication and network/transport layer ***encryption*** must be used for wireless connections to protect wireless access to Commonwealth networks.

6.1.11.2. Abide by the security ***controls*** specified for wireless communication devices by the product manufacturers.

6.1.11.3. ***Information assets*** that connect to the secure wireless network must be owned and/or managed by the Commonwealth (e.g., laptop, wireless card, wireless client).

6.1.11.4. Wireless ***assets*** not owned and/or managed by the Commonwealth are not permitted to connect to the Commonwealth secured wired or wireless network.

6.1.11.5. Access points must use Commonwealth-approved authentication protocols and infrastructure. Implement WPA2 (or current industry standard) ***encryption*** for authentication and transmission. The use of WEP as a security control is prohibited. (*See Approved Cryptographic Techniques in IS.019 Cryptographic Management Standard)*.

6.1.11.6. All ***users*** must authenticate to the secure wireless access point using Commonwealth-approved ***multi-factor authentication***.

6.1.11.7. Visitor wireless access points must not permit connection to the enterprise network (i.e., MAGNet) and must be monitored for anomalous activity.

6.1.11.8. Commonwealth Agencies and Offices must ensure that Commonwealth ***personnel*** must not concurrently connect to the wired infrastructure and any non-Commonwealth wireless network (such as a wireless ISP or an “open” access point).

6.1.11.9. All wireless infrastructure devices that reside at a Commonwealth site or connect to the Commonwealth network must maintain a hardware address (i.e., MAC address) that can be registered and tracked.

6.1.11.10. Change wireless vendor defaults, including but not limited to default wireless ***encryption keys***, administrator usernames and passwords, and SNMP community strings.

6.1.11.11. Audit wireless access points at least quarterly to detect any unauthorized access points.

6.1.11.12. Collect and maintain wireless activity for security monitoring purposes.

6.2. Remote Access Security Management

6.2.1. All remote access connections into the Commonwealth's internal networks will be established through approved methods.

6.2.2. All external connections to the Commonwealth family of networks must be reviewed and approved by the ***Commonwealth CISO***, or his or her designee.

6.2.3. Document and inventory all connections external to the Commonwealth as well as internal connections between agencies.

6.2.4. Remote access will only be provided if there is a business need supported by the appropriate level of approvals (i.e., ***Information Owner***).

6.2.5. Remote connections must be achieved by approved, secure remote access solutions.

6.2.5.1. VPN connections can be either site-to-site or client-to-site. Regardless of the VPN type, appropriate access ***control*** restrictions must be implemented.

6.2.6. Remote access connections require proper levels of authentication and logging at the "point of entry" into the Commonwealth network. (*See IS.014 Access Management Standard).*

6.2.7. Remote access solutions must be approved by the Enterprise Security Office prior to connecting to Commonwealth networks. ***Controls*** will, at a minimum, include:

6.2.7.1. Remote access will require ***multi-factor authentication.***

6.2.7.2. Segregate Commonwealth ***remote access*** VPN ***users*** from non-Commonwealth ***remote access*** VPN ***users*** to allow for increased granularity.

6.2.7.3. The ***remote access*** VPN will employ a framework for ***encryption***, centralized mutual strong authentication and dynamic ***key*** management between the mobile client and the VPN termination platform (*see IS.019 Cryptographic Management Standard*).

6.2.8. Commonwealth will provide a public DNS name for all internal services accessed remotely by all ***users***, including ***third parties***.

6.2.9. All collaborative computing devices and ***applications*** (such as remote meeting devices and ***applications***, networked whiteboards, cameras, and microphones), with the exception of those approved by the Commonwealth, are prohibited. Additionally, when approved services are in use, they must display an indication of use to ***users*** present at the devices.

6.3. Network Access Management for Third of Third-Parties

6.3.1. Third-Party Access

6.3.1.1. If ***third parties*** require access to the Commonwealth's ***information assets***, access approval must be obtained from the Enterprise Security Office. ***Controls*** will, at a minimum, include:

6.3.1.1.1. Document and inventory all ***third-party*** access to the Commonwealth's family of networks.

6.3.1.1.2. ***Third parties*** must agree with and adhere to the Commonwealth's ***information*** security requirements. The Commonwealth will reserve the right to perform periodic audits of any ***third party's information*** security program.

6.3.1.1.3. All ***third-party*** access to the Commonwealth network will be formally evaluated and approved by the Enterprise Security Office.

6.3.1.1.4. ***User*** access will be limited to resources for which they have been authorized (see *User Access Management in IS.014 Access Management Standard*).

6.3.1.1.5. ***Information Custodians*** will develop explicit procedures or usage requirements for securing the ***information*** access and exchange medium (see *Information Classification in the IS.003 Asset Management Standard*).

6.3.2. ***Third-Party*** Business-to-Business (B2B) Connections

6.3.2.1. ***Third-party*** B2B connections to the Commonwealth's networks will adhere to:

6.3.2.1.1. Clearly defined and approved access control methods between the ***third-party*** network connection and the Commonwealth network.

6.3.2.1.2. Adopt approved ***encryption*** methods (e.g., TLS, SSL, VPN) to establish the connection between the ***third-party*** and the Commonwealth.

6.3.2.1.3. The Enterprise Security Office will establish extranet monitoring and logging procedures (*see IS.022 Logging and Event Monitoring Standard)*.

6.3.2.1.4. Commonwealth Agencies and Offices must ensure that ***Information Owners*** and ***Information Custodians*** impose a specific expiration date for the B2B connection and inform the supporting technology group when the connectivity can be terminated.

6.4. Secure File Transfer

6.4.1. Use Commonwealth-approved secure file transfer solutions (e.g., Interchange) to protect ***data*** from interception, unauthorized copying, unauthorized modification, misrouting and unauthorized destruction.

6.4.2. Use cryptographic techniques for ***encrypting*** transmission channels for file sharing purposes (*See IS.019 Cryptographic Management Standard)*.

6.4.3. Files will only transfer after positive authentication.

6.4.4. Credentials must be changed in accordance with *Password Management in IS.014 Access Management Standard*.

6.4.5. File transfer services, retention and disposal guidelines must be followed in accordance with *Information Labeling and Handling in IS.015 Asset Management Standard*.

6.4.6. Exchange of ***data*** and ***software*** between organizations will be based on a formal exchange agreement and will comply with any relevant legal or regulatory requirements.

6.4.7. Electronic Messaging

6.4.7.1. Protect messages from unauthorized access, modification, or denial of service in accordance with *Information Classification in IS.015 Asset Management Standard*.

6.4.7.2. Protect messages being processed, at rest or in transit via the use of ***encryption*** protocols (e.g., SSL and TLS) in accordance with *IS.019 Cryptographic Management Standard*.

6.4.7.3. Implement stronger levels of authentication controlling access from publicly accessible networks.

6.4.7.4. Implement approved technical ***controls*** to mitigate spam, ***malware***, and phishing threats.

6.4.7.5. Collect and monitor ***logs*** for security monitoring purposes (see *IS.022 Logging and Event Monitoring Standard*).

7. CONTROL MAPPING

Section	NIST SP800-53 R4 (1)	CIS 20 V6	NIST CSF
6.1. Network Security Management	AC-3	CSC 5	PR.AC-4
	AC-6	CSC 5	PR.AC-4
	AC-6	CSC 5	PR.AC-4
	AC-17	CSC 12	PR.AC-3
	AC-18	CSC 11	PR.PT-4
	PE-3	-	PR.AC-2
	MA-3	-	PR.MA-1
	MA-4	CSC 5	PR.MA-2
	SC-4	-	-
	CP-9	CSC 10	PR.IP-4
	CP-10	CSC 19	RS.RP-1
	AC-4	CSC 1	ID.AM-3
	AC-17	CSC 12	PR.AC-3
	AC-18	CSC 11	PR.PT-4
	AC-20	-	ID.AM-4
	CA-3	CSC 1	ID.AM-3
	CP-8	-	ID.BE-4
	PE-5	-	PR.AC-2
	SC-Family	-	-
	CA-3	CSC 1	ID.AM-3
	IA-2	CSC 16	PR.AC-1
	IA-3	CSC 16	PR.AC-1
6.2 Remote Access Security Management	IA-8	CSC 16	PR.AC-1
	IA-3	CSC 16	PR.AC-1
	AC-19	CSC 12	PR.AC-3
	AC-2	CSC 16	PR.AC-1
	IA-5	CSC 16	PR.AC-1

6.3. Management of Third-Party Network Access	SC-7	CSC 9	PR.AC-5
6.4. Secure File Transfer	AC-1	-	ID.GV-1
	AC-3	CSC 5	PR.AC-4
	AC-4	CSC 1	ID.AM-3
	AC-17	CSC 12	PR.AC-3
	AC-18	CSC 11	PR.PT-4
	AC-20	-	ID.AM-4
	CA-3	CSC 1	ID.AM-3
	PL-4	-	-
	PS-6	CSC 13	PR.DS-5
	SC-7	CSC 9	PR.AC-5
	SC-16	-	-
	SI-9	-	-
	CA-3	CSC 1	ID.AM-3
	SA-9	-	ID.AM-4
	MP-5	CSC 8	PR.PT-2
		CSC 15	

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	01/02/2018	Corrections, formatting
0.95	Sean Vinck	5/7/2018	Corrections and Formatting
0.96	Andrew Rudder	5/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	06/01/2018	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	Sean M. Hughes	08/29/2022	Annual Review. Updated to NIST 800-53r5
1.4	Thomas E. McDermott	11/27/2023	Corrections, Formatting, Updating and Annual Review
1.4	Anthony J. O'Neill	11/27/2023	Final Review
1.5	Thomas E. McDermott	11/22/2024	Corrections, Formatting and Annual Review
1.5	Anthony J. O'Neill	11/22/2024	Final Review

1.6	Thomas E. McDermott	2/10/2025	Updates, Corrections and Formatting
1.6	Miklos Lavicska	2/21/2025	Corrections and Formatting
1.6	Anthony J. O'Neill	3/13/2025	Final Review