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

Communication and Network Security Standard

Document Name: Communication and Network Security	Effective Date: October 15th, 2018
Document ID: IS.006	Last Revised Date: August 29, 2022

Table of contents

1. PURPOSE

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

- Network architecture requirements to include redundancy, network segmentation, encryption and the documentation of network diagrams
- Use of network infrastructure protection such as firewalls, intrusion detection systems, web-proxies and data loss prevention
- Controls to protect end-point computing systems
- Requirements for remote access
- Requirements for ***third-party*** business-to-business connections
- Requirements for secure file transfer

2. AUTHORITY

2.1. M.G.L. Ch. 7d provides that "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, electronic and computing devices, applications, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document, with respect to those services, as a condition of use. Executive Department 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 Security Office is responsible for the development and ongoing maintenance of this ***standard***.

4.2. The Enterprise Security Office is responsible for this ***standard*** and may enlist other departments to assist in the monitoring and maintaining of compliance with this ***standard***.

4.3. Any inquiries or comments regarding this ***standard*** shall be submitted to the Enterprise Security Office by sending an email to EOTSS-DL-Security Office.

4.4. Additional information regarding this standard and its related standards may be found at https://www.mass.gov/cybersecurity/policies.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Department including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus. Violations are subject to disciplinary action in accordance to applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

Exceptions) to any part of this document must be requested via email to the GRC Team (ITD-DL-Mass IT - Compliance). A policy exception may be granted only if the benefits of the exception outweigh the increased risks, as determined by the Commonwealth CISO.

6. STANDARD STATEMENTS

6.1. Network Security Management

Commonwealth Executive Offices and Agencies shall provide network security capabilities at a level that is reasonable and appropriate for the nature of the data being transmitted. Commonwealth Executive Offices and Agencies must ensure that that access to information assets is restricted to authorized ***personnel*** and protected at all times.

6.1.1. Network architecture and connectivity

The Commonwealth shall 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*** shall, at a minimum, include:

6.1.1.1 Network confidentiality: ***Controls*** shall include the use of encryption and device authentication to protect the confidentiality of transmitted information (see *Information Protection Requirements and Cryptographic Management Standards).*

6.1.1.2 Network segmentation: Networks shall 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.

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

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

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

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

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

6.1.1.5 Network documentation: the Commonwealth's network architecture shall be clearly documented.

6.1.1.5.1. Document internal and external network connections.

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

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

6.1.2. Use of firewalls

The Commonwealth shall 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. ***Controls*** shall, at a minimum, include:

6.1.2.1 Firewall and router configuration standards shall be established by the Enterprise Security Office that includes the following:

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

6.1.2.1.2. 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).

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

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

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

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

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

6.1.2.1.8. The process to track and monitor system and network configuration changes and resulting effects on the network (see *Change Management in the Asset Management Standard*). Changes shall only be approved after the completion of a formal risk acceptance.

6.1.2.2 Direct public access from the Internet to any internal system in the enterprise shall be prohibited. ***Controls*** shall, at a minimum, include:

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

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

6.1.2.2.3. 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.

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

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

6.1.3. Intrusion prevention and detection systems

The Enterprise Security Office shall 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 shall be configured to perform real-time analysis on traffic patterns for:

6.1.3.1 Networks with direct connectivity to open or untrusted networks.

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

6.1.3.3 Alert ***personnel*** of suspected compromises.

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

6.1.4. Denial of service protection

The Commonwealth shall implement and maintain controls to prevent denial of service events.

6.1.4.1 Application-layer flood denial of service attacks
6.1.4.2 Distributed denial of service attacks
6.1.4.3 Unintended denial of service attacks

6.1.5. Data loss prevention

The Commonwealth shall implement and maintain ***controls*** to prevent the loss of confidential information within the boundaries of legal and regulatory requirements. The DLP system shall be configured to perform analysis on data-at-rest, data-in-motion and data-in-use (see *Information Labeling and Handling in the Asset Management Standard*). The following guidance shall be considered in the data monitoring strategy for data-in-motion:

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

6.1.6. Domain name services (DNS)

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

6.1.6.2 Any external DNS query shall be handled by Commonwealth registered DNS servers.

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

6.1.6.4 Commonwealth shall implement controls to validate DNS queries and deny outbound connections for domains that are known to be untrusted.

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

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

6.1.6.7 A separate execution domain shall be maintained for each executing system process.

6.1.7. Dynamic host communication protocol (DHCP)

6.1.7.1 All ***information systems*** shall be assigned a Commonwealth assigned IP.

6.1.7.2 All IP addresses shall be centrally managed.

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

6.1.7.4 All DHCP assignment logs shall be collected and maintained for security monitoring purposes.

6.1.8. Web proxy

6.1.8.1 Internal host addresses must be hidden from the Internet.

6.1.8.2 Unauthenticated outbound traffic from the Commonwealth network is prohibited.

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

6.1.9. Administrative services protection

Access to administrative services shall be securely controlled, as follows:

6.1.9.1 Physical access to diagnostic and configuration ports shall be controlled and monitored.

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

6.1.9.3 All administrative access to any network device must use two-factor authentication.

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

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

6.1.9.5.1. Prior to the implementation of a firewall change, a risk assessment must be performed to assess the validity of the change request.

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

6.1.10. Wireless security

Authentication and network/transport layer encryption must be used for wireless connections to protect wireless access to Commonwealth networks. ***Controls*** shall, at a minimum, include:

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

6.1.10.2 ***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).

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

6.1.10.4 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 the Cryptographic Management Standard)*

6.1.10.5 All users must authenticate to the secure wireless access point using Commonwealth-approved two-factor authentication.

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

6.1.10.7 Commonwealth Executive Offices and Agencies 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).

6.1.10.8 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.

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

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

6.1.10.11 Collect and maintain wireless activity for security monitoring purposes.

6.2. Remote Access Security Management

All remote access connections into the Commonwealth’s internal networks shall be established through approved methods.

6.2.1. All external connections to the Commonwealth family of networks must be reviewed and approved by the Commonwealth CISO, Deputy CISO, or designee.

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

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

6.2.4. Remote connections shall be achieved by approved, secure remote access solutions.

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

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

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

6.2.6.1 Remote access shall require ***two-factor authentication.***

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

6.2.6.3 The ***remote access*** VPN shall employ a framework for encryption, centralized mutual strong authentication and dynamic ***key*** management between the mobile client and the VPN termination platform (refer to *Cryptographic Management Standard*).

6.2.7. Commonwealth shall provide a public DNS name for all internal services accessed remotely by all users, including third parties.

6.2.8. All collaborative computing devices and applications (such as remote meeting devices and applications, networked white boards, 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. Management of Third-party Network Access

6.3.1. Third-party access

Access shall be approved by the Enterprise Security Office if third parties require access to the Commonwealth's information assets. ***Controls*** shall, at a minimum, include:

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

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

6.3.1.3 All third-party access to the Commonwealth network shall be formally evaluated and approved by the Enterprise Security Office.

6.3.1.4 User access shall be limited to resources for which they have been authorized (see *User Access Management in Access Management Standard*).

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

6.3.2. Third-party business-to-business (B2B) connections

Third-party B2B connections to the Commonwealth's networks shall adhere to:

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

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

6.3.2.3 The Enterprise Security Office shall establish extranet monitoring and logging procedures (see *Logging and Event Monitoring Standard).*

6.3.2.4 Commonwealth Executive Offices and Agencies must ensure that ***Information Owners*** and ***Information Custodians*** shall ensure an expiration date is specified 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 Cryptographic Management Standard)*.

6.4.3. Files shall only transfer after positive authentication.

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

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

6.4.6. Exchange of data and software between organizations shall be based on a formal exchange agreement and shall be compliant with any relevant legal or regulatory requirement.

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 the 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 the *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 against spam, malware and phishing threats.

6.4.7.5 Collect and monitor logs for security monitoring purposes (see *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
6.3. Management of Third-party Network Access	IA-5	CSC 16	PR.AC-1
	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. RELATED DOCUMENTS

Document	Effective date

9. 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

The owner of this document is the Commonwealth CISO (or designee). It is the responsibility of the document owner to maintain, update and communicate the content of this document. Questions or suggestions for improvement shall be submitted to the document owner.

9.1 Annual Review

This *Communication and Network Security Standard* document shall be reviewed and updated by the document owner on an annual basis or when significant policy or procedure changes necessitate an amendment.