Information Security Policy

Effective Date: January 06, 2025	**Category:** Security
Scheduled Review: June 30, 2025	**Supersedes:** ITP-SEC000, ITP-SEC002, ITP-SEC010, ITP-SEC023, ITP-SFT005

1. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

2. Purpose

This Information Technology Policy (ITP) establishes a program to ensure that the Commonwealth meets or exceeds its legal and ethical responsibilities for securing its IT Resources

3. Scope

This policy applies to all offices, departments, boards, commissions, and councils under the Governor's jurisdiction and any other entity connecting to the Commonwealth Network (hereinafter referred to as "agencies").

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this policy as outlined herein.

4. Policy

For definitions found within this document, refer to the *IT Policy Glossary*.

OA/IT is responsible for protecting the Commonwealth's IT Resources in accordance with all applicable federal and state guidelines and regulations, as well as with effective information security practices and principles generally accepted as "due diligence" within the business community.

Appropriate action will be taken when loss, damage, or breach of confidentiality results from non-compliance with Commonwealth policies and Management Directives. Agencies found to be in non-compliance with ITPs must employ immediate corrective actions. Agencies must also have a compliance and risk management methodology in place to ensure agencies are maintaining compliance, remediating vulnerabilities, and reducing IT security risks.

In the absence of existing policies or procedures that cover new or existing security implementation, the Commonwealth will follow industry security best practices and/or well-known security standards such as the FIPS and Special Publications (SP) published by the NIST. If there is not a Security ITP that covers the scope of the security implementation, agencies must submit an exception for this policy accompanied by the specific proposed solution through the IT Policy Governance Process for review by the Enterprise Information Security Office (EISO). Refer to Section 6 for guidance on the IT Policy Governance Process.

4.1 Offshore Access

Offshore access to Commonwealth production systems, whether hosted by the Commonwealth or by third parties, is prohibited by anyone not physically located in CONUS. This includes, but is not limited to:

- Virtual Private Network (VPN)
- Remote desktop
- Virtual Desktop Infrastructure (VDI)
- Cloud infrastructure such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) offerings
- All access to Commonwealth "C" designated data, as defined in the *Data Classification Policy*
- Authorized Users are prohibited access to all Commonwealth IT Resources and data from countries which are blocked by the Enterprise GeoIP service in accordance with the *Firewall Policy*https://www.oa.pa.gov/Policies/Documents/itp_sec034.pdf.

It is required that all Commonwealth "C" designated data, as defined in the *Data Classification Policy,* reside in CONUS where it is subject to the laws and regulations of the United States and the various jurisdictions within the United States. Transmission to Offshore systems or storage on Offshore systems is prohibited.

Offshore direct remote access to "C" designated data on any Commonwealth production system is prohibited regardless of the file type or storage medium. This includes, but is not limited to:

- Databases
- Documents (PDF, Word, Text, etc.)
- Spreadsheets
- Images

Offshore direct remote access to networking equipment (including but not limited to routers, switches, firewalls, etc.)prohibited.

Offshore work will be strictly limited to lower and test environments. There shall be no offshore access to production servers or to production environments. Offshore resources will only receive test or anonymized data that is not traceable or linkable to "C" designated data. Offshore resources should have no access to production data.

Offshore work shall be performed in accordance with the *Security Requirement Traceability Matrix Guideline* All maintenance and support after system implementations shall be performed by resources located and authorized to work within CONUS. Offshore resources shall not be used for any post go live support.

4.2 Technical Security Assessments

This section provides guidance for Technical Security Assessments including, but not limited to, security tests, reviews, assessments, and audits. This policy minimizes the collective security risks associated with deficiencies in all agencies connected to the Commonwealth Network.

Technical Security Assessments shall be conducted on all systems and services that:

- Interact with the public; or
- Are on the Metropolitan Area Network (MAN) and not in a Demilitarized Zone (DMZ).

Technical Security Assessments shall be conducted when a system or service:

- Processes or stores Class "C" or Closed Records (as indicated in the *Data Classification Policy*; or
- Provides non-classified information (information that is not classified as Class "C" or Closed Records as above) to ensure compliance with implementation standards and that vulnerabilities from previously discovered threats are not present.

Agencies shall maintain a listing of critical agency functions. IT systems and services essential to supporting these critical agency functions shall have Technical Security Assessments conducted on them at least once (1) every year. Technical Security Assessments of a representative sample of all other systems and services shall be conducted at least once every two (2) years.

The Office of Administration, Office for Information Technology (OA/IT) Enterprise Information Security Office (EISO) is responsible for conducting ongoing Technical Security Assessments on IT systems and services on the Commonwealth network. These assessments are used to benchmark the Commonwealth's IT security readiness and risk posture. Agencies may choose to outsource the performance of the Technical Security Assessments to an Independent Third Party.

Agencies that choose to outsource the Technical Security Assessments shall ensure notification is provided to the EISO no less than five (5) business days prior to the start of the assessment. This is to provide the opportunity for the EISO to request additional information regarding the selected Independent Third-Party and the method proposed.

Service Organizations shall ensure all solution components are securely coded, vetted, and scanned. To this end, the Service Organization will be required to provide scan data from the required Technical Security Assessments to the Agency Information Security Officer (ISO). For propriety code, applications, software as a service (SaaS), a letter of attestation showing that the code is properly vetted, and applications are managed will suffice. Agencies and Services Organizations shall ensure all work performed is in alignment with this policy, section 4.1 Offshore Access.
Agencies that are having assessments conducted on systems and services shall provide reports to the Agency ISO and EISO Vulnerability Management Team (RA-OAEISOVulnMgmt@pa.gov) for a compliance review. If detailed reports are unavailable, a letter of attestation shall be provided showing the compliance status.

Agencies shall remediate pertinent vulnerabilities, complete questionnaires, conduct internal audits, and perform IT security tests to ensure that they are compliant with the Commonwealth's IT policies, procedures, and standards.

Agencies shall read and comply with the following supporting policy documents, which will provide detailed information about the required Technical Security Assessments:

- *Security & Compliance Assessment Testing Guideline*
- *Systems & Services Vulnerability Scanning Procedure*
- *Penetration Testing Procedure*
- *Nationwide Cyber Security Review Procedure*

4.3 Reverse-Proxy Servers and Services

This section provides direction regarding the use of Reverse-Proxy Servers and Services by Commonwealth agencies. In addition, it establishes policy for the utilization of the Office of Administration, Office for Information Technology (OA/IT) Reverse Proxy Managed Services and the approval process to continue to use existing or obtain new servers and/or services.

To ensure maximum security within the Commonwealth, OA/IT maintains Reverse Proxy Managed Services for agency use. Agencies are required to utilize the OA/IT Reverse Proxy Managed Services to fulfill their business requirements for Reverse Proxy Servers and Services.

An approved IT policy exception is required if an agency has a technical limitation that requires the implementation of its own Reverse-Proxy Server and/or utilization of a standard reverse proxy service for a web server at an agency location. Due to the criticality of enterprise-wide security standards for web applications, OA/IT strongly discourages agencies from seeking exemptions to this policy.

Reverse-Proxy Servers, and all corresponding web servers, whether at a Commonwealth Datacenter location or at an agency location, will be subject to security and vulnerability scans prior to network connectivity and on a regular basis thereafter, and will be required to comply with the *Enterprise Host Security Policy*. Agencies shall refer to the *eCommerce*

Policy and this policy for further guidance regarding the requirements for security and vulnerability scans.

The Enterprise Information Security Office (EISO) will create and assign a security incident ticket in Archer (governance, risk and compliance tool) to the SOA/IT Enterprise Data Center (EDC) Information Security Officer (ISO) or the respective agency ISO if a security vulnerability exists and/or a security incident occurs on a Reverse-Proxy Server or web server. A timeframe will be established for remediation based on the severity level of the security incident ticket and in alignment with the *IT Security Incident Reporting Policy*. If the concern is not addressed within the requested timeframe, OA/IT will take appropriate action to mitigate the threat.

4.4 Virtual Private Networks

This section establishes the policy, responsibilities, and procedures for mitigation of the risks associated with the transmission of sensitive information across networks when implementing Virtual Private Networks (VPNs) based on Internet Protocol Security (IPsec) or the Transport Layer Security (TLS) protocol.

This ITP represents the minimum operational standards for network-based IPsec, and TLS VPN configurations between trusted and untrusted networks. The use of an approved VPN connection is required for any access to the Commonwealth's IT resources from outside of the United States; this includes access to Microsoft Office 365 services (including email) and other cloud-based Commonwealth services from outside of the United States. Agencies shall comply with this policy and submit an IT policy exception request for all OCONUS access requests. Please note that approval is not guaranteed. Use of alternative connectivity such as Virtual Desktop Infrastructure (VDI) is strongly encouraged over VPN to further limit risk. Agencies shall refer to *Virtual Private Network Standard* for a listing of current VPN standards.

Agencies shall utilize the Gateway-to-Gateway or Host-to-Gateway (inbound) VPN integrated models to facilitate a secure connection between remote users and/or systems.

4.4.1 Gateway-to-Gateway VPN Minimum Policy Requirements

The Gateway-to-Gateway VPN model protects communications between two specific networks, such as from one agency central office network to another, from an agency central office network to another internal agency branch office network, or between an agency's central offices to trusted business partners networks. Split-tunneling is prohibited except for specific traffic as defined in the Configurations for *VPN Split-Tunneling and Host-to-Gateway Session Length Standard.*

Network-to-network VPNs shall use one of two protocols: IPsec, as a digital certificate (preferred) or pre-shared key, or TLS, which uses a digital certificate.

IPSec VPN pre-shared keys shall comply with the requirements defined in the *Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication Standard.*

Systems shall be configured to support at least the minimum configurations (ciphers, protocols, and signing) referenced in the *Encryption Policy*.

4.4.2 Host-to-Gateway (Inbound) VPN Minimum Policy Requirements

This model protects communications between one or more individual Hosts and a specific network belonging to an agency. The host-to-gateway VPN model is most often used to allow hosts on unsecured networks, such as traveling employees and telecommuters, to gain access to internal organizational services. Split-tunneling is prohibited except for specific traffic as defined in the *VPN Split Tunneling and Host-to-Gateway Session Length Standard,* Local Area Network (LAN) access to local resources (printers, file shares) while connected to VPN is prohibited. VPN-Connected Host to VPN-Connected Host traffic (i.e., between connected VPN Clients) is prohibited.

Multi-factor authentication, as described in the *Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication Standard* shall be utilized for a Host-to-Gateway VPN. Agencies are to comply with the standards as described in this document and the *Encryption Policy.*

4.4.3 Host-to-Gateway (Outbound) VPN Policy Restriction

Commonwealth Hosts are prohibited from being configured or utilizing any non-commonwealth VPN clients to individually connect and access any non-commonwealth IT resources (including networks). This includes host VPN connections to Business Partners, Federal partners, and Service Organizations. In instances where agencies require this type of secure collaboration with an external partner, the Gateway-to-Gateway VPN model is required.

4.4.4 Session Length Requirements

The Office of Administration, Office for Information Technology (OA/IT) has configured an Enterprise-wide Host-to-Gateway maximum VPN session length as defined in the *VPN Split Tunneling and Host-to-Gateway Session Length Standard* to meet compliance requirements. While connected to VPN, the remaining session time prior to the VPN session automatically terminating is continuously displayed in the VPN client on the main window. After this time expires, users must reauthenticate.

4.4.5 VPN Remote Access Multi-Factor Requirements

All remote access VPN logins require multi-factor authentication (MFA). MFA requires users to provide at least two proofs of their identity, which increases security for access to Commonwealth IT resources. It reduces the risk that business or personal information stored in administrative systems will be compromised.

4.4.6 VPN Remote Access Control Endpoint Checks

VPN elements of an endpoint check are enforced to check for current anti-virus software and operating system service pack levels before the remote user will be allowed access to the network.

The following requirements related to all agency managed or enterprise remote access systems and technologies (Desktop/Laptop Operating Systems and Mobile Devices) shall be met:

- Commonwealth-issued desktops or laptop operating systems shall be compliant with Current and Contain standards per the *Desktop and Laptop Operating System Standards.*
- Commonwealth-issued mobile devices shall comply with the *Mobile Device Policy* and are authorized for remote access.
- Non-Commonwealth electronic devices shall be compliant with the *Mobile Device Policy* and shall have been approved for such use through a current approved IT policy exception.

Any Commonwealth-issued desktop or laptop operating system categorized as Retired or not listed in *Desktop and Laptop Operating System Standards* is prohibited from being utilized for remote access. Hardware ownership may be checked upon connection attempt.

A list of supported anti-virus applications for endpoint checks can be found on the IT Central Security Services Page under Protection/Endpoint (Commonwealth authorized access only). In addition:

- Anti-virus definitions shall comply within a maximum of ten (10) definition file versions from the vendor's latest release.
- Desktop and laptop operating systems shall follow the *Desktop and Laptop Operating System Standards*.
- Internet browsers shall follow the *Internet Browser Standard*.

4.4.7 VPN Configurations for Service Organizations

Service Organizations shall refer to the *Site-to-Site VPN Configurations for Service Organizations Guideline* when determining the configurations for an appropriate VPN solution within their environment for systems which host or transmit Commonwealth Data.

4.5 Managed File Transfer

This section establishes policy for the use of the Enterprise Managed File Transfer (MFT) by the Commonwealth, its business partners, and the public to exchange files and data securely in various formats that are too large to be transferred via e-mail.
There is a need across the Commonwealth to securely transfer large volumes of data across agencies, business partners, and customers. While File Transfer Protocol (FTP) was used in the past, the technology was not designed to be a secure protocol, nor on its own, provide a way to secure or manage the payload or the transmission. With security and compliance in mind, MFT does more than simply secure files while being transferred. MFT manages the secure transfer of data from one computer to another through a network and offers a higher level of security and control than FTP, along with an increased focus on auditing, records management, and security.

Agencies shall review the enterprise MFT service offering, which is detailed in the Enterprise Service Catalog. Agencies are encouraged to leverage the enterprise MFT service offering when the offering meets their needs. Agencies interested in leveraging or obtaining more information regarding the enterprise MFT service offering should contact the Office of Administration, Office for Information Technology (OA/IT) at ra-enterpriseftpserv@pa.gov to discuss options for the use of the service.

Agencies shall adhere to the standards for MFT products detailed in the *Managed File Transfer Standard*. The use of any MFT or FTP service other than the Enterprise Service Offering or those listed as a current standard requires an approved IT policy exception.

All FTP servers shall have logging enabled. FTP logs shall meet the minimum logging requirement identified in the *IT Vendor Risk Management Policy* and the *Security Logging and Event Monitoring Policy*.

Prior to initiating any file transfers exceeding 500 Mbps, agencies shall first consult with the Enterprise Network Operation Section (ENOS) at ENS@pa.gov.

Internet-accessible Anonymous FTP has been identified as a security risk to the Commonwealth, and as such, shall not be made available without an approved IT policy exception against this policy. Any agency that has its own Internet-accessible FTP server shall remove Anonymous FTP capability immediately or submit an IT policy exception request for continued use.

Agencies shall ensure that if they are providing any sensitive data or data covered under the *Pennsylvania Breach of Personal Information Notification Act, as amended November 2, 2022, P.L. 2139, No. 151, 73 P.S. §§ 2301—2330*, the data shall be encrypted in accordance with the Encryption Policy.

All public facing sites shall contain a banner warning end users regarding the acceptable use of the site and the posting of sensitive information. Public facing MFT or FTP sites shall not be used for the distribution of commercial software that requires a valid license for use. MFT servers are subject to random scans by OA/IT.

5. Contact

Questions or comments may be directed via email to OA, IT Policy.

6. Exception from Policy

In the event an agency chooses to seek an exception from this policy, a request for a policy exception shall be submitted via the IT policy exception process. Refer to *IT Policy Governance Policy* for guidance.

7. Revision History

This chart contains a history of this publication's revisions. Redline documents outline the revisions and are available to Commonwealth users only during the drafting process.

Version	Date	Purpose of Revision
Original	01/06/2025	Base Document