pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Security Policy Requirements for Third Party Vendors

Number
OPD-SEC000B

Effective Date
January 2021

Category
Security

Supersedes
None

Contact
RA-ITCentral@pa.gov

Scheduled Review
July 2024

1. Purpose

This Operations Document (OPD) establishes the requirements for how third-party vendors, contractors, suppliers or offerors (collectively referred to herein as "contracted resources") shall meet the established guidelines within the Commonwealth's Information Technology Policies (ITPs).

2. Policy

Contracted resources shall comply with and adhere to the Commonwealth Security Policies and Standards for any developed materials under a Contract resulting from a procurement for IT products and/or services during the term of a contract. These IT Policies (ITPs) may be revised from time to time, and the contracted resource shall comply with all such revisions. The Offeror shall submit a narrative response with their proposal explaining how its proposal addresses each of the following Commonwealth security ITPs. The Commonwealth CISO or Agency ISO has discretion to review and monitor performance of compliance with IT Security Policies and ITPs.

IT Policy	Requirement
ITP-SEC000 - Information Security Policy	• Comply with requirements for all Commonwealth security ITPs listed within this document. • Ensure the location(s) of server and data centers as well as the location of the workforce accessing them are within the United States of America. • Ensure IT environments and systems that contain Commonwealth data comply with all Commonwealth ITPs, and as changes and revisions are made, reflect alignment with the most current Commonwealth ITPs.
ITP-SEC001 - Enterprise Host Security	• Promptly investigate any suspected security incidents. Implement procedures for responding to and reporting incidents, breaches, or misuse of IT Resources, as outlined in ITP-SEC024.

IT Policy	Requirement
Software Suite Standards and Policy	• Utilize the Commonwealth's standard software or an industry standard for EDR on all servers, desktops, and laptops that are utilized to access or host Commonwealth data. • Install and maintain appropriate EDR monitoring and management agents on all servers, desktops, and laptops that are utilized to access or host Commonwealth data. • Ensure systems which access or host Commonwealth data are being actively monitored and run weekly reports to ensure compliance EDR and anti-virus standards. • Implement procedures to mitigate overall and specific risks of breach or misuse of Commonwealth IT Resources and their associated damages and costs. This would include patching (ITP-SEC041 *Commonwealth IT Resources Patching Policy*), internal and external scanning (ITP-SEC023 *IT Security Assessment & Testing Policy*), and monitoring. • Utilize industry standard anti-virus, anti-malware, Host Intrusion Prevention, incident response procedures, monitoring, reporting, network, and application firewalls in accordance with ITP-SEC001 for real-time scanning, detection, removal, and blocking of potentially malicious content. • Ensure the names, work and mobile phone numbers, and work e-mail addresses for a primary and backup contact are provided to the Commonwealth CISO at ra-ciso@pa.gov.
ITP-SEC003 - Enterprise Security Auditing and Monitoring	• Implement services for internet access monitoring, content filtering, SSL decryption and inspection.
ITP-SEC004 - Enterprise Web Application Firewall	• Implement a web application firewall (WAF). The WAF shall be used to protect data as outlined in ITP-SEC019 and classified under ITP-INF015 as Class "C" Classified Records or Closed Records following the standards set forth in ITP-SEC004. In addition, the WAF shall: 1. Minimize the threat window for each exposure by blocking access to the vulnerability until the vulnerability can be fixed in the source code; 2. Meet PCI, HIPAA, and Privacy compliance requirements; 3. Monitor end-user's transactions with a web application; and 4. Provide an additional layer of web application hardening Open Web Application Security Project (OWASP) protection.
ITP-SEC005 – Commonwealth Application Certification and Accreditation	• Scan all application code for vulnerabilities using an industry standard static and dynamic code scanning tool. • Ensure internet facing and web facing applications applicable to this ITP go through the Commonwealth Application Certification and Accreditation (CA^2) process before being deployed to production. • Provide attestation of ongoing scanning in accordance with ITP-SEC023.

IT Policy	Requirement
	• Ensure secure coding practices are built within applications according to the Software Development Lifecyle (SDLC) process, refer to NIST SP 800-160v1r1. • Ensure applicable applications go through the CA[2] reaccreditation process every 3 years.
ITP-SEC007 - Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication (additional reference ITP-SEC039)	• Commonwealth's enterprise directories and password policies shall be utilized. • Implement multi-factor authentication (MFA) for contracted resources requiring direct access to a system from outside the Commonwealth network. Where possible, the Commonwealth's MFA solution shall be utilized. • Implement MFA for any systems containing Class "C" Classified Records or Closed Records (per ITP-INF015).
ITP-SEC009 - Minimum Contractor Background Checks Policy	• Conduct background checks and provide for each contracted resource and any subcontracted resources who will have access to Commonwealth data or Commonwealth owned or leased facilities, either through onsite or remote access. • Background checks are to be conducted via the Request for Criminal Record Check for in-state contracted or subcontracted resources or via a criminal background check through the appropriate state agency for out of state contracted or subcontracted resources. • The background check shall be conducted prior to initial access by the contracted or subcontracted resources and annually thereafter. • Ensure a fingerprint database search is conducted for contracted or subcontracted resources having access to Criminal Justice Information (CJI), Federal Tax Information (FTI), Criminal History Record Information (CHRI), and PA Commonwealth Law Enforcement Assistance Network (CLEAN) by either on site or remote computer access. • Be responsible for the payment of all fees associated with background checks for their contracted or subcontracted resources.
ITP-SEC010 - Virtual Private Network Standards	• Require Virtual Private Network (VPN) access to its networks and/or connected systems. • Utilize a VPN connection for any access to the Commonwealth network from an external source.
ITP-SEC015 - Data Cleansing Policy	• Implement process(es) for the cleansing of data from electronic media when the data retention requirements have expired, the data is no longer needed, or the data is scheduled for disposal as determined by the Commonwealth. • Degauss, wipe or destroy decommissioned electronic media in accordance with ITP-SEC015 and by following best practices outlined in NIST SP 800-88r1.
ITP-SEC016 - Commonwealth of Pennsylvania - Information	• Provide contact information for an Information Security Officer (ISO) and backup ISO who are responsible for all security matters related to the Commonwealth account.

IT Policy	Requirement
Security Officer Policy	
ITP-SEC017 – CoPA Policy for Credit Card Use for e-Government	• Accept credit card payments and adhere to PCI requirements (if applicable as per the contract).
ITP-SEC019 - Policy and Procedures for Protecting Commonwealth Electronic Data	• Utilize a web application firewall (WAF) to protect data classified under ITP-INF015 as Class "C" Classified Records or Closed Records utilizing the standard set forth in ITP-SEC004. • Encrypt Class "C" Classified or Closed Records at rest using encryption standards set forth in the ITP-SEC031 and the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program. ○ For Criminal Justice Information, encryption must also meet CJIS policy requirements. ○ For systems receiving, processing, or storing Federal Tax Information (FTI), encryption must also meet IRS Publication 1075 requirements.
ITP-SEC021 - Security Information and Event Management Policy	Log events to include: 1. Log collection and consolidation; 2. Security event collection from multiple sources (firewalls, routers, servers, etc.); 3. Identification of security related events and incidents; 4. Automated response/alerting capability when incidents are detected; and 5. Correlation of events from multiple sources.
ITP-SEC023 - Information Technology Technical Security Assessments Policy	• Perform assessments, audits, vulnerability scanning, and/or penetration testing consistent with the standards as outlined in ITP-SEC023.
ITP-SEC024 - Cyber Security Incident Reporting Policy	• Provide notice to applicable agency as soon as reasonably practical upon discovery of a cyber security incident, but no later than the time period specified in the applicable terms of the contract and in accordance with the Pennsylvania Breach of Personal Information Notification Act. • Have a documented cyber security incident response process and ensure all suspected cyber security incidents are reported to the Enterprise Information Security Office at ra-ciso@pa.gov or 1-877-552-7478. • Follow a cyber security incident response process, including, but not limited to, disconnecting a system from the network, confiscating hardware for evidence, providing information for investigative purposes, that meets Commonwealth standards set forth in ITP-SEC024.

IT Policy	Requirement
ITP-SEC025 – Proper Use and Disclosure of Personally Identifiable Information (PII)	• Perform a data element inventory, identifying and classifying all PII generated, collected, stored, used, and disclosed by the agency or third party on the agency's behalf. • Ensure access or use of information utilizing PII, or other protected data types (CJIS, FTI, HIPAA, etc.) for any purpose, is properly controlled, encrypted, and restricted to prevent unauthorized use or disclosure (refer to ITP-SEC019, ITP-SEC031 and NIST 800-122). For Social Security Administration (SSA) compliance, the system's encryption methods must align with the guidelines established by NIST. SSA recommends the Advanced Encryption Standards (AES) or Triple Data Encryption Algorithm (Triple DES). • Take appropriate measures, implement necessary technology, and establish operating procedures to ensure data privacy is maintained. • Limit the generation, collection, storage, use, and disclosure of PII to that which is necessary for business purposes only. • Ensure that systems that require a unique identifier do not use PII as that identifier. • Assign a unique identification number to an individual for systems requiring it. The unique identification number cannot be the same as or cannot be traced back to users PII. Security must be applied, and care must be taken to ensure that access to the electronic system and use of these unique identification numbers are restricted in accordance with any law or other agency requirement. • Ensure contracted resource and agency hosted systems do not display PII visually, whether on computer monitors, printed forms, or other system output, unless required by any law or other requirement applicable to an agency, or business necessity. • Report security incidents involving PII following ITP-SEC024 in addition to any other laws or regulations for incidents or data breaches, such as the Breach of Personal Information Notification Act. • Use of cloud storage requires advanced approval by the contracting Agency and the Office of Administration.
ITP-SEC029 - Physical Security Policy for IT Resources	• Implement policies and practices to ensure the protection of physical facilities and appropriate screening for facility access for any IT facility or resource hosting Commonwealth data. • Ensure their personnel cooperate with Commonwealth site requirements, which includes providing information for Commonwealth badging and being escorted. Contracted resources and Commonwealth approved subcontracted resources who do not have a Commonwealth badge, shall always display their company identification badge while on Commonwealth premises. The Commonwealth reserves the right to request additional photo identification from contracted and subcontracted resources. • Document an inventory of items (such as tools and equipment) being brought onto the Commonwealth worksite, and to submit to a physical search at Commonwealth worksites that have this

IT Policy	Requirement
	requirement for persons entering their premises such as the State Police or Department of Corrections. ○ Ensure contracted and subcontracted resources always have a list of tools being brought onto the worksite and are prepared to present the list to a Commonwealth employee upon arrival, as well as present the tools or equipment for inspection. ○ Before leaving the worksite, contracted and subcontracted resources will again present the list and the tools or equipment for inspection and may be searched by Commonwealth staff, or a correctional or police officer. • Restrict access to their IT facilities and resources to only authorized persons. • Ensure their IT facilities and resources hosting or accessing Commonwealth data designate a certified party to review access records and visitor logs in accordance with ITP-SEC029 and any applicable legislation. Access records and visitor logs shall be retained for a period of no less than one year. • Ensure their IT facilities and resources hosting or accessing Commonwealth data are physically protected in proportion to the data or application's criticality or functional importance.
ITP-SEC031 - Encryption Standards	• Ensure protection of Commonwealth data that is stored within the contracted resource's systems. • Ensure Commonwealth Class "C" Classified or Closed Records (per ITP-INF015) are encrypted during rest and transit per ITP-SEC019, ITP-SEC031 and NIST Cryptographic Module Validation Program. • Ensure use of Full Disk Encryption for archiving and back up Class "C" Classified or Closed Records. • Ensure non-Windows environments requiring Full Disk Encryption, utilize Full Disk Encryption that conforms to ITP-SEC031, AES specifications and the NIST Cryptographic Module Validation Program. • Ensure use of Data Element Encryption when Class "C" Classified Records or Closed Records data elements are stored within a database. Transparent Data Encryption (TDE) or other database specific methods can be utilized to meet this requirement. • Ensure, for systems and data containing Criminal Justice Information, Criminal Justice Information Services (CJIS) Policy requirements are met. • Ensure, for systems receiving, processing, or storing Federal Tax Information (FTI) IRS Publication 1075 requirements are met.
ITP-SEC032 - Enterprise Data Loss Prevention (DLP) Compliance Standards	• Implement a Data Loss Prevention (DLP) technology/solution.
ITP-SEC034 - Enterprise Firewall Rule Set	• Ensure any devices with access to or hosting Commonwealth data are protected by a perimeter firewall system.

IT Policy	Requirement
	○ An audit must be performed to identify all application service protocols to ensure specific port requirements are documented and applied to the necessary firewall(s).
ITP-SEC035 - Mobile Device Security Policy	• If mobile device access to Commonwealth resources or data is permitted, a Mobile Device Management (MDM) solution shall be implemented to manage access and protect Mobile Devices in the event they are lost or stolen.
ITP-SEC038 - COPA Data Center Privileged User Identification and Access Management Policy	• Ensure default application and/or hardware passwords are changed and managed to meet the Commonwealth standards set forth in ITP-SEC007 *Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication*.
ITP-SEC039 – Keystone Login and Identity Proofing	• Ensure all citizen facing applications use Keystone Login for Authentication services. Provide technical controls for interfacing with Commonwealth authentication services.

ITP-SEC040 – IT Service Organization Management and Cloud Requirements	• Comply with the requirements of this ITP by coordinating with respective agencies to complete the Compute Services Requirements (CSR) document as part of the Use Case Review Process.
	• Submit relevant SOC reports and if required, an attestation letter for any Subservice Organizations on an annual basis or as otherwise set forth in the applicable contract.
	  • If using a Subservice Organization, the Service Organization is responsible for obtaining and reviewing the Subservice Organization reports to ensure compliance with Commonwealth requirements.
	  • In a timely manner, respond to any clarification requests, corrective action plan(s), and address, remediate, or mitigate identified concerns or nonconformities and recommendations.
	• Submit Accessibility Conformance Reports (ACRs) as applicable to the services being provided.
	• Submit any other relevant artifacts the Service Organization deems beneficial to complete the CSRC Review.

ITP-SEC041 – Commonwealth IT Resources Patching Policy	• Ensure security patches are applied in accordance with this ITP to any systems connecting to the Commonwealth network or supporting Commonwealth systems or applications.

This chart contains a history of this publication's revisions.

Version	Date	Purpose of Revision
Original	01/01/2021	Base Document
Revision	05/27/2022	ITP Refresh Updated OPD to streamline requirements throughout for consistency with those required for Third Parties. Removed ITP-SEC002, ITP-SEC006, ITP-SEC008, ITP-SEC011, & ITP-SEC012 from policy. Added ITP-SEC040 to policy. Added/updated links to policies and references throughout OPD.
Revisions	07/18/2023	Revisions were made to ITP requirements based on current third-party requirements listed in applicable ITPs.