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
June 2023

1. Purpose

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

2. Policy

The contractor 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 contractor 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 the Third-party Vendors', Business Partners', or Contractors' compliance with IT Security Policies and ITPs.

IT Policy	Requirement
ITP-SEC000 - Information Security Policy	The contractor shall ensure the location(s) of its server and data centers as well as the location of the workforce accessing them are within the United States of America. The contractor's IT environment and systems which contain Commonwealth data must comply with all Commonwealth ITPs, as changes and revisions are made, to reflect alignment with the most current Commonwealth ITPs.
ITP-SEC001 - Enterprise Host Security Software Suite	The contractor shall provide a mandatory information security awareness training and education program to all their employees and contractors.

Standards and Policy	The contractor shall ensure compliance with federal and state guidelines and regulations regarding the collection, maintenance, use, and security of IT Resources, as defined in Management Directive 205.34. The contractor shall ensure implementation of prudent, reasonable, and effective practices for the protection and security of IT Resources, which includes the protection of Class "C" Classified Records or Closed Records, as defined in ITP-SEC019, against accidental or deliberate unauthorized disclosure, modification, or destruction The contractor shall establish procedures for responding to incidents, breaches, or misuse of IT Resources, as outlined in ITP-SEC024. The contractor shall implement processes for protecting Class "C" Classified Records or Closed Records during transmission, processing, and storage. The contractor shall implement procedures to mitigate overall and specific risks of breach or misuse of Commonwealth IT Resources and the damages and costs associated with a breach or misuse. This would include patching, internal and external scanning, and monitoring. Industry standard antivirus, anti-malware, Host Intrusion Prevention, incident response, monitoring, reporting, network, and application Firewalls, must be utilized in accordance with ITP-SEC001 for real-time scanning, detection, removal, and blocking of potentially malicious content.
ITP-SEC003 - Enterprise Security Auditing and Monitoring	The contractor shall implement services for Internet access monitoring, content filtering, SSL decryption and inspection.
ITP-SEC004 - Enterprise Web Application Firewall	The contractor shall implement a web application firewall (WAF). The WAF shall be used to protect data classified under ITP-SEC019 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	The contractor shall scan all application code for vulnerabilities using an industry standard, static and dynamic, code scanning tool. Web facing applications are required to go through the Commonwealth

	Application Certification and Accreditation [(CA)2] process before being deployed to production. The contractor shall provide attestation of ongoing scanning in accordance with ITP-SEC023. Ensure secure coding practice are built within applications according to the Software Development Lifecyle (SDLC) process, refer to NIST SP 800-64r2. Applications are to undergo a (CA)2 reaccreditation process every 3 years.
ITP-SEC007 - Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication (additional reference ITP-SEC039)	The contractor shall utilize the Commonwealth's enterprise directories and password policies. Multi-factor authentication (MFA) shall be implemented by the contractor for users requiring direct access to the system from outside the Commonwealth network. Where possible, the Commonwealth's MFA solution shall be utilized. For systems containing Class "C" Classified Records or Closed Records (per ITP-SEC019) MFA shall be implemented.
ITP-SEC009 - Minimum Contractor Background Checks Policy	The contractor shall arrange for a background check for each of their contracted resources, as well as for 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 contractors or via a criminal background check through the appropriate state agency for out of state contractors. The background check is to be conducted prior to initial access by the contractor and annually thereafter. A fingerprint database search will be required for contracted resources having access to the PA Commonwealth Law Enforcement Assistance Network (CLEAN) by either on site or remote computer access. The contractor will be responsible for the payment of all fees associated with background checks for their contracted resources and/or subcontracted resources.
ITP-SEC010 - Virtual Private Network Standards	The contractor shall require Virtual Private Network (VPN) access to its networks and/or connected systems. Contractor-managed MFA shall be required for all VPN users. Contractor-managed endpoints with endpoint protection product(s) installed and enabled shall be required for VPN access. Endpoints shall be scanned for malware and current patch levels prior to any network access and/or connected system access being granted. Split-tunneling for general internet access shall be prohibited for all VPN connections.

ITP-SEC015 - Data Cleansing Policy	The contractor shall implement processes 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. Decommissioned electronic media must be degaussed, wiped, or destroyed in accordance with ITP-SEC015 and by following best practices outlined in NIST SP 800-88r1.
ITP-SEC016 - Commonwealth of Pennsylvania - Information Security Officer Policy	The contractor shall provide contact information for an information security officer who is responsible for all security matters related to the Commonwealth account.
ITP-SEC017 – CoPA Policy for Credit Card Use for e-Government	The contractor shall 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	The contractor shall implement processes for classifying sensitive data and protecting Class "C" Classified Records or Closed Records entrusted to its care. A data element inventory shall be performed, identifying and classifying all PII generated, collected, stored, used, and disclosed by the agency or third party on the agency's behalf. A web application firewall (WAF) shall be used to protect data classified under ITP-SEC019 as Class "C" Classified Records or Closed Records utilizing the standard set forth in ITP-SEC004. All Class "C" Classified or Closed Records at rest shall be encrypted 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), must also meet IRS Publication 1075 requirements.
ITP-SEC021 - Security Information and Event Management Policy	The contractor shall 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 Security Assessment and Testing Policy	The contractor must perform assessments, audits, vulnerability scanning, and/or penetration testing consistent with the standards as outlined in this policy.
ITP-SEC024 - Cyber Security Incident Reporting Policy	The contractor shall describe its processes to ensure compliance with the Pennsylvania Data Breach Notification Act. The contractor shall 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. The contractor shall 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, etc. that meets Commonwealth standards set forth in ITP-SEC024.
ITP-SEC025 – Proper Use and Disclosure of Personally Identifiable Information (PII)	The contractor shall 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. All entities maintaining files, utilizing PII, or Class "C" Classified Records or Closed Records for any purpose, shall ensure that access or use of such information is properly controlled, encrypted, and restricted to prevent unauthorized use or disclosure (refer to ITP-SEC019, ITP-SEC031 and NIST 800-122). All contractors shall take appropriate measures, implement necessary technology, and/or 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. Systems that require a unique identifier shall not use PII as that identifier. All systems, which must assign an identifying number for an individual, must assign a unique identification number that is not 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 requirement applicable to an agency. Systems that are contractor or agency hosted shall not display PII visually, whether on computer monitors, or on printed forms or other

	system output, unless required by any law or other requirement applicable to an agency, or business necessity. Ensure security incidents involving PII are reported following ITP-SEC024 in addition to any other laws or regulations for incidents or data breaches. Use of cloud storage requires advanced approval by the contracting Agency and the Office of Administration.
ITP-SEC029 - Physical Security Policy for IT Resources	The contractor shall implement policies and practices to ensure the protection of physical facilities and appropriate screening for facility access. While working at any Commonwealth facility, the contractor's personnel shall ensure cooperation with Commonwealth site requirements, which includes providing information for Commonwealth badging and being escorted. Contractors and Commonwealth approved subcontractors 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 contractor and subcontractor personnel. Some Commonwealth sites, e.g., the State Police and Department of Corrections, require each person entering the premises to document an inventory of items (such as tools and equipment) being brought onto the site, and to submit to a physical search of his or her person. Therefore, contractor and subcontractor personnel shall always have a list of tools being brought onto a site and be prepared to present the list to a Commonwealth employee upon arrival, as well as present the tools or equipment for inspection. Before leaving the site, contractor and subcontractor personnel will again present the list and the tools or equipment for inspection. Upon both entering the site and leaving the site, contractor and subcontractor personnel may be searched by Commonwealth staff, or a correctional or police officer. The contractor shall restrict access to their IT facilities and resources to only authorized persons. The contractor shall 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. The contractor shall ensure their IT facilities hosting Commonwealth data maintain and archive access records and sign-in logs for a period of not less than one year. The contractor shall 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	The contractor shall ensure protection of Commonwealth data that is stored within contractor's systems. The contractor shall ensure Commonwealth Class "C" Classified or Closed Records are encrypted during rest and transit per ITP-SEC019, ITP-SEC031 and NIST Cryptographic Module Validation Program. Full disk encryption shall be used for archiving or backing up Class "C" Classified or Closed Records to any offline or storage media. Non-Windows environments requiring full disk encryption shall utilize full disk encryption conforming to AES specifications and conform to the NIST Cryptographic Module Validation Program listing and ITP-SEC031. Data element encryption shall be used when Class "C" Classified Records or Closed Records data elements are stored in a database. Transparent Data Encryption (TDE) or other database specific methods can be utilized to meet this requirement. *For Criminal Justice Information, encryption must also meet CJIS policy requirements. * For systems receiving, processing or storing Federal Tax Information (FTI), must also meet IRS Publication 1075 requirements.
ITP-SEC032 - Enterprise Data Loss Prevention (DLP) Compliance Standards	The contractor shall implement a Data Loss Prevention (DLP) technology/solution.
ITP-SEC034 - Enterprise Firewall Rule Set	The contractor shall implement a perimeter firewall system. 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 the contractor permits mobile device access to its systems, it shall implement a Mobile Device Management (MDM) system to manage such access and protect those systems in the event of a lost or stolen mobile device.
ITP-SEC038 - COPA Data Center Privileged User Identification	The contractor shall implement a privileged user management solution for administrative level access to applications and systems containing Commonwealth data.

and Access Management Policy	
ITP-SEC039 – Keystone Login and Identity Proofing	All citizen facing applications are to use Keystone Login for Authentication services. The contractor shall describe its use of the Commonwealth's established identity proofing service.
ITP-SEC040 – IT Service Organization Management and Cloud Requirements	The contractor shall coordinate with respective agencies to complete the Cloud Services Requirements (CSR) as part of the Cloud Use Case Review Process. The contractor is responsible for submitting SOC reports on an annual basis or otherwise set forth in the applicable contract. If using a Subservice Organization, the contractor is responsible for obtaining and reviewing the Subservice Organization reports to ensure compliance with ITP-SEC040. In a timely manner, the contractor shall respond to any clarification requests, corrective action plan(s), and address, remediate, or mitigate identified concerns or nonconformities and recommendations.

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.