pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Security Policy Requirements for Third Party Vendors

ITP Number OPD-SEC000B	**Effective Date** January 19, 2021
Category Security	**Supersedes** None
Contact RA-ITCentral@pa.gov	**Scheduled Review** January 2022

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.

IT Policy	**Requirement**
ITP-SEC000 - Information Security Policy	Requires that data and personnel be in the United States of America. The contractor shall describe the location(s) of its server and data centers as well as the location of the workforce accessing them. System 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 Policy	1. The contractor shall describe its general approach to information security awareness training, and education. 2. The contractor shall describe its compliancy with federal and state guidelines and regulations regarding the collection, maintenance, use, and security of **IT Resources**, as defined in Management Directive 205.34. 3. The contractor shall describe its 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

	4. The contractor shall describe its procedures for responding to incidents, breaches, or misuse of **IT Resources**. 5. The contractor shall describe its processes for protecting Class "C" Classified Records or Closed Records during transmission, processing, and storage. The contractor shall describe its 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-SEC002 – Internet Accessible Proxy Servers and Services	The contractor shall describe its environment for: 1. Anti-Virus Protection on endpoints enforce mode; 2. Host Intrusion Prevention on endpoints enforce mode; 3. Incident/Forensic Response ability to do forensic analysis on endpoints; and 4. Advanced Persistent Threat Endpoint Protection - malware protection enforce mode.
ITP-SEC003 - Enterprise Security Auditing and Monitoring	The contractor shall describe its services for Internet access monitoring, content filtering, SSL decryption and inspection. All internet traffic originating from within the Commonwealth network will be directed through the Commonwealth's Internet Access Control and Content Filtering (IACCF) Proxy Filter.
ITP-SEC004 - Enterprise Web Application Firewall	The contractor shall describe its utilization of a web application firewall (WAF) specific to: 1. Minimizing the threat window for each exposure by blocking access to vulnerability until the vulnerability can be fixed in the source code; 2. Meeting PCI, HIPAA, and Privacy compliance requirements; 3. Monitoring end-user's transactions with a web application; and 4. Providing an additional layer of web application hardening Open Web Application Security Project (OWASP) protection.

	A web application firewall (WAF) shall be used to protect data classified under ITP-SEC019 as Class "C" and/or CJIS data, utilizing the standard set forth in ITP-SEC004.
ITP-SEC005 – Commonwealth Application Certification and Accreditation	All application code must be scanned 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. Applications are to undergo a (CA)2 reaccreditation process every 3 years.
ITP-SEC006 - Commonwealth of Pennsylvania Electronic Signature Policy	Allows the Commonwealth to accept electronic signatures. The contractor shall describe its capabilities for implementing electronic signatures for relevant applications.
ITP-SEC007 - Minimum Standards for IDs, Passwords and Multi-Factor Authentication	The contractor shall utilize the Commonwealth's enterprise directories and password policies and describe its compliance and implementation capabilities. Multi-factor authentication (MFA) shall be implemented 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 CJIS data MFA shall be implemented for users requiring direct access to data, application, or infrastructure, from any location not designated as a physically secure location as per FBI CJIS policy.
ITP-SEC008 - Enterprise E-mail Encryption	The contractor shall describe its process for: 1. Protecting and encrypting all outbound e-mails where the e-mail contents contain sensitive information; 2. Compliance with federal mandates requiring secure e-mail transmissions; 3. Ensuring that sensitive communications and exchange of information originating from the Commonwealth will not be compromised; and 4. Decrypting secure messages received by external Commonwealth e-mail recipients.
ITP-SEC009 - Minimum Contractor Background Checks Policy	Due to the potential access to "C" or closed records all resources engaged in the delivery of services on the Contract must complete background checks. The contractor shall describe its process for ensuring staff and subcontractor compliance with the following requirements. 1. The Offeror shall arrange for a background check for each of its staff and subcontractors who will have access to Commonwealth Data or Commonwealth IT facilities, either through on site or remote access. Background checks must be conducted via form **SP 4-164 Request for Criminal Record**

	Check. The background check must be conducted prior to initial site access by a contracted resource and annually thereafter. 2. The background check must be checked for the previous five (5) years for: (1) Crimes against property; (2) Crimes involving theft; (3) Crimes involving telecommunications and electronics; (4) Crimes involving fraud; (5) Crimes against public administration; or (6) Crimes of violence. 3. A fingerprint database search will be required for contractor 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 contractor resources and/or subcontracted resources.
ITP-SEC010- Virtual Private Network Standards	The contractor shall describe its capabilities to provide Virtual Private Network (VPN) access to its networks and connected systems. A VPN connection will be required for any access to the Commonwealth network from external sources.
ITP-SEC011 - Enterprise Policy and Software Standards for Agency Firewalls	The contractor shall maintain perimeter defense and describe its firewall implementation.
ITP-SEC012 – Commonwealth of PA System Logon Banner and Screensaver Requirements	All computing devices hosting Commonwealth data shall utilize logon banners before access to the system is granted, notifying them that the system is for official use of authorized users only, and all activity is monitored.
ITP-SEC015 - Data Cleansing Policy	The contractor shall describe its processes for 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. Decommissioned electronic media must be degaussed, wiped, or destroyed in accordance with ITP-SEC015.
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 describe its processes for accepting credit card payments and its adherence to PCI requirements (if applicable as per the contract).
ITP-SEC019 - Policy and Procedures for Protecting Commonwealth Electronic Data	The contractor shall describe its processes for classifying sensitive data and protecting confidential or other sensitive data entrusted to its care. A data element inventory will 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" and/or CJIS data, utilizing the standard set forth in ITP-SEC004. Encrypt all sensitive data at rest to include, but not limited to; protected, exempt, or "C" Class data, using encryption standards set forth in the ITPs 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 describe its processes for logging 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 shall describe its processes for both internal and external security scans and shall provide the results of such to the Commonwealth upon request. Contractor must perform yearly security assessments, remediate pertinent vulnerabilities monthly, conduct internal audits, and perform IT security tests to Commonwealth standards.
ITP-SEC024 - IT Security Incident Reporting Policy	The contractor shall describe its processes to ensure compliance with The Pennsylvania Data Breach Notification Act.

	Contractor shall follow an 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)	A data element inventory will be performed, 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 other protected data types (CJIS, FTI, HIPAA) for any purpose, shall ensure that access or use of such information is properly controlled, encrypted, and restricted to prevent unauthorized use or disclosure. *For Social Security Administration (SSA) Compliance. the system's encryption methods must align with the Guidelines established by the National Institute of Standards and Technology (NIST). SSA recommends the Advanced Encryption Standard (AES) or Triple DES (Data Encryption Standard 3). All contractors will 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 which 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.
ITP-SEC029 - Physical Security Policy for IT Resources	The contractor shall describe its policies and practices to ensure the protection of physical facilities and appropriate screening for facility access. 1. 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. Contractor employees 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 employees. 2. Some Commonwealth sites, i.e., 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 personnel and subcontractors 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 personnel and subcontractors may be searched by Commonwealth staff, or a correctional or police officer. 3. Access to restricted IT facilities and resources is limited only to authorized persons. All IT facilities and resources hosting or accessing Commonwealth data are responsible for designating a certified party to review access records and visitor logs in accordance with ITP-SEC029 and any applicable legislation. Facilities hosting Commonwealth data are to maintain and archive access records and sign-in logs for a period of not less than one year. All IT facilities and resources hosting or accessing Commonwealth data are to be physically protected in proportion to the data or application's criticality or functional importance.
ITP-SEC031 - Encryption Standards	The contractor shall describe its processes for protection of confidential or other sensitive Commonwealth data that is stored within contractor's systems. File encryption is to be used when files containing sensitive, protected, privileged or prerequisite required data are transferred on physical media, through email, or across networks, without other forms of encryption or protection. Full disk encryption is to be used for archiving or backing up sensitive, protected, privileged or prerequisite required data to tape or optical media. Software or hardware mechanisms can be used provided they conform to AES specifications.

	Non-Windows environments requiring full disk encryption are to utilize Full disk encryption conforming to AES specifications and conform to the NIST Cryptographic Module Validation Program listing http://csrc.nist.gov/groups/STM/cmvp/. The contactor shall describe its processes for encrypting data at rest in accordance with established standards for protecting confidential or other sensitive data while stored in its systems. Data element encryption is to be used when sensitive, protected, privileged or prerequisite required data elements are stored in a database. Transparent Data Encryption (TDE) can be utilized to meet this requirement. Encrypt all sensitive data at rest to include, but not limited to; protected, exempt, or "C" Class data, using encryption standards set forth in the ITPs 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-SEC032 - Enterprise Data Loss Prevention (DLP) Compliance Standards	The contractor shall describe its processes for Data Loss Prevention (DLP) and related services. An industry standard DLP technology shall be deployed per Commonwealth standards set forth in ITP-SEC032.
ITP-SEC034 - Enterprise Firewall Rule Set	The contractor shall describe its 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 describe its procedures to grant such access and protect those systems in the event of a lost or stolen mobile device.
ITP-SEC038 - COPA Data Center Privileged User Identification and Access Management Policy	Default application and/or hardware passwords shall be changed and managed to meet the Commonwealth Standards set forth in ITP-SEC007.
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.

3. Related ITPs/Other References

Definitions of associated terms of this policy are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/Glossary.aspx

Commonwealth policies, including Executive Orders, Management Directives, and IT Policies are published on the Office of Administration's public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx

- Management Directive 205.34 *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- ITP-SEC000 - *Information Security Policy*
- ITP-SEC001 - *Enterprise Host Security Software Policy*
- ITP-SEC002 – *Internet Accessible Proxy Servers and Services*
- ITP-SEC003 - *Enterprise Security Auditing and Monitoring*
- ITP-SEC004 - *Enterprise Web Application Firewall*
- ITP-SEC005 – *Commonwealth Application Certification and Accreditation*
- ITP-SEC006 - *Commonwealth of Pennsylvania Electronic Signature Policy*
- ITP-SEC007 - *Minimum Standards for IDs, Passwords and Multi-Factor Authentication*
- ITP-SEC008 – *Enterprise Email Encryption*
- ITP-SEC009 - *Minimum Contractor Background Checks Policy*
- ITP-SEC010 - *Virtual Private Network Standards*
- ITP-SEC011 - *Enterprise Policy and Software Standards for Agency Firewalls*
- ITP-SEC012 – *Commonwealth of PA System Logon Banner and Screensaver Requirements*
- ITP-SEC015 - *Data Cleansing Policy*
- ITP-SEC016 - *Commonwealth of Pennsylvania - Information Security Officer Policy*
- ITP-SEC017 - *CoPA Policy for Credit Card Use for e-Government*
- ITP-SEC019 - *Policy and Procedures for Protecting Commonwealth Electronic Data*
- ITP-SEC021 - *Security Information and Event Management Policy*
- ITP-SEC023 - *Information Technology Security Assessment and Testing Policy*
- ITP-SEC024 - *IT Security Incident Reporting Policy*
- ITP-SEC025 – *Proper Use and Disclosure of Personally Identifiable Information (PII)*
- ITP-SEC029 - *Physical Security Policy for IT Resources*
- ITP-SEC031 - *Encryption Standards*

- ITP-SEC032 - *Enterprise Data Loss Prevention (DLP) Compliance Standards*
- ITP-SEC034 - *Enterprise Firewall Rule Set*
- ITP-SEC035 - *Mobile Device Security Policy*
- ITP-SEC038 - *COPA Data Center Privileged User Identification and Access Management Policy*
- ITP-SEC039 – *Keystone Login and Identity Proofing*

4. Authority

Executive Order 2016-06, Enterprise Information Technology Governance

5. Publication Version Control

It is the Authorized User's responsibility to ensure they have the latest version of this publication, which appears on https://itcentral.pa.gov for Commonwealth personnel and on the Office of Administration public portal: http://www.oa.pa.gov/Policies/Pages/default.aspx. Questions regarding this publication are to be directed to RA-ITCentral@pa.gov.

6. Exemption from This Policy

In the event an agency chooses to seek an exemption, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the enterprise IT Policy Waiver process. Refer to ITP-BUS004 *IT Waiver Review Process* for guidance.

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

Version	Date	Purpose of Revision
Original	01/19/2021	Base Document
Revision	2/10/2021	ITP-SEC001 Updated and Published 2/9/2021