pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

Computing Services Provided by Service Organizations

Number
ITP-SEC040

Effective Date
July 18, 2018

Category
Security

Supersedes
ITP-BUS011

Contact
RA-ITCentral@pa.gov

Scheduled Review
July 2024

1. Purpose

This Information Technology Policy (ITP) establishes guidance on the management of Service Organizations and establishes requirements for the procurement and use of any non-Commonwealth Hosted Application and/or Service (Computing Service).

2. Scope

This ITP applies to all departments, offices, 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 (Service Organizations, which include its Subservice Organizations) shall meet the policy requirements of this ITP as outlined in the Responsibilities section.

3. Definitions

Computing Service: Any service that is hosted by or within a Service Organizations or its subcontractor(s) (Subservice Organization(s)) managed infrastructure regardless of deployment model (public, private, or hybrid) or type such as, but not limited to, software-as-a-service (SaaS) for web-based applications, infrastructure-as-a-service (IaaS) for Internet-based access to storage and computing power, and platform-as-a-service (PaaS) that gives developers the tools to build and host web applications. Solutions deployed through traditional hosting methods and without the use of NIST Cloud capabilities (i.e., rapid elasticity, resource pooling, measured service, broad network access, and on demand self-service) are also included.

Computing Services Use Case Review (Use Case Review): An established process to ensure the procurement and use of any Computing Services is aligned with the Commonwealth's overall business and IT vision, strategy, goals, and

policies. This process includes representation and review from all domains to pro-actively identify, manage, and mitigate risk, if any, with the Computing Services being considered. As part of Use Case Review, the Service Organization is required to complete the Computing Services Requirements (CSR) document that is specific to the Computing Services being considered. Any procurement or use of a Computing Services requires prior approval from the Enterprise Architecture Review Committee (EARC).

IT Resources: Include, but are not limited to, the staff, software, hardware, systems, services, tools, plans, data, and related training materials and documentation that, in combination, support business activities. Examples of IT Resources include, but are not limited to, Commonwealth resources such as Commonwealth technology standardized services (e.g., ITSM, ERP, IAM), endpoints (e.g., desktop computers, mobile devices), email, telephones, network and security components (e.g., switches, routers), and servers..

4. Objectives

- Ensure prudent selection of business and technology solutions and services during the procurement process.
- Review and validate business and technology solutions and services align with enterprise and agency business requirements and policies.
- Establish guidance and framework for conducting business and IT risk assessments.
- Ensure agency business owners are notified, understand, and acknowledge the risks associated with procuring and implementing business and technology solutions and services.
- Increase awareness of the cybersecurity threats and their potential impacts to business operations.
- Confirm cybersecurity practices are compliant with ITPs, regulations, statutes, and industry standards.
- Ensure and actively monitor the Service Organizations through System and Organization Controls (SOC) Reporting to ensure effective controls are in place to protect Commonwealth IT Resources.

5. Policy

All Computing Services must meet the requirements outlined in this policy.

Prior to the procurement or use of any Computing Services, a Use Case Review shall be conducted by the Computing Services Review Committee (CSRC) and agencies may only proceed if approved by the EARC.

This includes, but is not limited to, the following:

- Any new Computing Services regardless if they are already covered by an existing contract.
- Any new Computing Services that an agency would like to test or view via a Pilot or Proof of Concept. This would need to be approved by the Department of General Services (DGS) in accordance with the DGS, Bureau of Procurement Policy Directive 2021-1, New Technology Pilot Program and Product Demonstrations.
- Original scope of an approved use case has significantly changed. Significant

changes may include, but are not limited to, the following:

- Change of hosting location and/or hosting provider.
- Change of data classification type (data collected/stored).
- Change in class of user type or population (not previously disclosed).
- New integration requirements with Commonwealth resources or between Computing Services.
- New bandwidth requirements or material change in bandwidth requirements used between the Commonwealth network and Computing Services.

Agencies shall perform an internal assessment of the Computing Services requirements (TABLE 1 below) to determine if the requirements will be met prior to submitting a use case for review. The internal assessments should include a comparison of the Computing Services requirements and the solution capabilities to ensure the applicable Computing Services requirements are met prior to the selection of a solution and Use Case Review submission to avoid its non-compliance and rejection.

An approved use case is a prerequisite prior to obtaining approval for any non-compliant IT Policy Waiver. If business requirements demand a "non-compliant" business solution and/or Computing Service, an IT Policy Waiver against this policy must be submitted by the designated IT Policy Waiver Submitter through the enterprise IT Policy Waiver Process (refer to *ITP-BUS004, IT Policy Waiver Process*). The submission for the IT Policy Waiver, if required per RFD-BUS004B or upon request within the IT Policy Waiver Process, must include a completed and signed Risk Assessment and Acknowledgement document (*OPD-SEC040A, Risk Assessment and Acknowledgement*) and must set forth the business requirements that demand a "non-compliant" business solution or Computing Service.

Agencies shall revaluate *OPD-SEC040A, Risk Assessment and Acknowledgement* on an annual basis and resubmit an IT Policy Waiver Renewal based on the changing threat landscape that identify emerging cyberthreats affecting particular product(s), service(s), industry sector(s), user groups, or a specific attack or vector that is most vulnerable at the moment.

Adherence to the Computing Service requirements, as set forth in TABLE 1 below, and submission of all required documentation does not guarantee approval of the use case request.

5.1 TABLE 1. Computing Service Requirements:

5.1.1 Legal/Procurement

Risk ID	Category	Requirement
CSR-L1	**Procurement Requirement**	• Agencies shall procure, or plan to procure, the Computing Service through an existing approved Contract or other Commonwealth approved procurement method.

Risk ID	Category	Requirement
CSR-L2	**Legal Review**	• Agencies shall conduct legal review to discern appropriateness of terms in existing or planned Contracts and to advise agencies of other legal requirements.
CSR-L3	**CONUS Access Control**	Agencies and Service Organizations shall provide access only to those staff, located within CONUS, that must have access to provided systems and services and Commonwealth data.
CSR-L4	**CONUS Hosting**	• Agencies and Service Organizations shall only host, handle, or process data in physical locations within CONUS.
CSR-L5	**System and Organization Controls (SOC) Reporting**	• Service Organizations shall submit appropriate Systems and Organizations Controls (SOC) report(s) and any required attestation letter for Subservices Organizations. Refer to section 5.1 System and Organization Controls (SOC) Reporting Requirements of this ITP and to *OPD-SEC040B, System and Organization Controls (SOC) Reporting Procedure*. • Solicitations for the procurement of Computing Services shall include a requirement that Offerors submit a SOC 1 Type 2 report, if hosting, handling, or processing financial information, and SOC 2 Type 2 report, if hosting, handling, or processing Class "C" Classified Records or Closed Records as part of the response to the solicitation.

5.1.2 Accessibility

Risk ID	Category	Requirement
CSR-A1	**Accessibility Standards**	Service Organizations shall comply with the Accessibility Standards in *ITP-ACC001, Digital Accessibility Policy,* Section 6. Service Organizations shall submit a completed Accessibility Conformance Report (ACR) using the most current version of the Voluntary Product Accessibility Template (VPAT) for the proposed Computing Service. • The VPAT template should be filled out in its entirety and include testing methodology, conformance level, and remarks for any partially supported or non-supported level. • If ACR(s) are submitted, using an older version of the VPAT, Service Organizations should provide an explanation, as to why the most current version is not being used. • If ACR is not submitted or if ACR score is determined to be low, Service Organizations shall complete the Policy Driven Adoption for Accessibility (PDAA) Assessment for review by the Accessibility Center of Excellence.

5.1.3 Information

Risk ID	Category	Requirement
CSR-IN1	**System Design Review of Electronic Information Systems Questionnaire**	• Agencies and Service Organizations shall comply with the requirements as outlined *in* *ITP-INFRM005, System Design Review of Electronic Systems*. • Agencies shall submit a completed *OPD-INFRM005A, System Design Review of Electronic Information Systems* for the proposed system or Computing Service.

5.1.4 Security

Risk ID	Category	Requirement

CSR-S1	**System Monitoring / Audit logging (Security)**	• Service Organizations shall ensure system monitoring and audit logging must be enabled and accessible to the Delivery Center/Agency Information Security Officer or designee. (Refer to Section 5.3 for additional guidance)
		  • It is recommended that verbose logging is enabled in order to provide detailed event information.
		  • Ability to correlate events and creates security alerts.
		  • Maintain reports online for a minimum of 90 days and archive for a minimum of 1 year. If the agency requires longer retention periods, the agency's longer retention requirement takes precedence.
		  • Reports should be easily accessible and in a readable format.

CSR-S2	**Boundary Protection / Network Protection**	• Service Organizations shall provide a network/architecture diagram showing what technical controls are performing the network segmentation within the proposed service.
		
		  • If solution spans more than one hosting environment (such as integration to Commonwealth managed environments, or across multiple hosting providers), Service Organizations shall provide details on what solution components and data are deployed in which environment.
		
		  • Diagram shall include border gateway, perimeter and/or network firewall, web application firewall, VPN tunnels, and security zone access as applicable to the solution.
		
		  • Diagram shall include the direction of connectivity (specify whether initiated inbound, outbound, or both) and specifications for API calls, protocols, etc.
		
		• Service Organizations shall implement technical and

Risk ID	Category	Requirement
		administrative controls that are utilized to ensure separation between the Commonwealth and other customers. • Service Organizations shall maintain the diagram throughout the Contract term and provide updates as changes occur.

CSR-S3	**Exploit and Malware Protection**	• Service Organizations shall provide and manage security controls. These are required to identify attacks, identify changes to files, protect against malware, protect user web services, data loss prevention (DLP), and provide for forensic analysis.
		  • File Monitoring Controls
		  • Antivirus Controls
		  • Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) Controls
		  • Data Loss Prevention (DLP) Controls
		  • Forensic Controls
		  • Advanced Persistent Threat (APT) Controls

CSR-S4	**Encryption**	Agencies and Service Organizations shall follow established standards to protect data in transit and data at rest per *ITP-SEC031, Encryption Standards* and *ITP-SEC019, Policy and Procedures for Protecting Commonwealth Electronic Data*.
CSR-S5	**Identity & Access Management**	• Agencies and Service Organizations shall comply with *ITP-SEC007, Minimum Standards for IDs, Passwords, Sessions, and Multi-Factor Authentication* and *ITP-SEC039, Keystone Login and Identity Proofing*. • Agencies and Service Organizations shall use Commonwealth Identity and Access Management (IAM) services, and where applicable Multi-Factor Authentication (MFA) to authenticate users that require access to the proposed service. • Service Organizations shall provide technical controls for interfacing with Commonwealth authentication services. • Service Organizations internal administration and operation of services being provided to the Commonwealth may use Service Organization internal IAM, with configuration aligned with Commonwealth configuration requirements, such as but not limited to use of MFA.
CSR-S6	**Vulnerability Assessment**	• Service Organizations shall ensure all Computing Solution components are securely coded, vetted, and scanned. • Service Organizations shall obtain an independent third-party vulnerability assessment within the first six (6) months of Contract execution and such assessment shall be completed annually thereafter. • Service Organizations shall obtain an independent third-party vulnerability assessment more frequently as required to comply with regulations.

Risk ID	Category	Requirement
		• Service Organizations shall obtain an independent third-party vulnerability assessment upon request by the Commonwealth due to other warranted circumstances such as, but not limited to, a cyber security incident or a major change to the solution. • Service Organizations shall provide, at minimum, an executive summary of any independent third-party vulnerability assessment results to the Commonwealth. Summary shall include, at minimum, scan date, identified vulnerabilities, severity classification, remediation plan, and remediation status.

CSR-S7	**Service Availability / Recovery**	• Service Organizations shall maintain a business continuity plan that addresses the following:
		  ◦ Data/Database Recovery
		  ◦ Application Recovery
		  ◦ Operating System Recovery
		  ◦ Infrastructure Recovery
		• Service Organizations shall perform a complete restoration in the event of a disaster within the timeframe as specified by Contract requirements.
		• Service Organizations shall ensure tests are performed as part of its disaster recovery plan in accordance with Contract requirements.
		• Service Organizations shall provide services during a pandemic event as required by the Contract.

CSR-S8	**Compliance**	• Agencies shall ensure Service Organizations are informed of type of data (per *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*) and applicable laws or regulations that are intended to be used with their solution prior to Service Organizations completion of CSR document.
		• Agencies and Service Organizations shall meet all applicable compliance requirements based upon the most restrictive data classification, per ITP-INF015, and any applicable laws or regulations such as, but not limited to, the following:
		  ◦ Criminal Justice Information Services (CJIS) and Criminal History Record Information Act (CHRIA) for criminal history data
		  ◦ Health Insurance Portability and Accountability Act (HIPAA) for health-related data
		  ◦ Internal Revenue Service (IRS) Publication 1075 and Social Security Administration (SSA) for federal protected data
		  ◦ Payment Card Industry (PCI)- Data Security Standards (DSS) for financial data

Risk ID	Category	Requirement
CSR-S9	**Security Incident Handling**	• Agencies and Service Organizations shall ensure compliance with *ITP-SEC024 IT Security Incident Reporting Policy*. Agencies and Service Organizations shall ensure the incident management processes, including escalation procedures, and the responsibilities of each party are documented. • Agencies and Service Organizations shall 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 Breach of Personal Information Notification Act, Act of November 3, 2022, P.L. 2139, No. 151, 73 P.S. §§ 2301-2330. • Service Organizations shall ensure all suspected cyber security incidents are reported 24/7/365 to the Enterprise Information Security Office (EISO) via PA-CSIRT Incident Response Hotline at 1-877-55CSIRT (1-877-552-7478).
CSR-S10	**Asset Inventory Management and Maintenance**	• Service Organizations shall ensure a complete, accurate, and up-to-date inventory of resources utilized within the delivery of services to the Commonwealth and shall be made available for review upon request. • Service Organizations shall not utilize resources that are prohibited pursuant to federal laws and regulations or state laws, regulations, and procurement policy. • Service Organizations shall ensure supply chain risk is appropriately managed to limit service availability impacts. • Service Organizations shall ensure patching is up to date and performed no less than on a monthly basis. • Service Organizations shall provide notice to the Commonwealth for any changes to the inventory of resources used in the delivery of services being provided to the Commonwealth that would negatively impact regulatory compliance.
CSR – S11	**Patching**	• Agencies and Service Organizations shall comply with requirements as outlined in *ITP-SEC041, Commonwealth IT Resources Patching Policy*, Section 5. • Service Organizations shall completely test and apply patches for all products prior to service release. • Service Organizations shall use industry best practices to update and patch all applicable systems and third-party software security configurations to reduce security risk.

5.1.5 Infrastructure

Risk ID	Category	Requirement
CSR-I1	**Connectivity**	• Agencies and Service Organizations shall utilize an approved Commonwealth perimeter network/security solution managed by enterprise operations for inspection of all traffic between the Commonwealth's enterprise network including any datacenters, Commonwealth managed cloud computing environments, end user networks, VPN remote connected devices, etc. and the Service Organization's services.
CSR-I2	**Interface Requirements**	• Agencies and Service Organizations shall conform to the Commonwealth's Network Interoperability Standards (See References section for details).

CSR-I3	**System Monitoring / Audit logging (Infrastructure)**	• Agencies and Service Organizations shall ensure real-time application and performance monitoring are enabled. Monitoring must include system and network impact.
		• Stakeholders must have access as required.
		  • It is recommended that verbose logging is enabled in order to provide detailed event information.Ability to correlate events and create operational alerts.
		  • Generate reports for a minimum of 90 days, archive for 1 year.
		  • Reports should be easily accessible and in a readable format.

CSR-I4	**Capacity**	• Agencies and Service Organizations shall maintain capacity estimates for all applications. These estimates shall include estimates of compute, storage, and network utilization.
		  • Estimates shall also include a rough order of magnitude for any expected deviation (growth or reduction) over the next 3 years for future planning.
		  • Network utilization estimates shall note any peak periods that may occur such as daily, weekly, monthly, seasonal, and yearly trends.
		  • Network utilization shall detail all interactions including but not limited to:
		  • User access
		  • Residents and/or general public
		  • Business Partner/Vendors
		  • Commonwealth Users
		  • System communication (ex: API calls) between major components in different locations/environments
		  • Backup and/or Synchronization traffic between different locations/environments.
		• Estimates shall be made available to the Commonwealth upon request and shall be attached as supplemental data for CSRC review, IT Policy Waiver, and similar submissions.

5.2 System and Organization Controls (SOC) Reporting Requirements

5.2.1 SOC Reporting Requirements

Agencies and Service Organizations shall follow SOC report procedures as detailed in *OPD-SEC040B, System & Organization Controls (SOC) Reporting Procedure*. If the Service Organization is using a Subservice Organization to provide any services, it is the Service Organization's responsibility to obtain and review SOC reports (or an alternative report to the extent permitted by the Commonwealth) from their Subservice Organization to ensure compliance with Commonwealth requirements.

Service Organizations shall provide an attestation letter, signed by an authorized IT security professional, with their SOC report (or an alternative report to the extent permitted by the Commonwealth), asserting they received and reviewed the Subservice Organization's SOC reports and verified the Subservice Organization has the proper IT controls in place to ensure compliance with Commonwealth requirements.

If any non-compliance is identified (i.e., control deficiencies, material weaknesses, cybersecurity incidents, etc.), the Service Organization shall provide a corrective action plan(s) with respect to the Service Organization or any Subservice Organizations.

The following guidance shall be used by agencies when determining when to request a SOC report and what type of SOC report should be requested from a Service Organization. It may be appropriate for the Commonwealth to request more than one type of report if circumstances make requiring multiple reports necessary.

5.2.1.1 SOC 1 Type 2 Report

A SOC 1 Type 2 Report is required if any of the following conditions exist:

- As a part of the technical proposal relating to an RFP or RFQ that includes Computing Services that would require a SOC 1 Type 2 report;
- The Service Organization is processing or hosting financial information that could affect or have a material impact on a Commonwealth agency's financial statements or reporting;
- Compliance mandate for federal or state audit requirements or policy; or
- A third-party provides financial service(s) (such as, but not limited to, payroll processing, accounts receivable, payable, or collection service).

Note: SOC 1 Type 2 reports will provide findings for Finance/Accounting controls and IT controls for services with integrated systems associated with financial transactions and reporting

5.2.1.2 SOC 2 Type 2 Report

A SOC 2 Type 2 Report is required if any of the following conditions exist:

- As a part of the technical proposal relating to an RFP or RFQ that includes Computing Services that would require a SOC 2 Type 2 report;

- The Service Organization is hosting, handling, or processing Class "C" Classified Records or Closed Records as defined in ITP-INF015 *Policy & Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*; or
- Compliance mandated with federal or state audit requirements or policy.

5.2.1.3 SOC for Cybersecurity Report

A SOC for Cybersecurity Report is required if any of the following conditions exist:

- Reoccurring findings in SOC 1-Type 2 or SOC 2-Type 2 reports;
- A cybersecurity incident or breach that impacts the Commonwealth has occurred and was not handled in accordance with the Service Organizations Incident Response Plan (IRP) including, but not limited to, providing timely notice to the Commonwealth as required by Contract or applicable law; or
- As agreed upon by the parties.

5.2.1.4 SOC Report Order of Precedence for IT Procurements

If a SOC 1 Type 2 report is not available, the Commonwealth, at its discretion and in writing, may accept a SOC 1 Type 1 report for low risk, immaterial financial systems as a temporary alternative until a SOC 1 Type 2 is available.

If a SOC 2 Type 2 report is not available to be submitted as part of a Technical Proposal, the Commonwealth, at its discretion and in writing, would accept one of the following (in the following order of precedence) as part of the Technical Proposal in response to a RFP or RFQ that includes Computing Service or as determined during a Commonwealth review or evaluation of a Computing Service that would require a SOC 2 Type 2 report.

i. SOC 2 Type 1
ii. Current ISO 27001 Certification
iii. Current FedRAMP Authorization
iv. Alternative Security Report

5.2.1.5 SOC 1 and 2 Report Required Data

At a minimum, the following information must be contained within any SOC 1 and SOC 2 report that is provided in compliance with this ITP:

- Cover letter indicating whether the Service Organization and all Subservice Organizations are or are not performing services in accordance with the contract. The cover letter must summarize the results of the audit and the audit tests performed. The letter must highlight unusual items, deficiencies, qualifications, and any inconsistencies with professional standards and provide an indication of actions being taken to address, remedy or mitigate these or other weaknesses noted in the applicable report;
- Independent Auditor's Summary Report including their opinion as to whether the Service Organization and all Subservice Organizations are or are not performing services in accordance with the contract and Service Auditor's Responsibilities;

- Service Organization's Management Assertion;
- Service Organization's Management attestation asserting that all Subservice Organizations are demonstrating the proper IT controls are in place to protect and secure Commonwealth resources;
- Overview of Service Organization (i.e., company overview, services provided to the Commonwealth, related information systems);
- Scope of SOC report and description of all control objectives and related description of controls examined, descriptions of tests for operational effectiveness, and test results;
- Service Organization Management responses to deviations when performing the tests of operating effectiveness of controls;
- Detailed description of all findings, exceptions and opinions rendered (i.e., qualified, disclaimer, adverse, unqualified) during the SOC reporting period; and
- Service Organization shall provide a corrective action plan(s) if any non-compliance is identified, with respect to the Service Organization or any Subservice Organizations.

5.2.1.6 SOC for Cybersecurity Report Required Data

At a minimum, the following information must be contained within any Cybersecurity report that is provided in compliance with this ITP:

- Independent Auditor's Opinion letter (either point in time or period of time);
- Management's Assertion (description criteria and control criteria) regarding the description and effectiveness of the program's controls; and
- Management's Description of the cybersecurity risk management program.

5.2.1.7 SOC Reporting Contract Language:

SOC Reporting requirements shall be inserted in new or amended Service Organization agreements that support business and IT operations. Service Organization agreements shall require the Service Organization use an independent CPA-certified auditor to review andmonitor Service Organization's controls for all types of SOC reports.

5.2.2 SOC Report Review/Evaluation Requirements

The SOC report, in accordance with the type of SOC report, that is provided to the Service Organization by an independent CPA-certified auditor shall provide the Service Organization's customers assurance on the Internal Controls over financial reporting and IT controls relevant to security, availability, processing integrity, confidentiality, privacy, and/or specific frameworks and procedures relevant to an entity's cybersecurity risk management program.

5.3 System Monitoring / Audit Logging (Security) Guidance

Agencies are responsible for configuring auditing at the application, database, and virtual machine level as necessary to capture the following events:

<u>Operating System (OS) Events</u>

- start up and shut down of the system;

- start up and shut down of a service;
- network connection changes or failures; and
- changes to, or attempts to change, system security settings and controls.

OS Audit Records

- log on attempts (successful or unsuccessful);
- the function(s) performed after logged on (e.g., reading or updating critical file, software installation);
- account changes (e.g., account creation and deletion, account privilege assignment); and
- successful/failed use of privileged accounts.

Application Account Information

- successful and failed application authentication attempts;
- application account changes (e.g., account creation and deletion, account privilege assignment); and
- use of application privileges.

Application Operations

- application startup and shutdown;
- application failures;
- major application configuration changes; and
- application transactions, such as:
    - e-mail servers recording the sender, recipients, subject name, and attachment names for each e-mail;
    - web servers recording each URL requested and the type of response provided by the server; and
    - business applications recording which financial records were accessed by each user.

The details logged for each event may vary widely, but at minimum, each event should capture:

- timestamp
- event, status, and/or error codes
- service/command/application name
- user or system account associated with an event
- object access
- policy change
- privilege functions
- process functions
- process tracking
- system events
- all administrator activity
- authentication checks
- authorization checks
- data deletions
- data access
- data changes
- permission changes
- network event information (at minimum source and destination IPs, port(s), terminal session ID, web browser)

6. Responsibilities

6.1 Agencies shall:

- Submit a new Use Case Review for any Computing Service that meets the requirements outlined in Section 5, Policy.

- Only procure and utilize Computing Services that are approved through the Use Case Review process.

- Require Service Organizations to complete the CSR as part of the Use Case Review process.

- Ensure that external Service Organization and Subservice Organization SOC reporting requirements are detailed in contracts with those Service Organizations. Agencies are to develop and maintain internal SOC reporting procedures that comply with the guidance set forth in this ITP and OPDs. SOC reports shall be maintained and accessible upon request from authorized Commonwealth personnel.

- Be responsible for developing and managing internal policy for Computing Services that adhere to all Management Directives and ITPs.

- Reevaluate *OPD-SEC040A, Risk Assessment and Acknowledgement* on an annual basis and resubmit as part of the IT Policy Waiver renewal process based on the changing threat landscape that identify emerging cyberthreats affecting particular product(s), service(s), industry sector(s), user groups, or a specific attack or vector that is most vulnerable at the moment.

- Maintain appropriate IT Governance and access control measures for administrators needing access to Computing Services provided by Service Organizations.

6.2 Office of Administration, Office for Information Technology shall:

- Manage the service request process for all Compute Services and be responsible for working with agencies in developing the appropriate business and technology architecture requirements to provide the appropriate Computing Service.

- Conduct audits of approved use cases as needed and may submit requests for information (RFI) that support the agency's use case prior and after approval. This action is necessary to ensure compliance and aligns with the expectations of the use case.

6.3 Service Organizations shall:

- Comply with the requirements as outlined in this ITP by coordinating with respective agencies to complete the 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.

- In a timely manner, respond to any clarification requests, corrective action plan(s), and address, remediate, or mitigate identified concerns or nonconformities and recommendations.
- If using a Subservice Organization, be responsible for obtaining and reviewing all Subservice Organization reports to ensure compliance with Commonwealth requirements.
- Submit ACRs as applicable to the services being provided.
- Submit any other relevant artifacts the Service Organization deems beneficial to complete CSRC Review.

7. 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 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- *Management Directive 325.13, Service Organization Controls*
- *OPD-SEC040A, Risk Assessment and Acknowledgement*
- *OPD-SEC040B, System and Organization Controls (SOC) Reporting Procedure*
- *OPD-SEC040C, System and Organization Controls (SOC) Correspondence Procedure*
- *GEN-SEC040D, Alternative Security Reporting Requirements*
- *OPD-SEC040E, Alternative Security Report*
- Compute Services Requirements (CSR) and Requirements for non-Commonwealth Hosted Applications/Services: *https://collab.pa.gov/dgs/home/BOP/Pages/ITProcurement.aspx* (*Limited Access*)
- *Department of General Services, Bureau of Procurement Pilot-Demo Policy Directive 2021-01*
- Commonwealth's Network Interoperability Standards (Contact RA-ITCentral@pa.gov for information; *CWOPA authorized personnel only*)
- *RFD-BUS004B, IT Policy Waiver References Document*
- *ITP-SEC000, Information Security Policy*
- *ITP-SEC003, Enterprise Security Auditing and Monitoring*

- *ITP-SEC005, Commonwealth Application Certification and Accreditation*
- *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-SEC031, Encryption Standards*
- *ITP-SEC034, Enterprise Firewall Rule Set*
- *ITP-SEC038, COPA Data Center Privileged User Identification and Access Management Policy*
- *ITP-INF015, Policy and Procedures for Identifying, Classifying, and Categorizing Commonwealth Electronic Data*
- *ITP-SFT000, Software Development Life Cycle (SDLC) PolicyITP-SFT005, Managed File Transfer (MFT)NIST SP 800-92, Guide to Computer Security Log Management*
- *NIST SP 800-144, Guideline on Security and Privacy in Public Cloud Computing*
- *NIST SP 800-145, NIST Definition of Cloud Computing and Deployment Models*
- *NIST SP 800-146, NIST Cloud Computing Synopsis and Recommendations*
- *NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.*

8. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

9. 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 shall be directed to RA-ITCentral@pa.gov.

10. Exemption from this Policy

In the event an agency chooses to seek an exemption from the guidance within this ITP, a request for a policy waiver shall be submitted via the enterprise IT Policy Waiver Process. Refer to ITP-BUS004 *IT Policy Waiver Review Process* for guidance.

This chart contains a history of this publication's revisions. Redline documents detail the revisions and are available to CWOPA users only.

Version	Date	Purpose of Revision	Redline Link
Original	07/18/2018	Base Document	N/A
Revision	01/27/2020	• Clarified policy language throughout	N/A

Version	Date	Purpose of Revision	Redline Link
		• Added SOC guidance and OPD-BUS011B, OPD-BUS011C • Updated Cloud Service Requirements table and added "Responsible Party" column • Updated References section	
Revision	12/1/2020	• Updated definition section and added hyperlinks to OA Glossary • Updated 4.1.1.2 to address all categories that are Class "C" as defined by SEC019.	N/A
Revision	11/10/2021	• Changed ITP Number from BUS011 to SEC040 • Changed Policy Category from Business to Security • Added Third-party vendors to Scope and Responsibilities sections • Added OPD-SEC040D and OPD-SEC040E • Added Subservice Organization to definition section • Removed definitions that can be found in the OA Glossary • Updated 4.1 and all subsequent sections to include Subservice Organization Added links	N/A
Revision	01/06/2022	• Removed reference to COPPAR from policy • Added language that the Service Organization is required to obtain and review Subservice Organization's SOC reports • Service Organizations are required to attest that their Subservice Organizations comply with Commonwealth requirements • Corrective action plans shall be provided by the Service Organization for themselves and any Subservice Organizations in the event of non-compliance	N/A
Revision	07/18/2023	Updated title, purpose, scope, definitions, and objectives sections Updated references Changed "cloud computing service" to "computing service" Changed "Cloud Services Review Committee" to "Computing Services Review Committee (CSRC)." Table 1 – Split into multiple tables with section headings added. Updated CSR-L3, CSR-L4, CSR-L5, CSR-A1, CSR-IN1, CSR-S2, CSR-S4, CSR-S5, CSR-S6, CSR-S7, CSR-S9, CSR-S10, CSR-S11, CSR-I1, AND CSR-I4. Clarified that attestation letter should be signed by an authorized IT security professional Updated conditions for when a SOC for Cybersecurity Report is required.	Revised IT Policy Redline <07/18/2023>