pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

IT Service Organization Management and Cloud Requirements

Number
ITP-SEC040

Effective Date
July 18, 2018

Category
Security

Supersedes
ITP-BUS011

Contact
RA-ITCentral@pa.gov

Scheduled Review
January 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 Cloud Computing Services for the Commonwealth that support enterprise and agency business requirements.

2. Scope

This ITP applies to all departments, offices, boards, commissions, and councils under the Governor's jurisdiction (hereinafter referred to as "agencies"). Agencies not under the Governor's jurisdiction that utilize Commonwealth IT Resources are to follow this ITP.

Third-party vendors, licensors, contractors, or suppliers shall meet the policy requirements of this ITP that are applicable to the products and services provided to the Commonwealth.

3. Objective

- Ensure prudent selection of business and technology solutions and services during the procurement process.
- Certify 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/or implementing business and technology solutions and services.
- Increase awareness of the cybersecurity threats and their potential impacts to business operations.

- Confirm acceptable Cybersecurity practices are compliant with OA/OIT policies and industry cybersecurity standards.
- Ensure and actively monitor the Service Organizations and their Subservice Organizations through System and Organization Controls (SOC) Reporting to ensure controls are put in place and are effective to protect Commonwealth IT Resources.

4. Policy

All Cloud Computing Services must meet the requirements outlined in this policy. Any Cloud Computing Service that does not meet these requirements should not be procured or implemented for use by the Commonwealth.

Cloud Use Case (CUC) Review and approval is required prior to procurement or use of any Cloud Computing Service. This includes, but is not limited to, the following:

- Any new Cloud Computing Service regardless if already covered by an existing contract.
- Any new Cloud Computing Service that an agency would like to test or view via a Pilot and/or Proof of Concept. This would need to be in accordance with and approved by DGS per the DGS, Bureau of Procurement Pilot-Demo Policy Directive 2021-01 for New Technology Pilot Program and Product Demonstrations.
- Original scope of an approved CUC 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 and/or population (not previously disclosed).
    - New integration requirements with Commonwealth resources and/or between Cloud Computing Services.
    - New bandwidth requirements or material change in bandwidth requirements used between the Commonwealth network and Cloud Computing Service.

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

Approval of the Cloud Use Case Review request 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 Cloud 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 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 and/or Cloud Computing Service.

Agencies shall revaluate on an annual basis OPD-SEC040A *Risk Assessment and Acknowledgement* and resubmit 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 Cloud Computing Service requirements, as set forth in TABLE 1 below, and submission of all required documentation does not guarantee approval of the Cloud Use Case Review request.

TABLE 1. Cloud Computing Service Requirements:

Risk ID	Category	Requirement
Legal / Procurement		
CSR-L1	**Procurement Requirement**	• Agencies shall procure, or plan to procure, the Cloud Computing Service through an existing approved contract or other Commonwealth approved procurement method.
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	**Access to Commonwealth specific systems, data, and services**	• Agencies and Service Organizations shall limit access to Commonwealth-specific systems, data and services and provide access only to those staff, located within CONUS, that must have access to provide services proposed.
CSR-L4	**Data Hosting**	• Agencies and Service Organizations shall only host, store or backup Commonwealth 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) per guidance set in contracts. 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 Cloud Computing Services shall include a requirement that suppliers submit a SOC 2 Type 1 report, if hosting 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.

Risk ID	Category	Requirement
Accessibility		
CSR-A1	**Accessibility Standards**	Service Organization shall comply with the Accessibility Standards in ITP-ACC001, Section 6. Service Organization shall submit a completed VPAT using the most current version of the VPAT template for the proposed cloud service(s). • 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 VPAT(s) are submitted, using an older version of the template, Service Organization should provide an explanation, as to why the most current version is not being used.
Security		
CSR-S1	**System Monitoring / Audit logging (Security)**	• Service Organization 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 5.2 for additional guidance) • Verbose recommended. 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	**Data Segmentation / Boundary Protection**	• Service Organization 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), provide details on what solution components and data are deployed in which environment. • Include border gateway, perimeter and/or network firewall, web application firewall, VPN tunnels, security zone access as applicable to the solution. • Describe data encryption methods at rest and in transit across environments. • Include the direction of connectivity (specify whether initiated inbound, outbound, or both) and specifications for API calls, protocols, etc. • Service Organization shall describe how data segregation

Risk ID	Category	Requirement
		(physically or logically) of Commonwealth data from non-Commonwealth data is guaranteed. Service Organization shall maintain the diagram throughout the contract term and provide updates if 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 for the encryption of Commonwealth data as per ITP-SEC031 *Encryption Standards* and ITP-SEC019 *Protection of Commonwealth Data*. • Agencies and Service Organizations shall provide encryption technical controls to protect Data in Transit and Data at Rest. Both are required to protect Data in Use.
CSR-S5	**Identity & Access Management**	• Agencies and Service Organizations shall provide technical controls for authenticating users, provisioning and deprovisioning users, identity interaction and nonrepudiation needs for admins, internet users, and internal users. • Agencies and Service Organizations shall use Commonwealth Authentication services. Agencies and Service Organizations shall use Commonwealth Multi-Factor Authentication services.
CSR-S6	**Vulnerability Assessment**	• Service Organizations shall ensure all cloud applications are securely coded, vetted, and scanned. • Service Organizations shall conduct a third-party independent vulnerability assessment annually or sooner if due to compliance regulations or other requirements, or upon a major change to the solution. • Service Organizations shall provide vulnerability assessment results to the Commonwealth upon request. • Service Organization shall identify and validate vulnerabilities required for remediation. Service Organization shall ensure patching is up to date.

Risk ID	Category	Requirement

CSR-S7	**Data Protection / Recovery**	• Service Organization shall provide a business continuity plan that addresses the following:
		  • Data/Database Recovery
		  • Application Recovery
		  • Operating System Recovery
		  • Infrastructure Recovery
		• Service Organizations shall describe its capability to do a complete restoration in the event of a disaster.
		• Service Organizations shall describe what tests are performed as part of its disaster recovery plan.
		• Service Organizations shall describe its capability to provide services during a pandemic event.

CSR-S8	**Compliance**	• Agencies shall determine the type of data (Refer to ITP-SEC019 for categorization guidance) and ensure all Service Organizations meet compliance requirements based upon the Commonwealth Data and any applicable laws, regulations, policies, best practices and protections.
		• Service Organizations shall meet all applicable compliance requirements based upon the most restrictive data classification, per ITP-SEC019, and any applicable laws or regulations such as, but not limited to, the following:
		  o CJIS and CHRIA for criminal history data
		  o HIPAA for health-related data
		  o IRS Pub 1075 and SSA for federal protected data
		• PCI-DSS for financial data

CSR-S9	**Security Incident Handling**	• Agencies and Service Organizations shall ensure the incident management processes, including escalation procedures, and the responsibilities of each party are documented.
CSR-S10	**Inventory**	• Service Organizations shall ensure a complete, accurate, and up-to-date inventory of Commonwealth deployed resources within the cloud infrastructure and must be made available for review upon request.
Infrastructure		
CSR-I1	**Connectivity**	• Agencies and Service Organizations shall utilize an approved Commonwealth perimeter managed by Enterprise operations for inspection of all traffic between the Commonwealth's enterprise network including any datacenters, clouds, etc. that are defined to be within the Commonwealth's perimeter, and the Service Organization or its subcontractor's managed infrastructure.
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 is enabled. Monitoring must include system and network impact.
		• Stakeholders must have access as required.
		  • Verbose recommended.
		  • Ability to correlate events and create operational alerts.

Risk ID	Category	Requirement
		• 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 Organization shall maintain capacity estimates for all applications. These estimates shall include estimates of compute, storage, and network utilization.
		• These 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
		  • Constituent
		  • 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 enterprise operations teams upon request and shall be attached as supplemental data to CUC, IT Policy waiver, and similar submissions.

5.1 System and Organization Controls (SOC) Reporting Requirements

5.1.1 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 Organization shall provide an attestation, 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 verifying 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.

5.1.1.1 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 Cloud 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 and/or reporting;
- Compliance mandate for federal or state audit requirements and/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

5.1.1.2 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/RFQ that includes Cloud 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-SEC019 *Policy and Procedures for Protecting Commonwealth Electronic Data*; or
- Compliance mandated with federal or state audit requirements and/or policy.

5.1.1.3 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 has occurred;
- Cybersecurity incidents or breaches are not being detected, prevented, reported, and/or mitigated in a timely manner (as determined by the Commonwealth);
- Cybersecurity incidents or breaches are not being properly managed by the Service Organization or Subservice Organization;
- Uncertainty that the Service Organization or Subservice Organization has an effective cybersecurity risk management program;
- The Service Organization has been engaged in a merger or acquisition during the term of the contract; or
- The Service Organization has restructured its service offerings and/or business model.

5.1.1.4 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 Cloud Computing Service or as determined during a Commonwealth review and/or evaluation of a Cloud 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

5.1.1.5 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.

5.1.1.6 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.

5.1.1.7 SOC Reporting Contract Language:

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

5.1.2 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.

5.2 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:

Operating System (OS) Events

- start up and shut down of the system;
- start up and 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)

5. Responsibilities

7.1 Agencies shall:

- Submit a new Cloud Use Case Review request for any Cloud Computing Service that meets the requirements outlined in Section 4.

- Agencies may only procure and implement on the Commonwealth infrastructure Cloud Computing Services that are approved through the Cloud Use Case Request process.

- Agencies shall require third-party vendors, licensors, contractors, or suppliers to complete the Cloud Services Requirements (CSR) as part of the Cloud Use Case Review Process.

- Agencies are to 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 are to be maintained and accessible upon

request from authorized Commonwealth personnel.

- Agencies are responsible for developing and managing internal policy for Cloud Computing Service that adhere to all Management Directives and IT policies.

- Agencies shall reevaluate on an annual basis OPD-SEC040A *Risk Assessment and Acknowledgement* and resubmit 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.

- Appropriate IT governance and access control measures for cloud-based administrators should be developed and followed as detailed in ITP-SEC003 *Enterprise Security Auditing and Monitoring*.

7.2 Office of Administration, Office of Information Technology shall:

- Manage the service request process for all cloud-based services and is responsible for working with agencies in developing the appropriate business and technology architecture requirements to provide the appropriate Cloud Computing Service.

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

7.3 Third-party vendors, licensors, contractors, or suppliers shall:

Shall comply with the requirements as outlined in this ITP by coordinating with respective agencies to complete the Cloud Services Requirements (CSR) as part of the Cloud Use Case Review Process.

Third-party vendors, licensors, contractors, or suppliers are responsible for submitting SOC reports on an annual basis or otherwise set forth in the applicable contract. If using a Subservice Organization, they are responsible for obtaining and reviewing their reports to ensure compliance with Commonwealth requirements. In a timely manner, responds to any clarification requests, corrective action plan(s), and addressing, remediating, or mitigating identified concerns or nonconformities and recommendations.

6. 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*
- Cloud 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-ACC001, *Digital Accessibility Policy*
- 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-SFT000 - *Software Development Life Cycle (SDLC) Policy*
- 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.*

7. Authority

Executive Order 2016-06 *Enterprise Information Technology Governance*

8. 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.

9. 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 is to 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 • Added SOC guidance and OPD-BUS011B, OPD-BUS011C • Updated Cloud Service Requirements table and added "Responsible Party" column • Updated References section	N/A
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	N/A

Version	Date	Purpose of Revision	Redline Link
		Organization for themselves and any Subservice Organizations in the event of non-compliance	
Revision	01/30/2023	No changes - Update to OPD-SEC040A only	Revised IT Policy Redline <01/30/2023>