pennsylvania
OFFICE OF ADMINISTRATION

Information Technology Policy

IT Service Organization Management and Cloud Requirements

ITP Number ITP-BUS011	**Effective Date** July 18, 2018
Category Business	**Supersedes** --
Contact RA-ITCentral@pa.gov	**Scheduled Review** December 2021

1. Purpose

This Information Technology Policy (ITP) establishes guidance on the management of Service Organizations and establishes requirements for the procurement and implementation of cloud computing services for the Commonwealth that support enterprise and agency business processes.

2. Scope

This ITP applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction that utilize Commonwealth IT Resources are to follow this ITP.

3. Definitions

3.1 Cloud Computing Service - A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction that is provided from a cloud service provider.

3.1.1 Infrastructure as a Service (IaaS) – A Cloud Computing Service that provides processing, storage, networks, and other computing resources where the consumer can deploy and run software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications, and possibly limited control of select networking components.

3.1.2 Platform as a Service (PaaS) – A Cloud Computing Service that provides the ability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the cloud service provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

3.1.3 Software as a Service (SaaS) – A Cloud Computing Service that provides the capability using the cloud service provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, apart from limited user-specific application configuration settings.

3.2 Cloud Service Provider (CSP) - An entity (private or public) that provides Cloud Computing Services.

3.3 Commonwealth Data – Any recorded information, regardless of form, the media on which it is recorded or the method of recording, that is owned, managed, processed, generated or stored by the Commonwealth, which may be protected by law, order, regulation, directive or policy and may be sensitive or confidential so that it requires security controls and compliance standards.

3.4 Internal Control - A process that provides reasonable assurance of the achievement of an organization's objectives.

3.5 Service Organization – An entity that is external to the Commonwealth that provides services to the Commonwealth (also known as a user organization) that are part of the Commonwealth's information system.

3.6 Supplier Management - Refers to the governance and processes of obtaining and managing third-party entities that supply the Commonwealth with essential goods and services.

3.7 System and Organization Controls (SOC) – A suite of service offerings provided in connection with system-level controls of a Service Organization or entity-level controls of other organizations.

3.8 United States Jurisdiction - Consists of all fifty (50) States of the United States and the District of Columbia.

4. Policy

All cloud computing services must meet the requirements outlined in this policy. Any cloud computing service that does not meet these requirements are not to be procured or implemented for use by the Commonwealth.

A Cloud Use Case Request approval is required for:

- deploying at any stage (staging, development, production, etc.) any cloud computing service not on a state contract;
- deploying at any stage (staging, development, production, etc.) any cloud computing service Proof of Concept or Pilot;
- Any procurement for cloud computing services;
- Original scope of an approved cloud use case has significantly changed.

The agency should perform an internal assessment of the cloud services requirements (detailed below) prior to submitting a Cloud Use Case Review service request to define the scope and determine if the requirements will be met. The internal assessments of potential cloud service solutions should include a comparison of the cloud services requirements and the solution capabilities to ensure the cloud 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.

If business requirements demand a "non-compliant" cloud computing service, an IT policy waiver against this policy must be submitted through the enterprise policy waiver process (refer to ITP-BUS004 *IT Policy Waiver Process*). The submission for the policy waiver must include a completed and signed Acceptance of Risk and Risk Registry document (OPD-BUS011A *Acceptance of Risk / Risk Registry – Cloud Services Requirements*) and must set forth the business requirements that demand a "non-

compliant" cloud computing service. Approval of the waiver request is required for potential approval of a "non-compliant" cloud computing service Cloud Use Case Review request.

Adherence to the cloud services requirements, set in the table below, and submission of all required documentation does not guarantee approval of the Cloud Use Case Review request.

Risk ID	Category	Requirement
Legal / Procurement		
CSR-L1	**Procurement Requirements**	• Must procure, or plan to procure, the cloud computing services through some existing approved contract or other approved procurement mechanism
CSR-L2	**Legal Review**	• Must ensure legal review to discern appropriateness of terms in existing or planned contracts and to advise Agencies other legal requirements.
CSR-L3	**Data Storage Provisioning**	• Under no circumstances will Commonwealth Data be directly or indirectly transmitted or downloaded to, stored in, or accessible from any location that is not subject to the laws and jurisdiction of the United States
CSR-L4	**Data Hosting**	• Service Organization must offer a data hosting solution that ensures Commonwealth Data is hosted in physical locations subject to the laws and jurisdiction of the United States.
CSR-L5	**System and Organization Controls (SOC) Reporting**	• Must submit appropriate Systems and Organizations Controls (SOC) per guidance set in contracts. Refer to section 4.1 System and Organization Controls (SOC) Reporting Requirements of this ITP and to OPD-BUS011B *System and Organization Controls (SOC) Reporting Procedure* (refer to Reference section of this ITP); • Solicitations for the procurement of cloud services shall include a requirement that suppliers submit a SOC 3 report as part of the response to the solicitation.

Security		

CSR-S1	**System Monitoring / Audit logging (Security)**	• Must be enabled and accessible to the Agency Information Security Officer or designee. (Refer to Section 4.1 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 customer (i.e. agency) requires longer retention periods, the customer's longer retention requirement takes precedence.
		  • Reports should be easily accessible and in a readable format

CSR-S2	**Data Segmentation / Boundary Protection**	• Must provide a network/architecture diagram showing what technical controls are performing the network segmentation and how the technical control is used to protect COPA's networks connections both from the internet and back to COPA datacenters (i.e. border gateway, perimeter firewall, web application firewall (WAF), VPN tunnels, etc.)

CSR-S3	**Endpoint Protection**	• Must provide security controls if the cloud services are accessed from the internet. These are required to identify attacks, identify changes to files, protect against malware, protect user web services, data loss prevention (DLP), and perform 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**	• Must enable encryption for all records involved with the proposed cloud services • Must provide encryption technical controls to protect Data in Transit and Data at Rest. Both are required to protect Data in Use • It is recommended that agencies safeguard cryptographic keys and secret keys by using keys that are protected by Hardware Security Module (HSMs). (Will become a requirement in future policy revision)
CSR-S5	**Identity & Access Management**	• Must provide technical controls for authenticating users, provisioning and deprovisioning users, identity interaction and nonrepudiation needs for admins, internet users, and internal users • Must use Commonwealth Authentication services • Must use Commonwealth Multi-Factor Authentication services
CSR-S6	**Vulnerability Assessment**	• Must ensure all cloud applications are securely coded, vetted, and scanned • Must conduct a third-party independent vulnerability assessment quarterly or sooner if due to compliance regulations or other requirements, or upon a major change to the solution • Must provide vulnerability assessment results to the Commonwealth on a quarterly basis during the term of the contract and upon Commonwealth request and required on a

		quarterly basis from the time of contract is active (Refer to ITP-SEC021 and ITP-SEC023 for reporting guidance) • Must be able to identify and validate vulnerabilities required for remediation • Must ensure patching is up to date

CSR-S7	**Data Protection / Recovery**	• Must provide a business continuity plan that addresses the following:
		  • Data/Database Recovery
		  • Application Recovery
		  • Operating System Recovery
		  • Infrastructure Recovery

CSR-S8	**Compliance**	• Agencies must determine the type of data (Refer to ITP-SEC019 for categorization guidance) and ensure all cloud service providers meet compliance requirements based upon the Commonwealth data and any applicable laws, regulations, policies, best practices and protections
CSR-S9	**Security Incident Handling**	• Must ensure the incident management processes, and the responsibilities of each party, are documented
CSR-S10	**Inventory**	• Must 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**	• Must utilize the Commonwealth's Enterprise Perimeter Security (EPS) solution for inspection for all traffic sourcing from a non-Commonwealth facility/network.
CSR-I2	**Interface Requirements**	• Must conform to the Commonwealth's Network Interoperability Standards (See References section for details)

CSR-I3	**System Monitoring / Audit logging (Infrastructure)**	• Must 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
		  • Generate reports for a minimum of 90 days, archive for 1 year
		  • Reports should be easily accessible and in a readable format

4.1 System and Organization Controls (SOC) Reporting Requirements

4.1.1 SOC Reporting Requirements

Agencies and Service Organizations are to follow SOC report procedures as detailed in OPD-BUS011B *Systems & Organization Controls (SOC) Reporting Procedure*. The following guidance should 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.

4.1.1.1 SOC 1 Type II Report is required if any of the following conditions exist:

- 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; or
- 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 II reports will provide findings for Finance/Accounting controls and IT controls for services with integrated systems associated with financial transactions and reporting.

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

- 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.

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

- Reoccurring findings in SOC 1-Type II or SOC 2-Type II reports; or
- A cybersecurity incident or breach has occurred; or
- Cybersecurity incidents or breaches that are not being detected, prevented, reported, and/or mitigated in a timely manner (as determined by the Commonwealth); or
- Cybersecurity incidents or breaches are not being properly managed by the Service Organization; or
- Uncertainty that the Service Organization has an effective cybersecurity risk management program; or
- 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.

4.1.1.4 SOC 3 Report is required if any of the following conditions exist:

- Pre-RFP selection technical evaluation artifact or services that would require a SOC 1-Type II or SOC 2 Type II report; or
- As determined during a Commonwealth review and/or evaluation of cloud services that would require a SOC 1-Type II or SOC 2 Type II report.

4.1.1.5 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 subcontractors 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 and Service Auditor's Responsibilities;
- Service Organization's Management Assertion;
- Independent Auditor's Assertion;
- 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; and
- Detailed description of all findings, exceptions and opinions rendered (i.e. qualified, disclaimer, adverse) during the SOC reporting period.

4.1.1.6 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.

4.1.1.7 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.

4.1.2 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.

4.2 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
- 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)
- 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)
- use of application privileges

Application Operations

- application startup and shutdown
- application failures
- major application configuration changes
- 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
    - 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 be captured.

- 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

5.1 Office of Administration, Office for Information Technology (OA/OIT) will 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.

5.2 Commonwealth Agencies shall submit a new use case request for any cloud computing service if at least one criterion is met:

- any new cloud computing service, (i.e. product, platform, or provider not under state contract);
- a Proof of Concept or Pilot;
- a Request for Proposal (RFP);
- original scope of an approved cloud use case has significantly changed

Agencies may only procure and implement on the Commonwealth infrastructure cloud computing services that are approved through the Cloud Use Case Request process.

Agencies are to ensure that external Service 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 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. 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*.

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 - *Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*
- Management Directive 325.13 – *Service Organization Controls*
- Requirements for non-Commonwealth Hosted Applications/Services https://collab.pa.gov/dgs/home/BOP/Pages/Contract-Preparation.aspx (*Limited Access*)
- OPD-BUS011A – *Acceptance of Risk / Risk Registry – Cloud Services Requirements*
- OPD-BUS011B – *System and Organization Controls (SOC) Reporting Procedure*
- OPD-BUS011C – *System and Organization Controls (SOC) Correspondence Procedure*
- SOC Repository - https://itcentral.pa.gov/Pages/SOC_Reports.aspx (*CWOPA Limited Access*)
- Commonwealth's Network Interoperability Standards (Contact RA-ITCentral@pa.gov for information; *CWOPA authorized personnel only*)
- ITP-SFT000 - *Software Development Life Cycle (SDLC) 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-SEC020 – *Encryption Standards for Data at Rest*
- ITP-SEC021 - *Security Information and Event Management Policy*

- ITP-SEC023 - *Information Technology Security Assessment and Testing Policy*
- ITP-SEC031 – *Encryption Standards for Data in Transit*
- ITP-SEC034 – *Enterprise Firewall Rule Set*
- ITP-SEC038 - *COPA Data Center Privileged User Identification and Access Management 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*

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 IT policy, a request for a policy waiver is to 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. 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	Revised IT Policy Redline <01/27/2020>
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.	Revised IT Policy Redline <12/1/2020>