pennsylvania
OFFICE OF ADMINISTRATION
INFORMATION TECHNOLOGY

Information Technology Policy

Commonwealth Cloud Computing Services Requirements

ITP Number	**Effective Date**
ITP-BUS011	July 18, 2018
Category	**Supersedes**
Business	--
Contact	**Scheduled Review**
RA-ITCentral@pa.gov	July 2019

1. Purpose

Establishes the requirements for the procurement and implementation of cloud computing services for the Commonwealth that support enterprise and agency business processes.

2. Scope

This Information Technology Policy (ITP) applies to all departments, boards, commissions and councils under the Governor's jurisdiction. Agencies not under the Governor's jurisdiction but are utilizing the 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) – The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run arbitrary 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) – The capability provided to the consumer is 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) – The capability provided to the consumer is to use 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-based platforms, infrastructure, applications, security, and/or storage services for another entity/organization.

3.3 Cloud Storage - Infrastructure as a Services (IaaS) deployment model that provides block, file and/or object storage services delivered through various protocols. The service can be stand-alone with no requirement for additional managed services or be bundled with additional managed services.

3.4 Commonwealth Data – Consists of, but is not limited to, data is that intellectual property of the Commonwealth, data that is protected by law, order, regulation, directive or policy and any other sensitive or confidential data that requires security controls and compliance standards.

3.5 IT Governance - The processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals. It requires specification of the decision rights and accountability framework to encourage desirable behavior in the use of information technology.

3.6 Proof of Concept - A project that is evaluated exclusively on pass or fail success criteria. Failed success criteria can still be considered a successful proof of concept as the results gave definitive proof that the concept was not viable.

3.7 Pilot - A project that consists of a scaled down, but fully functional environment with the exact same capabilities that would be enabled if the environment were to be promoted to production.

3.8 Office of Administration, Office for Information Technology Enterprise (OA/OIT Enterprise) – Consists of the offices managed by the Commonwealth Chief Information Officer (CIO), Chief Technology Officer (CTO), Chief Information Security Officer (CISO), Director, Office of Strategy and Management, Director, Enterprise Services and their respective program areas.

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

4. Policy

All cloud computing services, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), must meet the requirements outlined in the Cloud Services Requirements table below. Any cloud computing service that does not meet these requirements are to be avoided for procurement and implementation within the Commonwealth.

A Cloud Use Case Request approval is required for:

- 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.

(For RFPs, this IT Policy is to accompany the request and prior to selection of winning bid, the Delivery Center/Agency must have approval of the Cloud Use Case Review to ensure the provider meets OA/OIT Enterprise requirements.)

The Delivery Center/Agency should perform an internal assessment of these Cloud Services Requirements prior to submitting a Cloud Use Case Review Service Request to define the scope and determine if the requirements will be met.

If business requirements demand a "non-compliant" cloud computing service, an IT policy waiver against this policy, submitted along with a completed and signed Acceptance of Risk and Risk Registry document (OPD-BUS011A - *Acceptance of Risk / Risk Registry – Cloud Services Requirements*) and must be submitted through COPPAR (refer to ITP-BUS004 – *IT Policy Waiver Process*). Approval of the waiver request is required for potential approval of a Cloud Use Case Review request.

Adherence to these Cloud Services Requirements and submission of all required documentation does not guarantee approval of the Cloud Use Case Review request. To submit a cloud use case request, refer to the Enterprise Architecture Review Committee (EARC) Process.

CLOUD SERVICES REQUIREMENTS (CSR)		
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 contract, to evaluate the cloud computing services for compliance purposes, and to advise Agency on the need for encryption and/or other recommended requirements
CSR-L3	**Data Storage**	• 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
Security		

CSR-S1	**System Monitoring / Audit logging (Security)**	• Must be enabled and accessible to the Agency/Delivery Center 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 using an approved Commonwealth scanning tool • Must conduct a vulnerability assessment quarterly or sooner if due to compliance regulations or other requirements, or upon a major change to the application or the server • 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**	• Must meet compliance requirements if the cloud service being proposed is subject to any law
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 Cloud Service Connectivity model. (See References section for details)
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 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 Enterprise (OA/OIT Enterprise) will manage the service request process for all cloud-based services and is responsible for working with agencies/delivery centers in developing the appropriate business and technology architecture requirements to provide the appropriate cloud computing service.

OA/OIT Enterprise 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/Delivery Centers shall submit a new use case request for any cloud computing service if at least one criteria are 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/Delivery Centers may only procure and implement on the Commonwealth infrastructure cloud computing services that are approved through the Cloud Use Case Request process.

Agencies/Delivery Centers are responsible developing and managing internal policy for cloud computing service that adhere to all Management Directives and IT policies. In addition, 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*
- OPD-BUS011A – *Acceptance of Risk / Risk Registry – Cloud Services Requirements*
- Enterprise Architecture Review Committee (EARC) Process (Contact RA-ITCentral@pa.gov for information)
- Commonwealth's Enterprise Cloud Service Connectivity model (Contact RA-ITCentral@pa.gov for information)
- Commonwealth's Network Interoperability Standards (Contact RA-ITCentral@pa.gov for information)
- 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-SEC020 – *Encryption Standards for Data at Rest*
- 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 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, for reasons such as the need to comply with requirements for a federally mandated system, a request for waiver may be submitted via the Commonwealth of PA Procurement and Architectural Review (COPPAR) process. Requests are to be entered into the COPPAR Tool located at http://coppar.oa.pa.gov/. Refer to ITP-BUS004 *IT Waiver Review Process* for guidance.

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

Version	Date	Purpose of Revision
Original	07/18/2018	Base Document