

ISMS-ISPS-020	Cloud Security Standard (For Departments)	
INTERNAL		Version: 1.1

# CITY UNIVERSITY OF HONG KONG

## Cloud Security Standard (For Departments)

---

*(Approved by the Information Strategy and Governance Committee  
in Jan 2024)*

**INTERNAL**

**Date of Issue: 2024-01-11**

ISMS-ISPS-020	Cloud Security Standard (For Departments)	
INTERNAL		Version: 1.0

## Document Control

Document Owner	Classification	Publication Date
CSC	INTERNAL	2024-01-11

## Revision History

Version	Date	Summary of Changes
1.0	2023-08-31	Initial Release
1.1	2024-01-11	Added 10.11.1 (c) – security vetting requirement

## Distribution

Copy	Issued to	Location
Master	Internal	<a href="https://www.cityu.edu.hk/csc/information-security/information-security-policies-and-standards">https://www.cityu.edu.hk/csc/information-security/information-security-policies-and-standards</a>

ISMS-ISPS-020	Cloud Security Standard (For Departments)	
INTERNAL		Version: 1.1

## Contents

1	Policy Statement .....	1
2	Objective .....	1
3	Scope.....	1
4	Terms and Definitions .....	1
5	Cloud Computing Model .....	1
6	Cloud Service Models.....	2
7	Deployment Models.....	2
8	Shared Responsibility Model .....	3
9	Cloud Security Principles.....	4
10	Security Requirements for Provisioning of Cloud Services .....	5
10.1	Data Security .....	5
10.2	Identity and Access Management.....	6
10.2.1	Cloud User Access Management .....	6
10.2.2	Privileged Account Management on Cloud .....	6
10.3	Cryptography .....	6
10.3.1	Data Encryption.....	6
10.4	Security Monitoring and Reporting.....	6
10.4.1	Security Incident Management.....	7
10.4.2	Incident Reporting .....	7
10.5	Operations Security.....	7
10.5.1	Data Backup .....	7
10.5.2	Vulnerability Management .....	8
10.5.3	Change and Configuration Management.....	8
10.6	Security Audit and Monitoring .....	8
10.6.1	Audit Log Management.....	8
10.6.2	Audit Log Review and Analysis.....	8
10.7	System Acquisitions and Development.....	9
10.7.1	Secure Development of Cloud Applications .....	9
10.8	Network Communications Security.....	9
10.8.1	Protection for data transmission .....	9
10.8.2	Network Attack Monitoring and Protection .....	9
10.9	Infrastructure Security .....	10
10.9.1	Virtual Network Segmentation .....	10

ISMS-ISPS-020	Cloud Security Standard (For Departments)	
INTERNAL		Version: 1.1

10.9.2	Virtualization Security .....	10
10.9.3	Container Security.....	10
10.10	Third Party Management.....	11
10.10.1	Contractual Requirements.....	11
10.10.2	Exit Management.....	11
10.10.3	Business Continuity Planning (BCP) .....	12
10.10.4	Disaster Recovery (DR).....	12
10.11	Compliance .....	12
10.11.1	Compliance with Applicable Standards and Regulatory Requirements .....	12
11	Appendix .....	13
11.1	Appendix A: Standard Security Requirements for Cloud Service Tender Preparation..	13
11.2	Appendix B: Checklist.....	15
11.3	Appendix C: Reference .....	17

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page 1 of 17
INTERNAL		Version: 1.0

## 1 Policy Statement

The City University of Hong Kong (“University”) must ensure the security when building private clouds and acquiring public cloud services from external cloud services providers.

## 2 Objective

The purpose of this document is to establish a security standard for adopting cloud services and to outline the fundamental security control requirements in a cloud environment.

## 3 Scope

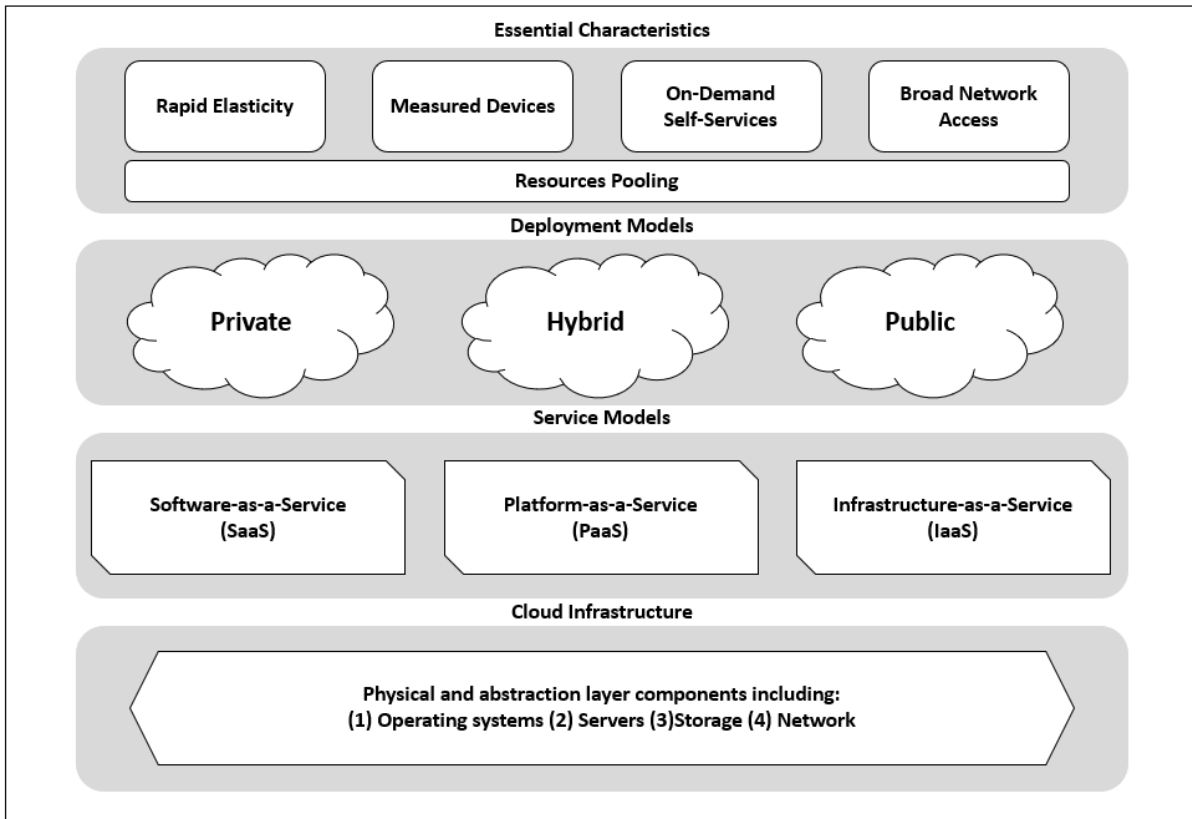
This standard applies to all cloud applications and cloud service adoptions at the University, including projects utilizing private or public clouds and any combination of Infrastructure-as-a-service, Platform-as-a-Service, and Software-as-a-Service cloud service models.

## 4 Terms and Definitions

Throughout the document, Cloud Service Provider (CSP) generally refers to a vendor or third party providing public cloud services to the University. This may include the underlying platform provider (e.g., AWS, Azure), the multi-cloud managed service provider (or cloud service broker), the system integrator supporting the cloud project, or the vendor supplying the SaaS application. The actual responsible party may vary depending on each project's arrangement.

## 5 Cloud Computing Model

As defined by National Institute of Standards and Technology (NIST), cloud computing is a model that enables ubiquitous, convenient and 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. Cloud computing infrastructure can be categorized into three service models and three deployment models, as illustrated in the diagram below.



## 6 Cloud Service Models

There are three typical types of cloud service models, outlined as follows:

(a) Infrastructure-as-a-Service (IaaS):

IaaS is a service delivery model in which the basic computing infrastructure, including servers, software, and network equipment, is provided as an on-demand service. This allows for the establishment of a platform to develop and execute applications.

(b) Platform-as-a-Service (PaaS):

PaaS is a service delivery model in which the computing platform is provided as an on-demand service, enabling applications to be developed and deployed. Its main purpose is to reduce the cost and complexity of purchasing, housing, and managing the underlying hardware and software components of the platform, including any necessary programming and database development tools.

(c) Software-as-a-Service (SaaS):

SaaS is a service delivery model in which one or more applications and the computational resources required to run them are provided for use on-demand as a turnkey service.

## 7 Deployment Models

There are three typical types of cloud deployment models, outlined as follows:

(a) Private Cloud:

A private cloud is provisioned for the exclusive use of a single organization comprising multiple user departments. It may be owned, managed, and operated, or any combination of them, by the organization itself or external service providers. The infrastructure may be hosted within the organization's data center or externally.

(b) Public Cloud:

A public cloud is provisioned for public use. It supports multi-tenancy and may be owned, managed, and operated, or any combination of them, by an external CSP. The infrastructure is hosted at the CSP's premises.

(c) Hybrid Cloud:

A hybrid cloud consists of more than one distinct cloud infrastructure (e.g., private and public) that may be provisioned by different CSPs. This model enables data and application portability.

## 8 Shared Responsibility Model

Adopting cloud services adheres to a shared responsibility model, which means that cloud users assume some responsibilities for security when moving applications, data, and workloads to the cloud environment, while the CSP takes on other responsibilities simultaneously. However, the shared responsibility varies by the CSP and cloud service models, and it is essential to define the boundary between the cloud users' responsibilities and those of the CSP to reduce the risk of introducing security control weaknesses or security loopholes into the cloud environment.

The table below provides a high-level overview of the shared responsibilities between the University and the CSP:

Layer	Software-as-a-Service (SaaS)	Platform-as-a-Service (PaaS)	Infrastructure-as-a-Service (IaaS)	On-premises
Data	Managed by CityU	Managed by CityU	Managed by CityU	Managed by CityU
Application	Managed by CityU	Managed by CityU	Managed by CityU	Managed by CityU
Operating System	Managed by CityU	Managed by CityU	Managed by CityU	Managed by CityU
Virtualization	Managed by CityU	Managed by CityU	Managed by CityU	Managed by CityU
Servers	Managed by CityU	Managed by CityU	Managed by CityU	Managed by CityU
Storage	Managed by CityU	Managed by CityU	Managed by CityU	Managed by CityU
Network	Managed by CityU	Managed by CityU	Managed by CityU	Managed by CityU
Physical	Managed by CityU	Managed by CityU	Managed by CityU	Managed by CityU

■ Managed by CityU  
■ Managed by CSP

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page 4 of 17
INTERNAL		Version: 1.0

### Cloud User's Share of Responsibilities:

When using a server-based IaaS, serverless infrastructure, or a PaaS cloud service model, cloud users are responsible for several key tasks, including:

- a) Managing information and data, and controlling how and when data is used;
- b) Securing application code repositories from malicious intrusion or misuse, including application build testing throughout the development and integration process;
- c) Maintaining all aspects of identity and access management, including but not limited to:
  - i. Authentication and authorization mechanisms;
  - ii. Single sign-on ("SSO");
  - iii. Multifactor authentication ("MFA");
  - iv. Access keys;
  - v. Certificates;
  - vi. User creation and access provisioning processes;
  - vii. Password Management.
- d) Maintaining platform and resources configurations, including but not limited to:
  - i. Operating system and application patching;
  - ii. Operating system and application hardening;
  - iii. Change and configuration management for IaaS instances.

### CSP's Share of Responsibilities:

Regardless of the cloud service models, the CSP is responsible for several key tasks, including:

- a) Controlling the provisioning of physical resources via virtualization;
- b) Ensuring network segmentation and customer isolation among multiple tenants in the shared pool of virtual resources;
- c) Protecting hardware, including physical hosts, network, and data center through various software and physical means; and
- d) Ensuring rapid failover and high-availability disaster recovery mechanisms.

## 9 Cloud Security Principles

The Cloud Security Principles require that:

- a) Different security control requirements should be considered depending on the following factors:
  - i. Data involved
  - ii. The cloud service model (e.g. IaaS, PaaS, SaaS or combinations)
  - iii. Business use cases (e.g. target users, operation models, etc.)
- b) Zero-trust, layered security, and defense-in-depth principles be adopted.
- c) Equivalent or stronger security controls or processes in the cloud environment compared to on-premise be implemented.
- d) Security control objectives should be vendor-neutral and can be achieved by native cloud security services or third-party solutions.
- e) Automation be considered as far as practically possible.



ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page 5 of 17
INTERNAL		Version: 1.0

- f) Data Privacy Principles be referenced for any information related to Personally Identifiable Information (PII) managed and stored in the private and public cloud environment.

## 10 Security Requirements for Provisioning of Cloud Services

### 10.1 Data Security

- a) System owners shall identify and classify all data stored and business applications hosted in the cloud environment.
- b) System owners shall ensure appropriate security controls have been implemented for each classification in the cloud environment.
- c) System owners shall define the ownership of the following data and communicate with the CSP prior to service adoption.
  - a) Content data and metadata in the public cloud environment;
  - b) Virtual machine image(s);
  - c) IT users' account information.
- d) System owners shall create and maintain an up-to-date inventory of data store/process for each cloud service. Privacy impact assessment (PIA) should be conducted prior to deployment of the respective cloud services.
- e) System owners shall prevent data migration, particularly CONFIDENTIAL and RESTRICTED data, to the cloud without prior approval.
- f) System owners shall observe data protection and privacy legislation, including but not limited to the Personal Data (Privacy) Ordinance (PDPO) (Cap. 486) and its Amendments, particularly the Data Protection Principle 4 (on security of personal data). If the data will be processed/stored in EU, UK, or the Mainland, the CSP shall also comply with EU/UK General Data Protection Regulation (GDPR) and the Mainland Personal Information Protection Law (PIPL). They shall also observe the University's Code of Practice on Personal Data (Privacy) Issues.
- g) System owners shall ensure that the CSP supports secure data destruction for disposal at the expiry or termination of service or upon request of the University.
- h) System owners should require the CSP to disclose the locations/jurisdictions where the data will be stored, so that this information may be made known to the data subjects.
- i) System owners should choose a CSP that allows them to choose or specify locations/jurisdictions where there is adequate legal protection to personal data.
- j) System owners shall make users aware of the transborder arrangement with regard to how their personal data is protected.
- k) System owners should enforce data de-identification (e.g. tokenization<sup>1</sup>, anonymisation<sup>2</sup> and randomisation<sup>3</sup>) to prevent data subjects' identities from being revealed with the processed results while business purposes are being fulfilled.

#### Notes:

- 1 Data tokenisation involves replacing sensitive data elements with substitutes without extrinsic meanings, usually referred to as tokens. These tokens can be mapped back to sensitive data afterwards.

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page 6 of 17
INTERNAL		Version: 1.0

- 2 Data anonymisation is the process of turning data into a form such that the identification of individuals is not likely to succeed.
- 3 Data randomisation adds noise to a data field. It does not preserve data truthfulness at the record level but reduces the risk of singling out identifying attributes. Generally the values are modified so that their new values differ from their true values in a random way.

## 10.2 Identity and Access Management

### 10.2.1 Cloud User Access Management

- a) System owners shall enforce a password policy by following the "Password Management and Multi-Factor Authentication Policy" as far as possible for all user accounts in the cloud environment.
- b) System owners shall enable multi-factor authentication (MFA) for cloud applications that process/store CONFIDENTIAL level or above data.
- c) System owners should follow the principles of least privilege and separation of duties when assigning data access rights and access privileges of information systems to cloud users.
- d) System owners shall manage and securely keep user login credentials for accessing the cloud application's production environment to prevent unauthorized access and change of cloud application programs and configuration files.
- e) System owners should assign permission to user roles or groups instead of to individual user accounts.
- f) System owners should gain access to service accounts through user roles instead of individual user accounts.
- g) System owners should regularly review user access rights to cloud applications, infrastructure, and backend systems (e.g., annually) or upon change of personnel, and disable all logical access and credentials upon contract termination.
- h) System owners should review and disable inactive user accounts where appropriate.
- i) System owners shall not write credentials (e.g., password) in code when using APIs, CLI, or SDKs to access cloud resources.

### 10.2.2 Privileged Account Management on Cloud

- a) System owners shall enable multi-factor authentication for privileged user accounts. Alternative security controls (e.g., PAM) shall be implemented if MFA cannot be enabled to prevent unauthorized privileged user account access.
- b) System owners shall not allow sharing of privileged user accounts, and must strictly enforce accountability of privileged users.

## 10.3 Cryptography

### 10.3.1 Data Encryption

System owner shall implement appropriate encryption controls to ensure that all CONFIDENTIAL or above data stored in the cloud environment is encrypted.

## 10.4 Security Monitoring and Reporting

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page 7 of 17
INTERNAL		Version: 1.0

#### **10.4.1 Security Incident Management**

- a) System owners shall follow the "Information Security Incident Management Standard" for handling security incidents directly related to the University systems deployed in the public cloud environment.
- b) System owners should regularly review the existing incident management procedure to incorporate potential changes caused by changes in public cloud service(s) and CSP(s).
- c) System owners shall define the roles and responsibilities of each stakeholder in the University and CSP to ensure all relevant stakeholders are aware of their action(s) to be taken during the incident response process for public cloud services.
- d) System owners shall maintain a list of contact points for incident response, which contains at least a point of contact from the CSP for incident reporting, and distribute the list to all relevant stakeholders in the University and the CSP to maintain effective communication during the incident response process.
- e) System owners should regularly review alerts and findings from the security monitoring and detection service provided by CSP, and remediate any identified issues in a timely manner.

#### **10.4.2 Incident Reporting**

CSP shall provide an incident report with all relevant information to the University for investigation within a reasonable time upon confirmation of an incident occurring in the CSP's public cloud environment that has impacted the University's service. The incident report should include the following information:

- i. Date and time of the incident identified;
- ii. Description of the incident;
- iii. Initial findings;
- iv. Systems affected;
- v. Physical location of the affected systems;
- vi. Impact;
- vii. Root cause;
- viii. Action plan for remediation (short-term/long-term);
- ix. Current system remediation status;
- x. Cost incurred (if any).

### **10.5 Operations Security**

#### **10.5.1 Data Backup**

- a) System owners should clearly define and agree upon the responsibilities for performing backups related to the adopted cloud services with CSPs.
- b) If the CSP is responsible for backups, system owners should request and review their backup capability specifications to ensure they meet the University's backup requirements. The specifications should include, but are not limited to:
  - i. Scope and schedule of backups;
  - ii. Backup methods and data formats (if relevant);
  - iii. Retention period for backup data.
- c) For critical system, system owner should obtain at least one offline regular backup copy of operational data to ensure the possibility of recovery to the most up-to-date state.

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page 8 of 17
INTERNAL		Version: 1.0

- d) System owners should perform regular backup recovery tests to confirm the proper functioning of recovery procedures, their up-to-date status, and their ability to meet the Recovery Time Objective (RTO) and Recovery Point Objective (RPO).
- e) System owners should store backups, log copies, access records, and other relevant information securely for legal and compliance purposes.
- f) System owners may utilize built-in backup capabilities and automated processes with policies in storage services.

### **10.5.2 Vulnerability Management**

- a) System owners should follow the "Network and Platform Security Standard" to fix identified security vulnerabilities in the cloud environment within defined timeframes, adopting a risk-based approach.
- b) System owners should scan any binary files before uploading them to non-compute resources (e.g., storage) in the cloud environment.

### **10.5.3 Change and Configuration Management**

- a) System owners should assess, authorize, and test changes to cloud applications/platforms before implementing them in the production environment to avoid undesired impacts on the University's services/operations.
- b) System owners should configure systems and applications hosted in the cloud environment according to regulatory requirements and the CSP's recommended security practices.
- c) System owners should continuously monitor for any unauthorized changes to the configurations of all systems and applications hosted in the cloud environment.

## **10.6 Security Audit and Monitoring**

### **10.6.1 Audit Log Management**

- a) System owners should define and agree upon the allocation of responsibilities and requirements for audit logging in cloud applications, infrastructure, and backend systems with CSPs.
- b) System owners should enable system auditing and logging for all cloud applications, infrastructure, and backend system components, including but not limited to:
  - i. Network;
  - ii. Operating system;
  - iii. Container;
  - iv. Application;
  - v. Function calls;
  - vi. Virtual instances.
- c) System owners should define the retention period for audit logs for all adopted cloud applications, infrastructure, and backend system components.
- d) System owners shall strictly control access to audit logs and ensure they are tamper-resistant to prevent unauthorized modification.

### **10.6.2 Audit Log Review and Analysis**

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page 9 of 17
INTERNAL		Version: 1.0

- a) System owners should continuously perform log reviews using correlation tools to analyze any abnormal activities occurring in the cloud applications, infrastructure, and backend systems within the cloud environment.
- b) System owners should configure and enable alert notifications for analysis and remediation.
- c) If a CSP performs log review and analysis functions, system owners should request a regular log review report (e.g., monthly) from the CSP, including but not limited to the following items:
  - i. System faults;
  - ii. System performance;
  - iii. Malicious activities;
  - iv. Event summary and trend analysis.

## 10.7 System Acquisitions and Development

### 10.7.1 Secure Development of Cloud Applications

- a) System owners shall follow the "Information System Acquisition, Development, and Maintenance Standard" during the development of applications in the cloud platform.
- b) System owners should apply a secure software development lifecycle to cloud applications and address security threats throughout the development process with proactive checks, including:
  - i. Conducting threat modeling during the design process to identify and mitigate potential security issues early;
  - ii. Following development best practices and secure coding standards (e.g. security code review, de-identification of personal data, data input validation and output encoding requirements) for preventing web application vulnerabilities; and
  - iii. Using various tools (e.g. code scanning and analysis tools, testing tools and code obfuscation tools) for testing, verification and code protection before deployment.

## 10.8 Network Communications Security

### 10.8.1 Protection for data transmission

- a) System owners shall follow the "Network and Platform Security Standard" and implement strong communication channel encryption protocols for data transmission involving sensitive information.
- b) System owners shall implement secure protocols such as TLS, Virtual Private Network (VPN), or dedicated connections for end-to-end data transmission between the cloud and the University's network.
- c) System owners shall follow the "Logical Access Control Security Standard" to define and implement network-level access controls (e.g., deny public access to internal cloud services by default, do not open management ports such as TCP port 22 and 3389 directly to the public network, but allow managed remote access service provided by the CSP).

### 10.8.2 Network Attack Monitoring and Protection

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page <b>10</b> of <b>17</b>
INTERNAL		Version: 1.0

System owner should implement network security monitoring and protection measures to continuously detect and immediately respond to network-based attacks on the University's network, including the virtual network. These measures should include, but not be limited to:

- i. Network Firewall;
- ii. Web Application Firewall;
- iii. Anti-DDoS;
- iv. Network Traffic Information;
- v. Log Monitoring Tool.

## **10.9 Infrastructure Security**

### **10.9.1 Virtual Network Segmentation**

- a) System owners should create security zones to isolate virtual instances based on the following criteria:
  - i. Implementation phase (i.e. development, testing and production environment);
  - ii. Data classification;
  - iii. Architecture layer;
  - iv. Criticality of the cloud systems/applications.
- b) System owners should implement network access controls at both container and platform levels to control network traffic between nodes and master nodes, as well as between master nodes and external nodes.

### **10.9.2 Virtualization Security**

- a) System owners shall perform hardening to remove and/or disable all unnecessary configurations, services, and ports on system components, covering at least the following:
  - i. Host and Guest OS;
  - ii. Container images;
  - iii. Hypervisors;
  - iv. Container orchestration stack and control plane.
- b) System owners should perform periodic vulnerability scanning for the host and guest OS/image used for virtualization.
- c) System owners should enable logging for all privileged accounts' activities in virtual instances and hypervisors to trace unauthorized access to virtual instances' images or snapshots.
- d) System owners must handle VM images and snapshots with care, as they may contain captured CONFIDENTIAL data on the system at the time the image/snapshot was taken. They must also wipe VM image copies and snapshots when no longer needed.
- e) When deleting a VM from a physical server or moving it to another physical server, system administrators shall ensure no data is left behind on the disk that makes data recovery possible.
- f) System owners should clear VMs using secure deletion solutions.

### **10.9.3 Container Security**

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page <b>11</b> of <b>17</b>
INTERNAL		Version: 1.0

- a) Define a standardized process for securely managing centralized container images and repositories in the cloud environment to:
  - i. Perform periodic container image scanning to identify potential security vulnerabilities;
  - ii. Rebuild container images for security patching;
  - iii. Perform hardening on container images and pertinent configuration files according to the defined configuration baseline;
  - iv. Use base images from trusted sources only, update base images frequently and select base images from minimalistic technologies like Alpine Linux and Windows Nano Server to reduce attack surface areas.

## **10.10 Third Party Management**

### **10.10.1 Contractual Requirements**

- a) The agreement of terms and conditions of cloud services between the University and the CSP shall include at least the following:
  - i. A list of services and support tasks that will be provided by the CSP;
  - ii. An agreement on handing confidential information; and
  - iii. Actions and penalty clauses applicable in the event of security breach caused/performed by the CSP, as well as their failure to comply with the agreed service level; especially their obligation to notify the University of any data breaches that occur within a reasonable timeframe after they become aware of the breach.
  - iv. Security requirements/checklist for the adopted cloud services.
- b) If there is a sub-contracting arrangement, system owners should obtain formal contractual assurance from the CSP that the same level of protection and compliance controls are equally applicable to their sub-contractors.
- c) The Service Level Agreement (SLA) between the University and CSP shall include confidentiality and non-disclosure clauses that explicitly state that all cloud user data would be safely and securely removed from the CSP when the cloud service is terminated.
- d) System owners should regularly review and evaluate the CSP's performance against the SLA, and address any non-conformance.
- e) System owners should regularly check with the CSP for any notices of changes in the common statements of Service Level Agreement as the CSP may reserve the rights to update some terms in the SLA with limited advance notice.

### **10.10.2 Exit Management**

- a) System owners shall formulate an exit plan with the CSP during contract establishment for the provisioning of cloud services to define procedures to retrieve data and virtual instances out of the CSP and securely remove the data and virtual instances from the CSP's environment.
- b) In the event of termination or change of CSP, system owners should implement at least the following measures:
  - i. Prepare a formal handover document that covers a checklist of the assets to be handed over and is signed-off by both the University and the CSP.

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page <b>12</b> of <b>17</b>
INTERNAL		Version: 1.0

- ii. Modify the implemented authentication and authorization controls (e.g., passwords, credential information for authentication, etc.) to terminate CSP's access rights to the University's application data and information.
- iii. Include in the exit plan on how to retrieve data and the virtual environments out of the CSP and how to clean up data and the virtual environments.
- iv. Ensure the legal notice clearly states that all data or configuration settings stored in the CSP's system, including the backup data, are permanently removed.

### **10.10.3 Business Continuity Planning (BCP)**

- a) System owners should follow the "Business Continuity Management Standard" to conduct a business impact analysis and assess how changes in cloud service adoption may impact the cloud environment's systems or data.
- b) System owners should develop a Business Continuity Plan (BCP) for the adopted cloud services, which includes, at a minimum, the following scenarios:
  - i. Loss of the CSP's public cloud services;
  - ii. Loss of third-party dependent capabilities.
- c) System owners should conduct regular BCP drill tests to ensure that all relevant stakeholders, including the CSP, understand the BCP procedures and that the BCP functions properly.

### **10.10.4 Disaster Recovery (DR)**

- a) System owners should define and agree on the disaster recovery arrangements with the CSP, including:
  - i. Recovery Point Objective ("RPO") and Recovery Time Objective ("RTO");
  - ii. Restoration priorities;
  - iii. Location of the disaster recovery site(s);
  - iv. Roles and responsibilities of the recovery teams;
  - v. Lines of communications during the DR arrangements.

## **10.11 Compliance**

### **10.11.1 Compliance with Applicable Standards and Regulatory Requirements**

- a) System owners shall request and review the CSP's third-party audit reports or compliance certificates (e.g., ISO 27001, ISO 27018, SOC2 Type 1 and Type II report) to verify its level of compliance level with globally recognized industry security standards.
- b) System owners shall ensure the CSP is CSA STAR Level 2 (attestation) compliant or completes the CSA STAR Level 1 Self-Assessment. The Consensus Assessments Initiative Questionnaire created by the Cloud Security Alliance can be used as a reference set of questions for assessing a CSP.
- c) System owners shall obtain security vetting from Information Security Unit (ISU) of CSC if the cloud services being utilized will store or process information categorized as CONFIDENTIAL or RESTRICTED. System owner shall make sure cloud services provider to comply Standard Security Requirements set out in Appendix A during provision the cloud services.



ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page 13 of 17
INTERNAL		Version: 1.0

## 11 Appendix

### 11.1 Appendix A: Standard Security Requirements for Cloud Service Tender Preparation

The following standard clauses set out the mandatory security requirements that shall be included in a Tender for the provision of Cloud Services.

- 1) Cloud Service Provider (CSP) shall comply with the data protection and privacy legislation in Hong Kong, including the Personal Data (Privacy) Ordinance (PDPO) and its Amendments. If data is processed/stored in EU, UK or Mainland China, the CSP shall also comply with their corresponding data protection regulations :
  - a. EU General Data Protection Regulation (GDPR)
  - b. UK General Data Protection Regulation (GDPR)
  - c. Personal Information Protection Law (PIPL) of the Mainland
- 2) CSP shall disclose to the University the locations/jurisdictions where the data will be stored.
- 3) CSP shall support secure data destruction for disposal at the expiry or termination of service or upon request of the University.
- 4) The proposed Cloud System/Application shall support Multi-Factor Authentication (MFA) for systems or applications that may process or store confidential data. If MFA is not supported, the CSP must provide compensating security controls (e.g. strong password and regular password change) to protect cloud user accounts.
- 5) The proposed Cloud System/Application shall support MFA for privileged user accounts. Alternative security controls shall be provided (e.g. PAM) if MFA is not supported to prevent unauthorized privileged user account access.
- 6) The proposed Cloud System/Application shall support encryption for both data-at-rest and data-in-transit to protect confidential data.
- 7) CSP shall provide a list of contact points for security incident response and inform the University when the list changes.
- 8) CSP shall provide an incident report and provide information to the University for investigation within reasonable time upon the confirmation of security incidents in the CSP's cloud environment that have impacted the University's service. The incident report should include the following information:
  - a. Date and time of the incident identified;
  - b. Description of the incident;
  - c. Initial findings;
  - d. Systems affected;
  - e. Physical location of the affected systems;
  - f. Impact;
  - g. Root cause;
  - h. Action plan for remediation (short-term/long-term);
  - i. Current system remediation status;
  - j. Cost incurred (if any).
- 9) The proposed Cloud System/Application shall only allow authorized persons from the University to access the audit logs, and all audit logs must be tamper-resistant to prevent unauthorized modification.

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page <b>14</b> of <b>17</b>
INTERNAL		Version: 1.0

- 10) CSP shall support secured connections (e.g. TLS, VPN or dedicated connections) to protect end-to-end data transmission between the proposed Cloud System/Application and the University.
- 11) The proposed Cloud System/Application shall be hardened so that all unnecessary configurations, services and ports on its system components are removed or disabled.
- 12) CSP shall handle VM images and snapshots with care as they may contain capture of CONFIDENTIAL data on the system at the time the image/snapshot was taken.
- 13) CSP shall notify the University at least one month in advance of any significant changes (e.g. service upgrade, cease offering a particular service) in the proposed Cloud System/Application.
- 14) CSP shall ensure that the same level of protection and compliance controls apply to their sub-contractors.
- 15) CSP shall provide the procedures to retrieve the University's data/virtual instances and securely remove the data and virtual instances from the CSP's environment when the cloud service is terminated.
- 16) CSP shall comply with the following security standards and provide the latest certificates/audit reports for the University to review whenever the certificates/audit reports have been renewed.
  - a. ISO 27001
  - b. SOC2 Type 1 and Type II
  - c. ISO 27018
  - d. CSA STAR Level 2 or Level 1

## 11.2 Appendix B: Checklist

The following checklist can help cloud service subscribers to check if they can comply with this Cloud Security Standard.

Item	Description	Reference	Checked (Yes,No,N/A)
1	Ensure Cloud Service Provider (CSP) comply with applicable data protection laws and regulations	10.1	
2	Confirm with CSP the locations/jurisdictions where the data will be stored	10.1	
3	Ensure CSP supports secure data destruction for disposal at the expiry or termination of service or upon request of the University	10.1	
4	The password policy for the user accounts in the cloud environment shall follow the University's prevailing password policy as far as possible	10.2.1	
5	Ensure Multi-Factor Authentication (MFA) has been enabled for cloud applications that process/store confidential data	10.2.1	
6	Ensure Multi-Factor Authentication (MFA) or equivalent security control has been enabled for privileged user accounts.	10.2.2	
7	Ensure privileged user accounts shall not be shared and the accountability of privileged users shall be strictly enforced.	10.2.2	
8	Ensure appropriate encryption controls have been implemented to ensure that all confidential data processed/stored in the cloud environment is encrypted	10.3.1	
9	Get a list of contact points from CSP for security incident response and ensure CSP will inform the University when the list changes	10.4.1	
10	Ensure CSP will provide an incident report and provide information to the University for investigation within reasonable time upon the confirmation of security incidents occurring in the CSP's cloud environment which have impacted the University's service	10.4.2	
11	Ensure the access to audit logs shall be strictly controlled and all audit logs are tamper-resistant to prevent unauthorized modification	10.6.1	
12	Ensure secure protocols, such as TLS, Virtual Private Network (VPN) or dedicated connections has been implemented for end-to-end data transmission between the Cloud and the University	10.8.1	
13	Ensure network-level access controls has been implemented to prevent unauthorized access	10.8.1	
14	Ensure hardening has been performed to remove or disable all unnecessary configurations, services and ports on cloud system components	10.9.2	
15	Ensure the VM images and snapshots will be handled with care as they may contain capture of CONFIDENTIAL data on the system at the time the image/snapshot was taken	10.9.2	
16	Ensure the same level of protection and compliance controls apply to CSP's sub-contractors	10.10.1	

17	Ensure CSP has provided the procedures to retrieve the University's data/virtual instances and securely remove the data and virtual instances from the CSP's environment when the cloud service is terminated	10.10.2	
18	Ensure CSP complies with relevant industry standards and provides the latest certificates/audit reports for the University to review whenever the certificates/audit reports have been renewed	10.11.1	

ISMS-ISPS-020	Cloud Security Standard (For Departments)	Page <b>17</b> of <b>17</b>
INTERNAL		Version: 1.0

### **11.3 Appendix C: Reference**

- This Standard is prepared with reference to the following documents :Information Security Policies (ISMS-ISPS-001)
- Network and Platform Security Standard (ISMS-ISPS-010)
- Information System Acquisition, Development and Maintenance Standard (ISMS-ISPS-012)
- Logical Access Control Security Standard (ISMS-ISPS-011)
- Information Security Incident Management Standard (ISMS-ISPS-014)
- Business Continuity Management Standard (ISMS-ISPS-015)
- Password Management and Multi-factor Authentication Policy
- Practice Guide for Cloud Computing Security [ISPG-SM04], the Government of Hong Kong Special Administrative Region;
- Information technology – Security techniques – Information security management systems – Requirements, ISO/IEC 27001:2022, dated 25 October 2022;
- Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144
- Application Container Security Guide, NIST Special Publication 800-190
- Cloud Controls Matrix, Cloud Security Alliance (CSA)
- "Privacy Risks of Cloud Computing" -- Privacy Commissioner's article contribution at Hong Kong Lawyer (December 2019)
- Cloud computing (Information leaflet, July 2015), PCPD