# CITY UNIVERSITY OF HONG KONG
# Supplier Management Standard

---

*(Approved by the Information Strategy and Governance Committee in January 2023)*

## Document Control

| Document Owner | Classification | Publication Date |
|---|---|---|
| CSC | INTERNAL | 2023-01-28 |

## Revision History

| Version | Date | Summary of Changes |
|---|---|---|
| 1.0 | 2013-12-19 | Initial Release |
| 1.1 | 2015-06-19 | Typo corrections and multiple rephrases<br>For multiple activities, actor changed from “CSC” to “CSC/ESU” to reflect actual practice<br>Allowed disclosure of information only if “as required and permitted by the contract terms of the University”<br>Removed requirement for NDA for exchanging “INTERNAL” information which is not sensitive |
| 1.2 | 2023-01-28 | Revised the link and reference material in this document. |

## Distribution

| Copy | Issued to | Location |
|---|---|---|
| Master | Public | https://www.cityu.edu.hk/csc/information-security/information-security-policies-and-standards |

# Contents

# 1 Policy Statement

The City University of Hong Kong ("University") must ensure that IT related products and services delivered by suppliers and their practices on information security are compliant with the University's information security policy.

# 2 Objective

This standard is established to provide guidelines for the University to achieve the goals of information security in the supplier management process. This standard applies to the evaluation, monitoring, and controlling of suppliers to ensure provision of seamless and quality service

# 3 Roles and Responsibilities

Details procurement and tendering procedures are documented in "Financial Policies and Procedure Manual" of the University. The table below describes the information security related roles and responsibility of different parties at different stage of the purchase cycle.

| **Stages** | **Roles** | | |
|---|---|---|---|
| | **User Departments** | **CSC/ESU** | **Office of the Chief Information Officer** |
| **Identify Needs** | | | |
| All Products or Services | • Aware and conform to "Information Security Policies and Standards" and Information "Security Standard for Suppliers"<br>• Identify information used in services<br>• Classify information used<br>• Identify mode of service,<br>  ○ On-site Service,<br>  ○ Supplier is hosting/housing University's information,<br>  ○ Supplier has access to University's Internal Network and Servers<br>• Specify security requirements and controls in service specifications | | • Propose and maintain "University's Information Security Policies and Standards" and "Information Security Standard for Suppliers" and submit to ISGC for endorsement<br>• Assists in identifying information and classifying information<br>• Provide advisory services on security requirements and corresponding security controls |

| **Stages** | **Roles** | | |
|---|---|---|---|
| | **User Departments** | **CSC/ESU** | **Office of the Chief Information Officer** |
| IT Products or Services which will be hosted in the University or access to Networks or Servers of the University | • Liaise with CSC/ESU to have an initial understanding to suitability and compatibility to the University's IT Infrastructure and Requirements | • Provide advice and verify suitability and compatibility of service to the University's IT Infrastructure and Requirements | |
| **Approved Requisitions by Budget Controller** | | | |
| All Products or Services | • Include cost for security requirements and controls when preparing and approving budget | | • Provide advice on security requirements and controls |
| **Quotation/ Tendering Assessment & Approval** | | | |
| For any products or services that handle or use "CONFIDENTIAL" or "RESTRICTED" information of the University | • Consider suppliers' ability in handling sensitive information of suppliers when evaluating suppliers<br>• Notify CSC if purchase value is over HK$500,000. | | • Provide advice on supplier selection and evaluation |
| IT Products or Services which will be hosted in the University or access to Networks or Servers of the University | • Liaise with CSC/ESU ensure suitability and compatibility of suppliers' proposed services to the University's IT Infrastructure and Requirements | • Provide advice and verify suitability and compatibility of suppliers' proposed services to the University's IT Infrastructure and Requirements | |
| **Issue of Purchase Order/Contract** | | | |
| All Products or Services that handles or uses "CONFIDENTIAL", or "RESTRICTED" information | • Sign Mutual NDA with Supplier before exchanging any "CONFIDENTIAL", or "RESTRICTED" information with supplier | | |

| **Stages** | **Roles** | | |
|---|---|---|---|
| | **User Departments** | **CSC/ESU** | **Office of the Chief Information Officer** |
| **Receiving of Goods & Services** | | | |
| For all Services | • Monitor and ensure compliance to applicable policies of the University, including but not limited to "Data Privacy Policy", "Information Security Policies and Standards"<br>• Monitor and ensure compliance to applicable legislations, including but not limited to PDPO | | |
| For all Departmental managed Online IT Services | • Liaise with CSC/ESU and ISU to conduct vulnerability assessment before launch of services.<br>• Manage risks before service launch | | • Conduct tool-based vulnerability scanning<br>• Provide consultation service on risk management |
| For all Online IT Services managed by Central IT | • Liaise with CSC/ESU and ISU to conduct vulnerability assessment before launch of services<br>• Manage risks before service launch | • Conduct tool-based vulnerability assessment<br>• Revert findings to user departments<br>• Provide consultation service on risk management | • Conduct tool-based vulnerability scanning<br>• Provide consultation service on risk management |

# 4 Impact Analysis

Impact analysis is required to be conducted for all new products or services that will handle or use “CONFIDENTIAL” and/or “RESTRICTED” information of the University, and requires "4 or more written tenders".

Impact analysis is a process to determine:

- Processes impacted by the new product or service (manual or automated);

- Details of type and sensitivity of information impacted;
- Availability requirement for the new product or service;
- Risk of the product or service(If applicable);
- Additional information security requirements needed to safeguard the data (regardless of hosting location), if information impacted is sensitive or specifically protected by laws
- Requirements needed to limit access and safeguard data transmission, storage, and retention, if the system/ application/process is developed, outsourced and/or hosted at a supplier's location

Information Security Unit is responsible for ensuring the appropriateness of impact analysis process and providing advice on the risk management strategy.

The result of impact analysis shall be reviewed by User departments, CSC/ESU and Information Security Unit to ensure the suitability of new services.

# 5 Supplier Selection

When selecting and evaluating suppliers for services or products which involves the handling of "CONFIDENTIAL" and/or "RESTRICTED" information, the following aspects and capability of supplier shall be considered:

- Maturity of supplier's information security policies, standards, and procedures
- Security protections in architecture, including network, application, server, remote access, etc.
- Configuration management, such as patches, baseline security configurations, etc.
- Security features in product design, such as features for compliance to PCI-DSS, security measures against common web application vulnerabilities, etc.
- Access control mechanisms in the product
- Monitoring and ability of the supplier in detecting abnormalities
- Physical security if the service or product is hosted under supplier's location
- Contingency plan, disaster recovery objectives and disaster recovery capability
- Data ownership, such as confidentiality agreements, and data removal requirements up on termination of services, and etc.

When the purchase value of a service or product is over HK$500,000, and the service or product will involve the handling of "CONFIDENTIAL" and/or "RESTRICTED" information, the User Department shall notify the Computing Services Centre ("CSC"). The CSC shall provide advice in supplier selection and evaluation.

# 6 Supplier Contracts

Before using the supplier's services or products, the University shall establish and sign a contract with the supplier.

A Statement of Work ("SOW") or Scope of Service ("SOS") must be established by the University in each contract to clearly state the products, services and deliverables provided the supplier.

The contract must also clearly state the security requirements or the supplier to ensure that their products or services are consistent with the University's Information Security Policies and Standards.

The following terms and conditions shall also be included in the contracts:

- The supplier shall observe laws and the University's policies for privacy, copyright and security;
- A mutual non-disclosure agreement ("NDA") shall be established between University and suppliers if sensitive information (any information classified as "CONFIDENTIAL" or "RESTRICTED") is used, stored and processed by the supplier;
- The supplier must use the University's sensitive information only for the purpose for which the University is entrusted to it.
- The supplier shall prevent disclosure of the University's sensitive information to other third parties including subcontractors, except as required and permitted by the contract terms of the University.
- Where subcontracting is allowed, the supplier's agreement with subcontractor should impose the same obligations in relation to processing on the subcontractors as are imposed on the supplier by the University; and the supplier shall remain fully liable to the University for the fulfillment of the imposed obligations.
- The supplier shall define a plan, subject to acceptance of the University, for the handling, return and destruction of the University's sensitive information upon completion of the contractual requirements in accordance with the University's "Information Classification and Handling Standard".
- The supplier shall implement formal procedures to grant and remove authorization permission to its staff and subcontractor for accessing to the University's sensitive data based on "need-to-know" and "need-to-use" basis.
- The supplier shall ensure that its relevant staff will carry out the security measures and comply with the obligations under the contracting regarding the handling of sensitive information.
- The supplier is responsible for immediately reporting to the University of any sign of abnormalities and working with the University in recovery and remediation, in event of security breach.
- If "CONFIDENTIAL" or "RESTRICTED" information will be hosted in the supplier's location, the University should have the rights to carry out periodic security assessment and inspect how the supplier handles and stores the University's sensitive information within a mutually agreeable time to both parties; or the supplier shall provide security audit or assessment reports issued by qualified independent professionals and organizations.

- The consequence for violation of the contract.

The User department shall also ensure that a Service Level Agreement ("SLA") is established in the contract.

# 7 Supplier Control and Monitoring

The User Department shall carry out regular monitoring on the performance of supplier and review the security level achieved by the supplier. The evaluation on performance of suppliers shall cover:

- Complaints, incidents, problems (e.g. service interruption, security breach, degradation of service level) encountered by the supplier;
- Contingency plan in the event the supplier cannot provide the services

If agreed service level is not attained, or the supplier is providing non-conforming products/ services, User Department and Finance Office shall discuss with the supplier for rectification. Records of discussion and follow-up plan shall be prepared for monitoring purposes.

If non-conformance persists, User Department and Finance Office can consider contract termination.

# 8 Service Transition

The User Department shall ensure that quality of service is attained and security risks are managed during and after service transition.

# 9 Service Termination

Upon termination of contracts, the User Department must inform suppliers to return or destroy all relevant data and resources of the University and require formal acknowledgement.

User Department shall ensure that the quality of service is attained and security risks are managed during and after transition of service back to the University.

# Reference

The following documents were consulted during the preparation of this document:

City University of Hong Kong (2022), *Financial Policies and Procedure Manual*
https://www.cityu.edu.hk/fo/stafflan/htm/FPPM_FO.htm

GE Internal (2007), *General Electric Third Party Information Security Policy*

Fujitsu (2012), *Information Security Enhancement Measures in Cooperation with Suppliers*

Oracle (2012), *Oracle Supplier Information and Physical Security Standards*