CITY UNIVERSITY OF HONG KONG
Compliance Management Standard

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

Document Control

Document Owner	Classification	Publication Date
OCIO	PUBLIC	2023-01-28

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial Release
1.1	2015-06-19	Replaced “IT Security Officer” with “Information Security Unit” Allowed disclosure of information only if “as required and permitted by the contract terms of the University” Modified to allow asset/process owners to report noncompliance to “University’s management” as well as ISU
1.2	2023-01-28	Revised the link in this document. Added applicable legislations and regulations (PDPO amendments, GDPR & PIPL) in section 3.1.

Distribution

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

Contents

1 Policy Statement

The City University of Hong Kong ("University") shall ensure full compliance with all legal, statutory, regulatory and contractual requirements that are applicable to the operations of the University.

2 Roles and Responsibility

2.1 Information Security Unit (ISU)

- Check for updates or additions to the relevant legal, statutory, regulatory or contractual requirements that the University needs to comply
- Coordinate with the asset or process owners of relevant University Units in the identification and implementation of compliance process within the University
- Develop, maintain and monitor implementation of Compliance Management Standard
- Follow up on noncompliance and escalate to senior management of the University

2.2 Asset or Process Owners

- Inform the ISU of any updates or additions to relevant law, statutory, regulatory or contractual requirements that his or her responsible Unit needs to comply
- Update the inventory of contracts relevant to his or her responsible asset or process
- Communicate the responsibilities for compliance with relevant law, statutory, regulatory or contractual requirements to the staff, students or contractors under his or her responsible Unit
- Report any noncompliance to the University's management and/or ISU

2.3 Legal Counsel

- Provide professional advice regarding the compliance issues encountered by the University
- Assist the impact assessment of noncompliance or deviations noted around the compliance status of the University

2.4 All staff of the University

- Comply with all applicable legal, statutory, regulatory and contractual requirements

3 Compliance Management for Legislation

3.1 Applicable Legislations and Regulations

The following is a list of legislations related to the protection of information security in the University:

Legislation & Regulations	Regulatory Bodies
Telecommunications Ordinance (Cap. 106)	Communications Authority (CA)
Unsolicited Electronic Messages Ordinance (Cap. 593)	Communications Authority (CA)
Personal Data (Privacy) Ordinance (Cap. 486) and its Amendments	Privacy Commissioner for Personal Data (PCPD)
Copyright Ordinance (Cap. 528)	Intellectual Property Department (IPD)

Employment Ordinance (Cap. 57)	Labour Department (LD)
Crimes Ordinance (Cap. 200)	Department of Justice (DOJ)
Theft Ordinance (Cap. 210)	Department of Justice (DOJ)
Electronic Transactions Ordinance (Cap. 553)	Office of the Government Chief Information Officer (OGCIO)
General Data Protection Regulation (GDPR)	European Union (EU)
Personal Information Protection Law (PIPL)	Mainland China

Overseas units and offshore units of the University must also comply with all applicable laws and regulations from all applicable jurisdictions.

3.2 New Legislation

Whenever there is a new legislation related to information security, the ISU shall perform an assessment of their applicability to the University. The ISU should seek clarification from the regulatory body as necessary.

For the relevant legislations, the ISU shall initiate the implementation of the new standards. All members of the University shall be informed of the new legislation and the actions taken by the University to achieve compliance.

The Management of the University shall be informed of any new legislations and reviews the corresponding actions taken by the University.

3.3 Update to Existing Legislation

The ISU shall check for updates to the above legislation on a monthly basis. The ISU should regularly visit the web pages of relevant regulatory organizations, subscribe to relevant web sites or consult the Legal Counsel and relevant administrative units of the University.

Upon identification of any changes to the above legislation, the ISU shall perform an assessment of their applicability to the University. The ISU should seek clarification from the regulatory body as necessary.

For applicable changes, the ISU shall drive the implementation of the revised policies, standards, procedures and guidelines by coordination with respective University Units or third parties.

The Management of the University shall be informed of any updates to the existing legislations and reviews the corresponding actions taken by the University.

3.4 Monitoring

The Asset/Process Owners shall monitor the information security compliance status of the legislations applicable to their responsible area. The ISU shall provide guidance to relevant queries raised by the Asset/Process Owners and consult the Legal Counsel of the University when necessary.

Any noncompliance noticed shall be reported to the University's management and/or ISU who will then escalate to the University's senior management and handle according to the "Information Security Incident Management Standard".

4 Compliance Management for Contractual Requirement

4.1 Establishment of Contractual Requirement for the University

When sensitive information is provided to third party vendors, the written contractual requirement shall include the following terms at minimum:

- Require all contractors, consultants, or external vendors to observe laws and the University's policies for privacy, copyright and security;
- Prevent disclosure of sensitive information to other third parties including subcontractors, except as required and permitted by the contractual terms of the University;
- Require a plan for the handling, return and destruction of sensitive information upon completion of the contractual requirements in accordance with the University's "Information Classification and Handling Standard";
- Require access or authorization permissions for the fulfillment of contractual requirements to be specified. These permissions should be terminated once the contractual obligations have been completed; and
- Require compensation plan for any noncompliance noted.

4.2 Contractual Requirement Required by Third Party Vendors

When the third party vendors' sensitive information is provided to the University, the Asset/Process Owner shall initiate the review of relevant contractual requirements in relation to the protection of such information. The Asset/Process Owner and the ISU shall determine whether the University's information security policies, standards and procedures (e.g. "Information Classification and Handling Standard") are sufficient to fulfill such contractual requirements, or whether any additional actions should be taken.

4.3 Monitoring

The Asset/Process Owners shall monitor the information security compliance status of the contractual requirements applicable to their responsible area. The ISU shall provide guidance to relevant queries raised by the Asset/Process Owners and consult the Legal Counsel of the University when necessary.

Any noncompliance noticed shall be reported to the University's management and/or ISU, who will then escalate to the University's senior management, and handle according to the requirements established in "Information Security Incident Management Standard".