CITY UNIVERSITY OF HONG KONG
Information & IT Asset
Inventory and Ownership 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	2013-12-04	Initial Release
1.1	2015-06-19	Typo corrections Definition of Information asset corrected to both "IT and non-IT asset" Added elaborations of terms "Information Owners", "IT Asset Owners", "Information Delegates" and "IT Asset Delegates" Empowered "delegates" to propose classification of information, and suggest control measures
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/cio/information-security/information-security-policies-and-standards

Contents

1   Policy Statement

The City University of Hong Kong ("University") shall achieve and maintain appropriate protection of its information related assets. This standard outlines the specific requirements and guidelines for the implementation of Section "2) Information & IT Asset Inventory and Ownership" in the "Information Security Policies".

2   Objective

The objective of this standard is to establish the responsibility and management system of information related assets within the University. All the University members who may possess, access or use information related assets of the University are expected to familiarize themselves with this Information & IT Asset Inventory and Ownership Standard and follow it consistently.

3   Terms and Definitions

Asset

Asset is anything that has value to the University. There are many types of assets, including:

- information;
- software, such as a computer program;
- physical, such as computer;
- services;
- people, and their qualifications, skills, and experience; and
- intangibles, such as reputation and image.

IT asset

IT asset is the asset that related to the processing of digital information. Types of IT asset include hardware, software, digital storage media, IT services, etc.

Information asset

Information asset can be IT asset and non-IT asset. Information assets are knowledge and data that are of value to the University regardless of form or format.

Information resources

All data and information, as well as the hardware, software, personnel and procedures on collecting, storing, processing and generating of such data and information. This includes data networks, servers, PC's, storage media, printers, photo copiers, fax machines, supporting equipment, and back-up media.

The terms "Information Owners" and "IT Asset Owners" would be used, when the owners of asset are referred in the context of "Information" or "IT Asset".

The terms "Information Delegates" and "IT Asset Delegates" would also be used, when the delegates of asset are referred in the context of "Information" or "IT Asset".

4   Asset Management and Identification of Asset

Information and IT assets are owned by the University irrespective of their values, expected life-spans and fund sources. All tangible assets, including IT and other asset types, of the University must be managed in accordance with the "Financial Policies and Procedure Manual" of the University.

Management of Software Assets must also conform to "Software Asset Management" guidelines and policies of the University.

The University shall identify all the information and IT assets, including all tangible or intangible assets.

All Owners and Departmental Coordinators of Information and IT assets are responsible for maintaining an up-to-date IT Asset Register in the Department.

5   Responsibilities

Clearly defined responsibilities are needed for proper management and protection of the University's Information and IT assets.

Any staff members who failed to "use and manage University resources properly and responsibly" may be liable to disciplinary action or other appropriate actions by the University, as stated in the Code of Conduct in the Staff Handbooks.

This is achieved by establishment of the following roles:

5.1   Asset Owners

The Asset Owner shall be accountable for the assets assigned to him or her, and responsible for:

- Identifying the classification levels of all owned assets, by assessing the level of sensitivity and criticality of the assets;
- Understanding the principal risk associated with each asset and specifying the additional control measures required if needed;
- Periodically reviewing the appropriateness of classification;
- Defining and implementing appropriate safeguards to ensure the confidentiality, integrity, and availability of the assets;
- Monitoring safeguards to ensure their compliance and report situations of noncompliance;
- Authorizing access to those users who have a business need for the assets;
- Removing access privileges from those who no longer have a business need for the information;
- Implementing corrective and preventive actions to rectify non-compliance;
- Delegating responsibilities with clear instructions for implementing or maintaining controls to staff/subordinates reporting to him/her, however, the accountability still rest with the owner;

Head of Units are the asset owners and are accountable for unit level assets.

5.2 Asset Delegates

Asset Delegates are usually the administrative members of asset owners' units, and are responsible for:

- Proposing the classification levels of all delegated assets for asset owner's approval;
- Understanding the principal risk associated with each asset and suggesting the additional control measures required if needed;
- Periodically reviewing the appropriateness of classification;
- Maintaining the assets;
- Following the Asset Owner's instructions for handling or managing the assets;
- Suggesting appropriate technologies and procedures to the Asset Owner;
- Implementing security mechanisms;
- Performing backups regularly on Information or Software Assets and restoring data from backup copies when required; and
- Following the Asset Owner's instructions for maintaining the IT Asset Register.

5.3 Asset Users

An Asset User can be a member of the University or a third party that has access to and uses the assets of the University for performing his or her job responsibilities.

Asset Users' are responsible for:

- Obtaining authorization from the Asset Owner before accessing or using the asset;
- Adhering to security controls put in place by the Asset Owner and by the University's management; and
- Reporting any information security incidents to Asset Owner.

5.4 Information Security Unit

Information Security Unit is responsible for:

- Maintaining Information & IT Asset Inventory and Ownership Standard;
- Providing assistance to units on preparing and maintaining of IT Asset Register; and
- Verifying that the IT Asset Register is properly maintained by the Asset Owners.

6   Types of Asset

6.1   Information and IT Asset Categories

Assets are objects owned by the University with values for business operations. The Information and IT assets are grouped under the following categories:

Categories	Descriptions
Information Assets	Information of the University such as database and data files, documentation, contracts and agreements, research information, user manuals, operational procedures, archived information, etc. These in turn will be stored on various types of media including papers, magnetic tapes, hard disks, USB Flash memory drives, floppy disks, etc. Information of the University that is under the control or custody of contractors, or information of contractors that is under control or custody of the University is also included.
Software Assets	Those e-learning courseware, applications and system software/licenses used within the University.
Physical Assets	Visible and tangible equipment such as computer equipment, network communication equipment, storage media, etc.
Service Assets	Services which provided by combining resources and capabilities to user, such as Email service, Online Facilities booking service, etc.

6.2   Information Classification

The classification standard is described in "Information Classification and Handling Standard".

7   IT Asset Register

All University Units shall prepare and maintain an IT Asset Register. The register includes Information Assets, Software Assets, Physical Assets and Service Assets.

All University Units shall also assign staff member(s) to establish, maintain and safeguard the asset, review the IT Asset Register bi-yearly and arrange re-assess of asset classifications, if necessary, and update the asset inventory with newly purchased assets and the classification levels.

When necessary, the University Units may create separated Asset Registers for "RESTRICTED" and/or "CONFIDENTIAL" assets, if the knowledge of presences of such assets is sensitive and shall only be known by limited group of authorized staff.

The following attributes should be recorded for each information asset in the IT Asset Register:

- **Asset name**
  This is a collective name which represents a group of assets with similar natures and functions sharing the same "Description", "Classification" and "Value".
  For instance, a single entry "Office Desktop Computers" could be used to represent all desktop computers for staff members of a unit.

- **Asset category**
  "Information", "Physical", "Software", and "Service" assets shall be included in the IT Asset Register; optionally "People" and "Intangible" assets may also be included.
  For instance, asset category of "Office Desktop Computers" is "Physical".

- **Asset Description**
  A short statement which describes the type or purpose of use of the asset, e.g. "Desktop computers used by staff members in Office" could be a description for "Office Desktop Computers".

- **Asset Owner**
  An owner (or delegate) is a staff member or a unit who has final responsibility for the security of the asset. In particular, the owner will be responsible for granting, revoking and reviewing the access to the asset.

- **Asset Delegated to**
  Roles or employees designed by the Owner to access information for implementing and/or maintaining safeguards and controls. The accountability rest with the Asset Owner.

- **Classification**
  To ensure the proper protection of asset, the owner (or delegate) shall classify assets into one of the following classifications: "RESTRICTED", "CONFIDENTIAL", "INTERNAL", and "PUBLIC".

- **Asset Value**
  A qualitative value of the asset:

High	This asset is critical to business operations. The loss of confidentiality, integrity or availability of the asset will cause serious or significant consequences to business operations and legal position.
Medium	This asset is important to business operations. Detrimental, legal breach and damage/embarrassment which could be resulted if the asset is damaged or its confidentiality, integrity or availability is/are lost.
Low	This asset is useful to business operations. The loss of confidentiality, integrity or availability of the asset will have minimal or little business, legal damage or embarrassment.

- **Remark**
  A statement that provides additional details about the asset.

8   Reclassification

The University Units shall schedule bi-yearly a review process for all assets classified and reclassified if the impact of loss of confidentiality, integrity and availability changed. The Asset Owners may also change the classification when the impact changes.

Upon changing the classification the Units or Owners will increase, decrease, or remove the classification as appropriate.

9 Summary

To implement asset inventory and ownership, the University shall acquire or dispose of all its information and IT assets in accordance with the relevant asset acquisition and disposal policies within the University. An inventory list of important assets associated with information resources must be documented and maintained for recording purpose. In addition, roles, responsibilities and accountabilities are also needed for proper management and protection of the University's information and IT assets.

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

City University of Hong Kong (2022) *Software Asset Management, Guidelines on Compliance of Intellectual Property Ordinance*,
https://www.cityu.edu.hk/policies/ippolicy/software-asset-management

City University of Hong Kong (2023), *Information Security Policies*

City University of Hong Kong (2023), *Information Classification and Handling Standard*

City University of Hong Kong (2023), *Change Management Standard*

City University of Hong Kong (2013), *Code of Conduct*, 3 Jan 2011 (last updated on 13 Nov 2020),
https://www.cityu.edu.hk/hro/download/stafflan/admnote/cod_appendix_1.pdf