CITY UNIVERSITY OF HONG KONG
Physical Access Security Standard

(Approved by the Information Strategy and Governance Committee in December 2013)

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	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 or hereinafter referred as the “University” must ensure that unauthorized physical access to IT infrastructures, information, and information systems of the University are prohibited. These include the setups of all University Units.

2 Objective

The objective of this document is to govern physical security controls protecting information and information facilities of the University from unauthorized access, damage, and interference.

3 Securing Work Areas

Work areas are broadly referred to Offices, Rooms, Facilities, and Secure Area of the University.

Work areas shall be protected by security perimeters with limited entry and exit points, while fulfilling relevant health and safety regulations and standards.

The perimeter should be physically sound. There should be no gaps in the perimeter or areas where a break-in could easily occur. The external walls should be of solid construction and all external doors should be protected against unauthorized access using appropriate control mechanisms such as alarms, locks, CCTV, etc.

Suitable intrusion detection systems should be professionally installed and regularly tested to cover premises.

General buildings, offices, rooms and facilities should be protected by ensuring that all doors and windows remain closed and locked while unoccupied. Manned reception desks should be used to restrict access to offices of supporting and servicing units containing confidential information.

Critical equipment and information should be placed in secure areas (such as filing cabinet rooms, printing rooms, computer rooms, and data centers). Access areas to secure should be restricted to authorized personnel only.

The cost of implementing protection measures should commensurate with the identified level of acceptable risk.

Personnel should only be aware of the existence of, or activities within, a secure area on a need-to-know basis

Personnel of contracted third party service providers should be given restricted access to secured rooms and this should always be under supervision unless CCTV camera equipment monitoring the rooms.

4 Physical Entry Controls of Secure Area

Secure areas should be protected to ensure that they are only accessible to authorized personnel. Entry to secure areas should be handled as follows:

- Entrance of secure areas must be controlled by physical token, e.g. access control card, assigned to onsite personnel or authorized staff only;
- Visitors, including staffs and contractors, must be authorized before entering secure areas; access should be granted for specific, authorized purpose only and their access being recorded;
- Approval records and access log must be preserved
- Onsite personnel should wear physical badge;
- Visitors should wear physical visitor badges unless they are escorted by authorized staff of the University or onsite personnel who is wearing a badge;
- Visitor badges must be surrendered before leaving the secure areas;
- Moving of materials and equipment into and out of site must be escorted by onsite personnel, inventory being checked and logged;
- Transfer log shall be used to maintain a physical audit trail of change in equipment. Onsite personnel or authorized staff should document the following:
    - Owner, controller or custodian responsible for the equipment
    - Report number, Model number and Serial number equipment if available
    - Time in or out
    - Name of transferor
- Visitor log shall be used to maintain a physical audit trail of visitors’ activities. Retain this log for a minimum of three months. Onsite personnel or authorized staff should verify the identify and documents the following of visitors:
    - Name
    - Organization or company represented
    - Time in and out
    - Purpose of visiting
    - Signature of visitor
    - Signature of verifier
- System owner, custodian or controller should indicate the Information Classification and/or security requirements of equipment in secure area;
- Access to equipment in secure area shall be granted by system owner, custodian or controller
- Equipment Access log shall be used to maintain a physical audit trail of visitors activities. Onsite personnel or authorized staff should document the following:
    - Name
    - Equipment (e.g. Cabinet or Rack identifier)
    - Time start and end
- Visitor log and Equipment Access log should be regularly reviewed by Management to detect any unauthorized or inappropriate access
- CCTV cameras should be installed to monitor the access activities of secure areas. Access control and retention policy of recorded media should be defined and followed.

5 Equipment Security

Equipment should be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access and equipment theft.

Equipment, information or software should not be taken off-premises without prior authorization.

Appropriate security measures should be applied to equipment placed in public (e.g. Express Terminals) and area off-site equipment, taking into account the various risks of working

Appropriate power protection (e.g. Uninterruptable Power Supplies, Redundant Power Feeds), adequate fire protection, proper heating and cooling should be installed to prevent interruption of service or availability.

Maintenance contracts should be in placed to ensure that equipment will be correctly maintained.

6 Responsibilities

Clearly define responsibilities are needed for proper management and protection of physical access to the University's sensitive information and information processing facilities. This is achieved by establishment of the following roles:

6.1 System Owner, Controller, and Secure Area Personnel

- Authorize, control and monitor visitor's access to secure area, protected equipment, and information processing facilities;
- Control working in server area;
- Review and update access rights to secure area regularly;
- Control the physical security perimeter for secure area;
- Implement the physical entry controls for secure area;
- Control the isolated delivery and loading area for secure area; and
- Review the processes involved in the above protections.

6.2 Authorized Staff with Access to Sensitive Information and Facilities

- Escort authorized visitors within secure area; and
- Challenge and report any un-escorted strangers or anyone not wearing visible identification.

6.3 Visitors

- Comply with physical security standards of the University; and
- Obtain approvals from relevant management prior to access to the University's sensitive information or information processing facilities.

7 Summary

The University must restrict the physical access to its sensitive information and information processing facilities. Physical access rights are only granted on a need-to-know basis. Visitor logging must be implemented and access logs should be reviewed regularly.

Reference

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

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

City University of Hong Kong (2023), *Environmental Security Standard*