CITY UNIVERSITY OF HONG KONG
Environmental Security 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	2023-01-28	Revised the link 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 protect its information systems, information resources and members from environmental hazards or threats, including but not limited to:

- Fire
- Water leakage
- Power surge / loss
- Electric shocks
- Typhoon
- Earthquake
- Explosion
- Civil unrest

2 Objective

The objective of this standard is to describe the mechanisms and requirements to achieve the environmental security in the data center / server room(s) of the University.

3 Equipment Security

Computing equipment should be placed away from glass windows (unless additional window protection, such as tempered glass and curtains are in place) to avoid the computer equipment being revealed by outsiders and various natural disasters such as fire and typhoon.

Computing equipment should be properly installed in server room(s) to avoid accidental knock down.

Computing equipment should be sited away from risk of fire, explosives, water, dust, chemicals, electromagnetic radiation.

Eating, drinking and smoking must not be allowed near the University's computing equipment. Flammable materials must not be brought into the server room(s). Members causing damage to equipment due to spillage or other associated issue may be responsible for the cost of repair or replacement. Serious damage to equipment caused by professional negligence of staff shall be recorded, and should be used as criteria to be taken into account when considering promotion.

4 Cabling Security

Cable lines used by the University's information systems and infrastructures must be installed in a managed, clean and tidy manner.

Wherever possible, power and telecommunication lines should be installed in high level (e.g. ceiling) to allow better ventilation and should not route through public area without proper protection. For existing premises that overhead cabling cannot be implemented, power and telecommunication lines should be protected by ducting from source to sockets.

5 Temperature and Humidity Control and Monitoring

7 x 24 air conditioning equipment with temperature and humidity adjusting functionality must be implemented within the server room(s) of the University. The air conditioning must be configured to maintain the room temperature and humidity within normal operating range of server hardware and other computing devices.

Sensors should be installed within the server room(s) of the University to monitor the room temperature and humidity on a real-time basis. Alerts on abnormal temperature and humidity should be automatically communicated to IT operation staff on a timely basis.

Regular test of air conditioning equipment, temperature and humidity controls and monitoring devices should be conducted at least annually to ascertain their effectiveness.

6 Power Protection

The University shall provide power protection to ensure that the availability of its information systems. All sensitive and critical information processing systems shall be equipped with Uninterruptible Power Supply ("UPS"). All critical applications shall be configured to switchover to an alternative power source (e.g. backup power generator or electricity power from other facilities) immediately upon loss of power.

UPS should be tested at least annually to ascertain that the battery life can sustain a clean shut down of the University's critical information systems or holds the necessary loads until the disaster recovery site is in operation.

Regular monitoring of the output load of UPS should be performed to avoid and detect overloading issue. Physical access to UPS facility, including battery and cable connection, must be restricted to authorized personnel.

7 Fire, Smoke and Water Detection and Control

Fire, smoke and water detectors must be properly installed within the server room(s) of the University to protect computing equipment from environmental hazards.

Wherever possible, gas-based automatic fire suppression system (e.g. FM 200) should be implemented to suppress fires without damaging the computing equipment. Appropriate segmentation of fire suppression systems should be used so that a fire in one area will not activate all systems in the server room(s). In addition, regular inspection of fire suppression system should be performed by the vendor at least annually.

Hand-held fire extinguishers should be strategically placed within the server room(s). Signage should be used to clearly indicate the location of hand-held fire extinguishers. Regular inspection of fire extinguishers should be performed at least annually.

Raised floor should be deployed in the server room(s). Water detectors should be placed under the raised floor to provide effective detection on water leakage.

Alerts on occurrences of environmental hazards should be automatically communicated to IT operation staff immediately.

Regular test of fire, smoke and water detection and control devices should be conducted at least annually to ascertain their effectiveness.

8 Pest Control

Server room(s) must be maintained in good sanitation to prevent pest problems. No food should be kept inside the server room(s). Waste bags must be disposed and trash bins must be emptied at least daily.

Electronic pest control devices should be used to eliminate or drive pests away from the server room(s).

9 Evacuation / Activation Process

Documented operating manuals must be established by the University for systems and devices related environmental security, including:

- Fire suppression system
- Hand-held fire extinguisher
- Fire, smoke and water detectors
- UPS
- Environment monitoring system

Adequate trainings should be delivered to members for correct operating and maintenance of these equipment and devices.

Activation criteria of above equipment and devices (other than automatic systems such as fire suppression systems) should also be stated in the operational manuals.

Evacuation criteria and procedures must be established by the University to protect human life in the presence of environmental hazard. Clear evacuation routes and signage should be placed in strategic locations within the server room(s). Please refer to the University's Disaster Recovery Plan for details.

10 Pandemic and Other Arrangements

The University shall prepare for pandemic and special arrangement such as chemical or gas leakage of laboring laboratories leading to inappropriate environment of areas housing IT facilities or inappropriate access to them. Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) should be prepared to handle these kinds of situation.

11 Summary

The University must ensure sufficient environmental protection mechanisms are deployed to meet its performance and uptime objectives. University's premises should be protected against possible environmental hazards to minimize the damage from fire, flood, wind, earthquake, explosion, civil unrest and other forms of natural and man-made risk. Proper BCP and DRP have to be prepared and drilled to prevent loss of business.