恒生管理學院
HANG SENG
MANAGEMENT COLLEGE

Hang Seng Management College

Information Security Policies

Prepared by

Information Technology Services Centre

Last Update: May, 2016

Table of Contents

Version

Date	Changes
2016.02	First complete version submitted to PDQAO as a supporting document.
2016.05	First version to be endorsed by ITAC and approved by the Director of Information Technology.

Executive Summary

This document defines the policies for information security in Hang Seng Management College. It describes the goals, objectives, strategies, governance, and roles and responsibilities for users, information managers, and system owners.

This document is developed based on core principles for information security management, as described in ISO/IEC 27002, and covers the following aspects:

Security Management

- Physical Security
- Network Security
- System Security
- Application Security
- Database Security

Information Management

- Asset Management
- Security Classification
- Access Control
- User Management

Risk Management

- Risk Management
- Incident Management
- Continuity Planning

This document is subject to annual review or whenever necessary. All policy changes must be approved and signed by the Director of the Information Technology (DoIT).

Overview

Information security is concerned with the confidentiality, integrity, and availability of data regardless of the form (e.g., digital or paper record), storage (e.g., server, PC, databases, portable storage), or transmission media (e.g., Wifi, Internet, file copy). Information resources are important assets which must be properly protected from intentional or unintentional viewing.

All personnel who have access to information assets have responsibility to protect them, and to minimize the risks that assets would not be leaked to unauthorized parties.

The College is committed to protect its networks, systems, applications, and data from unauthorized security threats, to safeguard the confidentiality, integrity and availability of all physical and electronic information assets of the college, and to ensure that regulatory, operational and contractual requirements are fulfilled.

This document provides a high level view of policies for information security in the Hang Seng Management College (the College). It is subject to annual review or whenever needed. All policy changes must be approved and signed by the Chairman of the Information Technology Advisory Committee.

Security Objectives

The overall objectives for information security at the College are the following:

- Ensure compliance with current laws, regulations and guidelines;
- Comply with requirements for confidentiality, integrity and availability for the College's employees, students and other users;
- Establish controls for protecting the College's information and information systems against theft, abuse and other forms of harm and loss;
- Motivate administrators and employees to maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents;
- Ensure that the College is capable of continuing their services even if major security incidents occur;
- Ensure the protection of sensitive personal data (privacy);
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by the College;
- Comply with methods from international standards for information security, e.g. ISO/IEC 27001;
- Ensure that external service providers comply with the College's information security needs and requirements;
- Ensure flexibility and an acceptable level of security for accessing information systems from off campus.

Security Strategies

- **Security Model** - The College defines its work on information security based on the popular CIA model:

Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Integrity	The property of safeguarding the accuracy and completeness of assets
Availability	The property of being accessible and usable upon demand by an authorized entity

- **Security Framework** - The College's current framework for information security for identifying, assessing, evaluating and controlling information-related risks will be governed by the policy items to be defined in this document.
- **Security Execution** - The execution of information security initiatives will be defined and ensured by a set of supplementary guidelines. In order to secure operations at the College after serious incidents, the College shall ensure the availability of continuity plans, backup procedures, defence against damaging code and malicious activities, system and information access control, incident management and reporting.
- **Security Priorities** - Some of the most critical aspects supporting the College's activities are availability and reliability for network, infrastructure and services. The College practices openness and principles of public disclosure, but will in certain situations considers the priorities involved in confidentiality, availability and integrity.
- **Security Compliance** - Every user of the College's information systems shall comply with this information security policy and relevant user guidelines. Violation of this policy and of relevant security requirements will therefore constitute a breach of trust between the user and the College, and may lead to serious consequences and legal actions.
- **Security Governance** – The implementation and compliance of information security is continuously monitored by the Information Security Working Group under ITSC, who will report to the Senior Management Committee on any security incidents and handling.

Roles and Responsibilities

The College has formed an Information Security Working Group under ITSC, with the Director of Information Technology as the Chairman. The Working Group works closely with academic and administrative departments to formulate roles and responsibilities of information users. The College will review from time to time and implement new governance structures if needed.

Owner of Security Policy

The Information Security policy is owned by the Information Security Working group at the time being. It will be reviewed once a year or whenever necessary (such as occurrence of security incidents, additions or changes of college policies). All policy changes must be endorsed and signed by the Director of Information Technology, and formally approved by the chairman of ITAC.

Information Owners

In general, information assets are owned by the respective departments who are responsible in collecting and managing these assets. Some examples include:

- Registry, SAO – Student-related Information
- HRO – Staff-related information
- AAAO – Alumni information
- FO – Finance and Payment-related information
- CDMO – Facilities and security-related information
- VPAR – Research and academic-related information

In consultation with the System Administrator (ITSC), information owners will assign and authorize information officers to access the information assets, including but not limited to data fields, durations, and access rights (i.e. read/add/modify/delete).

Information Officers

Information Officers are academic or administrative staff, usually within departments who are Information Owners. They are appointed by Information Owners and have access rights to manage the information assets. Their access rights are subject to approvals by the Information Owner(s), and they have to sign undertakings before they are granted access to the information assets.

System Administrators

ITSC is the custodian of information systems and assets. It works under the supervision of senior management and works closely with academic and administrative departments. ITSC designates its staff as system administrators who will set up, develop, update, and manage the information assets on behalf of information owners. As a result, system administrators are to be approved by Information Owners to manage the information assets. They need to sign undertakings in order to execute their duties, to work as a team member for and on behalf of the information owners.

Users

Users consume and process information. They are required to follow recommendations set by ITSC when accessing and processing information. In addition, they are advised to receive education on information security when available and applicable to them.

External Parties

External parties are vendors, consultants, and guests who help to set up and/or have access to our information systems. External users must agree and subject to our user polices, and partners must consult and seek approval from ITSC and compliant to our information security policies and guidelines.

Security Management

Security Management is to control and make decisions regarding security. ITSC is responsible for the development and/or setting up of information systems for Information Owners. The following security control management are taken into consideration during the development and deployment of the solution to safeguard information assets.

Physical Security

1. Physical Security refers to control of access of physical information facilities such as data centers, computer laboratories, office spaces, etc.

2. The control access is assigned solely to ITSC system administrators. The facilities are managed by CDMO with consultation and coordination from respective offices, under approval from senior management and/or SAFMC.

3. Contactless smartcard and card reader technologies are used to implement the control.

Network Security

1. Network Security refers to the control of information access via wired or wireless network.

2. The control is managed by system administrators, under approval from the Director of Information Technology.

3. Security network devices, such as firewall, UTM devices, are used to implement the control.

4. System administrators need to establish and manage network security policies so as to safeguard the network from hacking and external intrusion.

System Security

1. System Security refers to the control via computing systems, such as file servers, storage servers, and other system appliances.

2. The control is managed by system administrators, under approval from the Director of Information Technology.

3. Security control, such as user authentication and authorization, are used to implement the control.

4. System administrators need to establish and manage system security policies so as to safeguard the servers from hacking via internal/external intrusion.

Application Security

1. Application Security refers to the protection of our applications, either adopted solutions and self-developed system.

2. The control is defined by application developers and managed by system administrators, under consultation and approval from the information owners and the Director of Information Technology.

3. Security control, such as user authentication and authorization, are used to implement the control.

4. Application developers need to define access and security control policies for information users, officers, and owners to ensure confidentiality, integrity, and availability of information.

Database Security

1. Database Security refers to the control implemented in the database system.

2. The control is managed by the system administrator, under consultation and approval from the information owner.

3. Security control, such as user authentication and authorization, information encryption and logging, are used to implement the control.

4. System administrators and application developers will work with the information owners to ensure the security of the databases resided in the database system.

Information Management

Information Management involves definition and control of activities to protect information from unauthorized access, no matter they are connected internally or externally. Information assets can only be secure if it is properly managed, used, and controlled by both approving authority and system administrators.

Assets Management

1. Asset Management refers to the management of information assets such as servers, PCs, software, license, computer laboratories, etc.

2. It is managed by the system owner, under consultation and approval from the Director of Information Technology.

Information Classification

1. Information Classification refers to the classification of information based on confidentiality, integrity, and availability.

2. It is managed by the system owner, under consultation and approval from information owner in consultation with ITSC.

3. In general, information is classified into the following:

Classification	Nature and Examples
Public	Available to general public. e.g. College and program information, name, job title, serving unit, etc.
Restricted	Restricted to individual and/or unit e.g. Office works, research proposal and outputs, policy papers, minutes, student examination results, etc.
Private	Private to individual e.g. HKID, salary, spouse information, address, etc.
Confidential	Confidential to the College, senior management e.g. Board papers, staff appraisal, student evaluation, etc.

4. Various technology management controls are applied based on the classification.

Access Control

1. Access Control refers to information access control either physically or digitally.

2. It is managed by CDMO and/or system owner, under consultation and approval from respective committees and/or information owner.

3. Various technology management controls are applied based on information classification.

User Management

1. User Management refers to user account management.

2. It is managed by the system administrator, under management of information owners.

Risk Management

1. Risk Management refers to the identification, assessment, prioritization and related coordination to maximize/minimize the impact of positive/negative risk.

2. The goal is to classify and document how to handle different risks by:

Risk Handling	Treatment
Avoidance	Eliminate, withdraw from or not become involved
Reduction	Optimize/mitigate the positive/negative risk
Sharing	Transfer the risk via outsourcing or insurance
Retention	Accept and budget to handle the risk

Incident Management

1. Incident Management refers to how the College reacts to different unexpected events.

2. The goal is to manage the incident and formulate a long term solution acceptable to all stakeholders.

3. A separate document will cover more details on Security Incident Management.

Continuity Planning

1. Continuity Planning refers to process planned to be effective in the event of critical incident.

2. The goal is to minimize the time to resume services at reasonable cost.

References

1. ITSC Website (http://itsc.hsmc.edu.hk)
2. Information Security Guidelines
3. Acceptable Use of IT Services
4. HSMC User Non-Disclosure Agreement Form
5. ISTF website, newsletters
6. Risk Management - https://en.wikipedia.org/wiki/Risk_management#Risk_management_and_business_continuity
7. Continuity Planning - https://en.wikipedia.org/wiki/Business_continuity_planning