CITY UNIVERSITY OF HONG KONG
Information Security Policies

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

Document Control

Document Owner	Classification	Publication Date
OCIO	PUBLIC	2013-12-24

Revision History

Version	Date	Summary of Changes
1.0	2013-12-19	Initial release.

Distribution

Copy	Issued to	Location
Master	Public	http://www6.cityu.edu.hk/infosec/isps/docs/?page=00.about

Distribution

The Office of Chief Information Officer ("OCIO") of the City University of Hong Kong is the distribution source of the document. The official URL of this set of documents is:

http://www6.cityu.edu.hk/infosec/studentlan/docs/?page=01.InformationSecurityPolicies

Copyright Statement

infosec@cityu.edu.hk
Office of Chief Information Officer
City University of Hong Kong
Tat Chee Avenue
Kowloon
Hong Kong SAR

Acknowledgements

The City University of Hong Kong ("University") would like to thank the Joint Universities Computer Centre Limited ("JUCC") for granting the University, as member of JUCC, the rights to use and modify JUCC materials for the developing of information security policies, practices and procedures within the University and Colleges of the University.

Contact information for requesting for original JUCC Information Security materials is listed below:

copyright@jucc.edu.hk
Joint Universities Computer Centre Limited (JUCC),
Room 223, Run Run Shaw Building,
c/o Computer Centre, The University of Hong Kong,
Pokfulam Road, Hong Kong

Contents

Introduction

The continuity of the City University of Hong Kong ("University") is highly dependent upon the way which the information resources are managed. The principles used in setting the foundations for the policies governing information security management are:

- Information resources that support information processing are important assets ("information assets") which must be appropriately protected from accidental or intentional compromise.
- The confidentiality, integrity and availability of information assets are essential for ensuring legal compliance and for maintaining competitive edge and the image of the University.
- Information assets are provided to support business processes and should be used to derive benefit for the University.
- All personnel who use information assets have a responsibility to protect them, and to minimize the risks that might result from inappropriate use.

Throughout the document the terms MUST, SHALL and SHOULD are used carefully. "Musts" and "shalls" are mandatory and not negotiable; "shoulds" are goals for the University. The terms "data", "information" and "information asset" are used interchangeably in the documents.

Hierarchy of Information Security Policies and Standards

The set of Information Security Policies and Standards consists of documents with different levels of details:

- **Policies**
  Policies are high-level statements driven by the University's requirements. They are technology and process independent statements setting the general principles, goals and objectives for the University. They are not statements of how the goals and objectives will be accomplished.
- **Standards**
  Standards are the next level in the hierarchy with increasing levels of detail for business requirements.
  Standards still remain platform independent. They are directed to the implementation of policies for specific subject areas. Standards can be further broken down into two types, with varying levels of latitude in their implementation.
  - "**Requirements**" are activities that must be followed – there is no leeway within a requirement.
  - "**Guidelines**" are not as stringent as requirements – guidelines should be followed, unless there is a compelling business reason for not doing so (for example, if there are specific legal requirements within a jurisdiction prohibiting the implementation of such a requirement, then there is a compelling business justification for not implementing the standard.)
- **Procedures**
  Procedures are process-level and/or platform-specific instructions for implementing Policies and Standards. One standard may require multiple procedures – one for each platform to satisfy the standard. For example, a standard dealing with password length would require procedures at least one separated for each platforms – Solaris, AIX, Windows, AS400 etc. – where that standard is implemented.

Objective

The objective of this "Information Security Policies" document is to define the principles to which all users of information assets in any form owned by or entrusted to the University. The principles cover the following areas:

- Defining the confidentiality, integrity and availability requirements for data and information resources used to support the University's objectives.
- Ensuring that the security requirements of those data and information resources are effectively communicated to individuals who come in contact with such information.
- Using, managing and distributing those data and information resources in any form (electronic or physical) in a manner that is consistent with their confidentiality, integrity and availability requirements.

In addition, this document also sets out the Information Security Governance Framework of the University based on international standard on information security, International Organization for Standardization ("ISO") 27001.

Definition of Information Security

Information security is critical to protect information and information resources from unauthorized access, use, disclosure, disruption, modification, or destruction and it is applicable to the lifecycle of the information from creation, use, transfer, storage to disposal.

Information security is primarily concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: digital (e.g. data files), material (e.g. printed papers), or unrepresented information (e.g. knowledge of internal affairs). These include text, picture, audio and video and covers information transmitted by mail, email, oral communication, telephone etc.

The University requires appropriate control measures for all forms of information to ensure their confidentiality, integrity and availability and avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

- **Confidentiality**. Protecting information from unauthorized access or disclosure
- **Integrity**. Protecting information from unauthorized or improper modification and destruction
- **Availability**. Ensuring timely and reliable access to and use of data and information resources.

The University shall also adopt control measures to ensure the authenticity, accountability, non-repudiation, and reliability of information and information services depending on circumstances.

- **Authenticity**. Assuring the correctness of the claimed identity of an entity.
- **Accountability**. Assuring the traceability and responsibility of an entity for its actions and decisions.
- **Non-repudiation**. Preventing the future false denial of involvement by any entities.
- **Reliability**. Assuring the correctness of service, and behavior and result of service is consistent and predictable.

Scope

This document is used as the University-wide Information Security Policies and all activities performed relating to the information resources must comply with the policies unless a written approval was obtained from the Information Strategy and Governance Committee ("ISGC"), which is the approval body of this standard. Also, this policy must be published and communicated to the University's staff members, students and relevant external parties.

Purpose

The purpose of these policies and standards is to ensure that due care is exercised in protecting the University's information assets. Due care is defined as the economical and practical protection of information at a level commensurate with its value. The value of the information is determined by considering not only the cost of its development, but also its non-monetary value, including intangible worth (e.g. intellectual property and competitive value) and rights of personnel affected (e.g. privacy). The value of information can also be impacted by its misuse. Good Information security can facilitate cost avoidance through the prevention of misuse.

Annual Review

The Information Security Unit ("ISU") in the Office of the Chief Information Officer ("OCIO") is responsible for the reviews and updates of this document from time-to-time to keep up with any changes in this policy.

Terms and Definitions

For the purpose of this set of documents, the following terms will be used:

Asset owner

Asset owner is the person or group of people identified by management as having responsibility for the maintenance of the security of that asset. The asset owner may change during the lifecycle of the asset.

The owner does not normally or necessarily personally own the asset. In most cases the employing organization, its customers or suppliers will be the entity with property rights to the asset.

The terms asset owner, asset controller, and asset custodian are used interchangeably. Information is one type of asset.

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 is one type of asset and IT asset. Information assets are knowledge or data that has value to the University regardless of form or format.

Information resources

All data, information as well as the hardware, software, personnel and processes involved with the storage, processing and output of such information. This includes data networks, servers, PC's, storage media, printers, photo copiers, fax machines, supporting equipment, and back-up media.

The terms and definitions listed in BS ISO/IEC 27000:2009 [1] will be also used.

Information Security Policies

1. Organization of Information Security

Each member of the University, including staff members, students, contractors and other third-parties, that are contractually engaged with the University are responsible for the security and protection of information resources over which he or she has control. He or she is obliged to adhere to the University's information security policies, standards, guidelines and procedures, and protect information resources from unauthorized intrusions, malicious misuse, or inadvertent compromise; and to preserve physical and logical integrity of these information resources.

The following bodies in the University are responsible for the governance of the Information Security in the University:

- "**Information Strategy and Governance Committee**" (ISGC). This is the top-most authority in the Information governance structure of the University. It represents the management of the University and is responsible for endorsing the policies, guidelines, rules and regulations governing the IT provision in the University. It is also responsible for making recommendations on resource and budget allocations to the campus for IT-related initiatives to the University and the monitoring and reviewing of the implementation of IT initiatives.

- "**Information Security Task Force**" (ISTF). It is the body for reviewing, and collecting the opinions on this University's Information Security Policies and Standards ("ISPS"), ISTF consists of members from key units such as Central IT, Internal Audit Office, etc.

- **"Central IT"**. It comprises the Office of the Chief Information Officer ("OCIO"), the Computing Services Centre ("CSC") and the Enterprise Solutions Office ("ESU"). The Central IT, while maintaining the University-wide ISPS, is also responsible for meeting the requirements in this ISPS.
    - The OCIO is responsible for the strategic development and co-ordination of all information services and technology in the University.
    - The CSC is officially responsible for the provision of central computing facilities and technical services including rendering to computer and network in the University.
    - The ESU is responsible for implementing and managing the University's central information systems. The ESU works in partnership with departments to integrate information technology into administrative processes.

- **"Information Security Unit" (ISU)**. It is a Unit under the OCIO. It is responsible for all security related activities. ISU is also responsible for the annual review of the University-wide ISPS, and recommending changes and enhancements to the ISTF.

- **"Academic Departments", "Administrative Units" and "Research Centers"**. The University comprises of many academic departments, administrative units and research centers. In this set of documents, all these will be collectively referred as "**University Units**".

- **"Departments" and "Departmental Information Technology Support Units" (Departmental ITSU)**. The Departments use the University's information in their daily operations. Some of the Departments maintain their own departmental IT functions and staff members to meet the specific departmental needs. Head of departments or their delegates shall ensure the conformity of their use of information and information resources to the University-wide ISPS.

- **"System Owner".** System Owner is an individual or an entity, which is responsible for the overall procurement, production, development, modification, maintenance, use of the system. While the System Owner has final responsibility for proper operation of the system, the System Owner could delegate some of the operational tasks to a System Custodian. System owner is also known as System Controller.

- "**System Custodian**". System Custodian is an individual or entity, which is responsible for the development, production, operation, modification and maintenance of the system according to the requirements from the System Owner. The System Custodian neither owns the system nor the information in the system. The System Custodian has limited authority, and is not normally authorized to make decisions on use of the system. For instance, the system custodian is not authorized to make decision on granting or revoking access to system and information in system.

2. Information & IT Asset Inventory and Ownership

An inventory list of important assets associated with information resources must be properly documented and maintained for record-keeping and auditing purposes.

The establishment of roles, responsibilities and accountabilities are needed for proper management and protection of the University's information assets.

All information and IT assets obtained by the University, used for work-related purpose, or storing the University's Information are subject to the University's control. They can only be disposed in accordance with the requirement defined in Section "4) Information Classification and Handling" policy of this document.

3. Acceptable Usage

The University values academic and intellectual freedom and encourages the use of the University's information resources to support the University's affairs and its mission of education, service and research. Priority must be given to the use of the information resources for the official affairs of the University.

The University recognizes the trend and demand of "Bring Your Own Device" (BYOD). Regardless of the ownership, "Information resources" means all information and communications technology; hardware and software; data and associated methodologies; infrastructure and devices that are:

- controlled or operated by the University;
- connected to the University's network;
- used at or for the University's activities;
- brought onto the University's facilities.

Information resources include but not limited to:

- Computers and mobile devices – such as desktops, laptops, tablets, Smartphones, Personal Digital Assistances ("PDAs"));
- Computer systems – such as the University's information systems and applications;
- Storage devices – such as Universal Serial Bus ("USB") flash memory devices, Compact Discs ("CDs"), Digital Versatile Discs ("DVDs"), floppy disks, network multi-function printers with built-in memory for caching printouts or storing scanned images;
- Telecommunication equipment – such as switches, routers, Private Branch Exchange ("PBX") systems and phones, VoIP systems and phones;
- Networks – such as Intranet and Internet via wired or wireless connections;
- Software, databases and any other similar technologies as they come into use; and
- Information or data stored in any carriers, service providers and third parties.

The use of information resources, including their handling and storage, must be legal and must be of the highest ethical standards, and must not involve with activities and/or material(s) unacceptable to the University's environment which include, but not limited to acts of a malicious or nuisance nature, invasion of privacy, violation of copyright and licensing, harassment, bullying, hacking, altering the settings on any information resources without authorization, plagiarism, impersonation/identity theft, spoofing, or cheating in an examination.

4. Information Classification and Handling

The University must classify all its information into appropriate levels (e.g. restricted, confidential, internal and public) to indicate the need, priority and degree of protection required.

The following classification levels shall be used for classifying the University's information assets:

- **RESTRICTED**. This classification applies to sensitive information that is strictly restricted by the University, the government or any other agreements between the University and third parties (including the government).
  Throughout the scope of this set of Information Security Policies and Standards, the terms "**RESTRICTED**" and "**SECRET**" are used interchangeably.
- **CONFIDENTIAL**. This classification applies to sensitive information that is intended for use by authorized personnel within the University.
- **INTERNAL**. This classification applies to information that is intended for internal use within a department or the University.
- **PUBLIC**. This classification applies to information that has been approved by authorized parties within the University for Public Consumption.

Every member of the University has responsibilities to consider security during the entire life-cycle of information in the course of their works.

The University has defined retention periods for certain kinds of information. Each member of the University shall observe these requirements. Section "16.2) University Policies and Regulations" of this document listed some sources of the University's Policies.

Each University Unit should establish procedures appropriate to the information held and processed by it, and ensure that all staff members and students are aware of those procedures.

5. Human Resources Security

5.1. Prior to Employment / Engagement

The University's staff members, students, contractors and third party users must understand their responsibilities and must be suitable for the roles they are considered for in handling or use of information assets. The University must implement appropriate controls to reduce the risk of theft, fraud or misuse of the University's information assets and resources.

- **Roles and responsibilities**. All the University's staff members, students, contractors and third party users are obliged to follow the security roles and responsibilities defined and documented by the University, and their respective University Units.
- **Screening**. Pre-employment screening is a mandatory requirement for candidates whose roles or positions may have access to sensitive information.
- **Undertaking**. All the University's staff members must agree to and sign a Confidentiality Pledge to indicate that they fully understand their responsibilities with respect to information security, and agree to comply with the University's ISPS.

5.2. During Employment / Engagement

The University's staff members, students, contractors, and third party users shall be aware of information security threats and concerns; and of their responsibilities and liabilities; and are expected to be properly equipped to support the University-level ISPS in the course of their normal work or studies, and to reduce the risk of human error.

- **Management responsibilities**. The University's management is responsible for ensuring that all the University's staff members, students, contractors, and third party users shall comply with the University's ISPS.
- **Information security awareness, education and training**. All the University's staff members, students, contractors and third party users should receive appropriate information security awareness training and regular updates of the University's ISPS relevant to their job functions.
- **Disciplinary process**. All the University's staff members, students, contractors, and third party users who have committed a security breach are subject to the University's disciplinary actions.

5.3. Terminations or Change of Employment / Engagement

The University's staff members, students, contractors, and third party users shall exit or change employment / engagement relationship with the University in an orderly manner.

- **Return of assets**. All the University's staff members, students, contractors and third parties must return all of the University's assets in their possession in condition acceptable to the University upon termination of employment, academic and contractual relationships.
- **Removal of access rights**. Access rights to information and/or information resources must be removed or de-activated upon termination of the responsibility, employment, academic and contractual relationships.
- **Change of responsibility or employment**. The University shall manage change of responsibility or employment as well as the termination of employment or responsibility. The new responsibility or employment should be managed as described in Section 5.1.

6. Physical Access Security

The equipment, records, and data comprising IT operations represent a critical asset for the University and they must be protected adequately commensurate with their value, confidentiality, and criticality of the information or data stored or accessible and the identified risks. Physical access control over the University's information resources must be implemented and should include the following implementation elements:

- Equipment control (into and out of site);
- A facility (e.g. place, site, office and room) security plan;
- Physical entry control including an evacuation plan and information asset protection plan, as appropriate, during an emergency evacuation;
- Procedures for verifying access authorizations prior to physical access;
- Maintenance records, including but not limited to, records of infrastructure changes such as adding or deleting network segments, adding servers, etc.;
- Need-to-know procedures for personnel physical access;
- Sign-in for visitors (e.g. staff members, students, contractors) and escort, if appropriate; and
- Testing and revision of the physical access controls.

These apply to all information processing facilities and premises, including data center, general offices and premises of contractors performing service for the University.

7. Environmental Security

Environmental security is important for the University to ensure its investment is capable of meeting its performance and uptime objectives. The University's premises should be protected physically against damage from fire, flood, wind, earthquake, explosion, civil unrest, theft, robbery, vandalism, and other forms of natural and man-made risk.

Environmental monitoring of the following conditions must be carried out for all business critical systems and are strongly recommended for all other hosts and server systems:

- Air conditioning (temperature and humidity);
- Fire and smoke detection and control;
- Electrical power supply;
- Uninterrupted Power Supply ("UPS") installations;
- Water leakage;
- Alarm and emergency systems; and
- Loading, grounding and other structural protection.

The relevant faculties, controllers or custodians are responsible for ensuring that these conditions are complied with.

8. Communications and Operating Management

The University must ensure that the operational procedures for correct and secure handling of information resources are documented and made available to appropriate staff members and contractors. The level of detail should match the criticality of the information being processed and complexity of the operations concerned.

The University shall segregate the duties and areas of responsibility of staff members and contractors to reduce the risk of unauthorized or unintentional access, modification or misuse of information assets. The level of segregation should match the confidentiality and security requirements of the information being processed.

9. Change Management

The University must ensure changes to its information systems, telecommunication equipment, software, and other information resources will not result in adverse impact on the confidentiality , integrity and availability of the University's IT environment unless a written approval on exemption being granted was obtained from the Information Strategy and Governance Committee (ISGC). All changes must be documented, authorized and in line with the University's operational and security requirements. In particular, the following items should be recorded:

- Change Request, with initiator, approval, implementer, and reviewer records
- planning and testing of changes
- assessment of potential impacts, including security impacts
- fallback procedures

The University should ensure that personnel responsible for change development and production migration are properly segregated. When duties cannot be separated, compensating controls should be implemented, for instance, a supervisory level employee should review the system regularly and/or after change.

The University should assign dedicated resources to monitor the change processes. Periodic system migration log checking of production systems should be performed by personnel with sufficient technical knowledge and independent from the change promotion teams responsible for the systems.

10. Network and Platform Security

10.1. Network Segregation

The University shall properly protect all networks with appropriate security measures and appropriate equipment. Network addresses, network configurations and related systems or network information shall be properly maintained and shall only be released to authorized parties.

The University shall segregate the Campus Network into separated network environments according to the usage, classification of information and services hosted in the network:

- **"Untrusted Network".** Devices on the untrusted network are either accessible to all the members of the University (e.g. computers in student labs), or fully controlled and managed by the general users or owners of the devices (e.g. tablets of individuals).
  Since these devices may be abused, or may not be properly configured, untrusted networks shall be used to isolate these devices. Direct access to any of the sensitive information or servers is not allowed.

- **"Managed Network"**. Devices on the managed network are managed by Departmental ITSU, Central IT and/or users of the devices. Access controls are enforced on these devices, which are accessible to named users or shared by small group of named users (e.g. office desktops for staff members). Managed network shall be used for day-to-day office tasks and activities of University Units.

- **"Secured Network"**. Critical services shall be hosted in secured network, and only be accessible to authorized staff, appropriate contractors and third party users. "RESTRICTED" and "CONFIDENTIAL" information shall primarily be stored in secured network, and only be transmitted to devices on other networks for processing when needed. Appropriate security controls shall be implemented to protect devices, services and information in the network. The University shall maintain multiple secured networks to segregate services and applications of different natures or security requirements.

- **"(Departmental) Internal network".** Departmental Internal networks are sub-networks inside the Campus network. They are controlled and maintained individually by the respective University Units. When "RESTRICTED", "CONFIDENTIAL" and "INTERNAL" information are required to be hosted and/or processed, departmental networks must be segregated into the "untrusted network", "managed network" and "secured network". The security levels of these departmental internal networks must conform to the University's ISPS.

The University shall manage and control the networks to maintain network security. Staff members, students, contractors and third party users shall not connect unauthorized devices into the networks or by any means to lower the security levels of the University's networks. Connections between networks must not compromise or downgrade the security of information processed in the networks.

The University shall document, monitor and control wireless networks with connection to its network. Staff members, students, contractors and third party users are prohibited from connecting

unauthorized wired/wireless network devices and/or setting up peer-to-peer or ad-hoc wireless network with connection to the University's networks, and sharing the University's networks to uncontrolled devices.

Proper authentication and encryption security controls shall be employed to protect data communication over wired/wireless networks with connection to the University's networks.

10.2. Internet and External Network Security

Centrally arranged Internet gateways are managed by Central IT. The University Units may arrange and manage their own Internet gateways according to University's prevailing policy and regulation.

All gateways (including Internet gateways and gateways to External Networks between the University, partners of the University and/or the remote sites of the University) must be approved by and registered with Central IT, and all Internet access shall be channeled through registered gateways. All gateways must also conform to the "Network and Platform Security Standard" of the University.

All Inbound and outbound traffic to and from the University's networks and systems must pass though the registered gateways.

"**RESTRICTED**", "**CONFIDENTIAL**" and "**INTERNAL**" data must be encrypted when transmitted over an untrusted network, including the "**Campus network**" of the University.

In circumstances where it is not feasible to fulfill the standards or the network is designed to meet special purposes (e.g. research in network security, setup of honeypot, etc.), the department shall isolate the network from the other networks of the University. The owner shall register the network with Central IT; shall implement appropriate security control and must not connect this network to the other systems of the University.

10.3. Application, Service and Platform Security

The owners, controllers or custodians of Information Systems must ensure that their Information Systems are protected from threats and must implement the following:

- Anti-virus and Firewall Systems
- Intrusion detection Systems
- Information and System backup Systems
- Network and Application logging and monitoring Systems
- Application and Platform Configuration Management and Hardening
- Hardware and Software Patch Management
- Configuration management

11. Access control

Access control to critical, important information assets based on functional and security requirements of the University is essential to safeguard the confidentiality, integrity and availability of information assets within the University.

11.1. Access Control Policy

The University must implement the following:

- Access control that will restrict access to resources and allow access only by privileged entities. Either of the following implementation features may be used:
    - Role-based access; and/or
    - User-based access;
- Security event control that will record and examine system activities, especially those performed by privileged accounts, and respond to "security events";
- Authorization control that will require obtaining consent for the use and disclosure of the University's information; and
- Password control that corroborate an entity – the individual user of a data network or system, or a computational process – to whom it claims to be.

University Units shall regularly review access privileges to services and data granted to roles and users; to ensure the appropriateness of privileges possessed by the relevant roles and individuals.

11.2. Password and Screen Lockout Policy

All accounts of the University's information systems must be password protected to help maintain the confidentiality, integrity and availability of the University's data as well as to help protect the University's information resources.

Each member of the University's campus community is responsible for ensuring that strong passwords are used and the passwords are maintained according to the University's password standard. This is to reduce overall risks to the University by helping authorized users reasonably avoid security and privacy risks that result from weak password choices.

The University shall also enforce screen lockout policy on user desktops of all staff members and students, except desktops designated or special purpose, e.g. monitoring console for network performance, tutor's terminal in teaching studio.

12. Information System Acquisition, Development and Maintenance

The University must ensure that information security is considered throughout the lifecycle of any system that holds and processes the University's information assets, from conception and design, through creation and maintenance, to ultimate disposal. This policy outlines the basic requirements and responsibilities to achieve this.

12.1. Security Requirement of Information Systems

Any department with requirements for IT systems must discuss them with Central IT at the project initiation stage.

Business requirement documentation for new systems or enhancements to existing systems must contain the requirements for security controls. Security vulnerabilities must be recognized from the outset through undertaking a risk assessment and the security requirements must be developed alongside the functional requirements.

Appropriate controls and audit trails must be designed into applications to prevent error, loss and unauthorized modification or misuse of information in application systems.

Application systems must implement input validation to ensure that data input is properly encoded and sanitized (i.e. filter all unaccepted and unsupported input, reject insertion and injection of codes, commands and instructions, eliminate buffer overflow and divided by zero, prevent path transversal, etc.). Input validation must be mandatory at server-side and client-side as appropriate.

12.2. Security in Development and Implementation

The University must ensure an IT system is comprehensively tested for all its functional and security features prior to the implementation in the production environment.

Any of the University's data that is used during the development and test phase of preparing application software must be protected and controlled.

Security controls must be applied to the implementation of IT systems in the production environment.

Application must be tested for an extensive period against predetermined criteria and methodologies by personnel not directly involved in the development of the system.

Testing results must be documented and retained. Testing results must be accepted and approved by system owner before the application rollouts.

13. Supplier Management

The University must ensure that purchase of equipment, supplies, products, services and maintenance is conducted in a manner that is consistent with the University's ISPS. Information systems and services used to store or process the University's sensitive information will have significant impact on security of the University's environment. The corresponding vendors should implement appropriate measures to meet the objectives below:

- Comply with the University's information security policies and any other legal and regulatory requirement where applicable;
- Ensure the confidentiality, integrity and availability of the University's information resources or processes managed by internal users and suppliers;
- Protect against any potential threats or hazards to the security of the University's information;
- Protect against any unauthorized access to or use of the University's information that could result in substantial harm or inconvenience to the University, its staff members, its students and any other third party users;
- Dispose of the University's sensitive information in a secure manner in accordance with the University's information handling policy and standards; and
- Inform any security breaches involving the University's sensitive information immediately and take appropriate safeguard measures to minimize the impact of such breaches.

The University should assign dedicated resources to review the Service Level Agreements ("SLA") of its vendors to confirm that they have satisfied obligations described above. Periodic monitoring of vendor service levels and performance should be performed by relevant University Units to ensure that any breaches of SLAs will be timely reported and investigated by the University's Information Security Unit ("ISU").

Non-disclosure Agreements ("NDA") should be established between the University and vendors if sensitive information related to the University, its staff members, students, sub-contractors and/or other third parties is used, stored and processed by the vendors.

The University management must evaluate existing vendors' compliance and performance results based on the regular monitoring feedback at least annually or before the renewal of service contracts, whichever is earlier.

14. Information Security Incident Management

As a key part of any organization's overall information security strategy, it is essential to have in place a structured well planned information security incident management approach.

14.1. Responsibility

Information Security Unit ("ISU") will manage all information security incidents with the assistance from all parties within the University, this include but not limited to the deans, department heads and the departmental IT support units.

An Information Security Incident Response Team ("ISIRT") shall be established and led by ISU to provide the University with appropriate personnel for assessing, responding to and learning from information security incidents, and providing the necessary co-ordination, management, feedback and communication.

All staff members and students of the University have responsibilities to report any security incidents to CSC Help Desk or ISIRT.

Security incidents include but not limited to:

- Known information security breaches, such as theft;
- Disruptions or loss caused by the failure of a security mechanism, such as computer virus infection or abnormal system behavior; and
- Known or suspected security incidents, such as system outage or traffic congestion.

14.2. Information Security Incident Reporting and Response Procedure

The University's staff members, students, contractors and third-party users who come across any evidence of information being compromised or who detects any suspicious activity that could potentially expose, corrupt or destroy information must report such information to his or her immediate supervisor, to CSC Help Desk or ISIRT. "Critical" or "Significant" security incidents should not be investigated by individuals without the authorization of the ISU.

An Information Security Incident Reporting Procedure must be defined to handle information security incidents. The procedure will include the following:

- Types and severities of information security incidents;
- Incident reporting procedures setting out the actions and point of contact;
- Incident response procedures for different types and severities of incident, including appropriate analysis and identification of causes, containment, communication with those actually or potentially affected by the incident, reporting of the incident to appropriate authorities, planning and implementation of corrective action to prevent reoccurrence as appropriate;
- Seizure of IT equipment and the relevant data and log files, collection and use of audit trails and similar evidence as part of the incident management and investigation process, and appropriate management of this evidence for use in subsequent legal or disciplinary proceedings;
- Formal controls for recovery and remediation, including appropriate documentation of actions taken; and

- Mechanisms used to perform ongoing monitoring of information resources to detect events and incidents.

14.3. Post Information Security Incident Review Procedures

After information security incidents have been resolved or closed, the following review activities are necessary:

- Identifying the lessons learned from information security incidents; and
- Identifying improvements to information security safeguard implementation, as a result of the lessons learned, whether from one information security incident or many.

14.4. Information Security Awareness Training

Heads and supervisors of the University Units should ensure that appropriate information security awareness training is regularly conducted for their staff members and students of the University.

The training programs should:

- Include reviewing the University's information security policy, guidelines, procedures, and standards, as well as departmental procedures and best practices established to safeguard sensitive information;
- Conform with the laws governing specific categories of confidential information, such as the Personal Data (Privacy) Ordinance, etc.;
- Include topics such as password management, best practices for protecting confidential information, incident reporting, and security reminders regarding current threats and recent incidents to technical environments in which individuals are working; and
- Include awareness on the part of all University staff members, students, contractors and third-party users in timely reporting information security incidents.

15. Business Continuity Management

Business Continuity Plans ("BCP") and Disaster Recovery Plans are required to maintain the operations of the University in the event of an incident or a disaster.

Each University Unit must develop plans that will allow it to perform its core required operations in an alternative fashion as well as an appropriate disaster recovery policy and plans for their working environment.

Each information system of the University must have periodic backups of data, facilities for continuing critical operations available in case of an emergency, and disaster recovery plans in place. While the development of a BCP is a general business issue with the IT component as a part of the overall plan, having a BCP is a significant element in providing the "availability" component of the University's Information Security.

An effective business continuity management must include the following:

- A Crisis Management Team, which is an administrative and decision-making group of senior management personnel from each administration division and/or academic unit that is responsible for coordination of BCP in the event of an incident or a disaster;
- A BCP Team consists of a group of personnel with necessary technical skills, business process knowledge and leadership from each academic unit and administration division that are responsible for implementation of BCP in the event of an incident or disaster;
- An emergency operation center and operational plan;
- A disaster recovery and business resumption plan; and
- Regular testing and revisions procedures.

16. Compliance Management

16.1. Legal and Regulatory Compliance

The University shall comply with laws regarding information security requirements. Dedicate resources (e.g. legal professionals, compliance staff or advisor) should be assigned or engaged by the University Units to monitor latest statutory and regulatory requirements that the University has to comply with. A formal management plan for each regulation should be developed and executed.

Currently, the University shall comply with all applicable laws, in particular with the following laws:

- Cap 106 Telecommunications Ordinance;
- Cap 593 Unsolicited Electronic Messages Ordinance;
- Cap 200 Crimes Ordinance;
- Cap 210 Theft Ordinance;
- Cap 486 Personal Data (Privacy) Ordinance;
- Cap 528 Copyright Ordinance;
- Cap 57 Employment Ordinance; and
- Common Laws.

16.2. University Policies and Regulations

The University has a set of internal policies and regulations which its staff members, students, contractors, and third party users must observe and comply with. The University must inform these parties about the policies and regulations and these parties shall get themselves familiar with the policies and regulations.

16.2.1. All Staff members, Students, Contractors and Third Party Users

All members of the University must comply with the following policies and guidelines of the University:

- Personal Data (Privacy) Issues - Code of Practice
- Policy on University Intellectual Property and Related Matters
- Policy on Acceptable Use of IT Services and Facilities

16.2.2. All Students

All students of the University must comply with this set of ISPS and the following University's policies and guidelines:

- Code of Student Conduct and Disciplinary Procedure

A comprehensive list of important policies and guidelines, which all students shall comply with, are maintained by the Academic Regulations and Records Office and available through the hyperlink below:

- http://www6.cityu.edu.hk/arro/content.asp?cid=229

16.2.3. All Staff

All staff of the university must comply with this set of ISPS and the following University policies and guidelines:

- Code of Conduct
- Conflict of Interest
- Declaration of Interest by Members of University Committees
- Regulations Governing Staff Discipline

A comprehensive list of important policies and guidelines, which all staff members shall comply with, are maintained by the Human Resource Department and accessible through the hyperlink below:

- http://www6.cityu.edu.hk/hro/stafflan/new-employee/academic-faculty/policy.asp

16.3. Other Contractual Compliance

Contractual requirements that were established with a third party shall provide assurances that the contracting third party will appropriately safeguard information in accordance with laws, regulations, and the University's policies. When providing access to or passing confidential information to a third party agent of the University, the written contractual agreements should include terms and conditions that:

- Require all contractors, consultants, or external vendors to observe laws and the University's policies for privacy, copyright and security;
- Prevent disclosure of confidential information to other third parties including subcontractors, except as required and permitted by the contract terms of the University;
- Require a plan for the return or destruction of confidential information upon completion of the contractual requirements; and
- 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.

Consideration should be given to limiting outside vendor access to sensitive information resources.

17. Information System Internal Assessment

Internal Audit Office of the University conducts Independent Internal Audits in the University. The roles and responsibilities of Internal Audit Office are defined by the Audit Charter of the University.

The University must ensure that all information systems and applications, which are critical to the University's operations and financial reporting, or contain sensitive information of the University, and its related infrastructure, shall be evaluated as an ongoing process to improve the quality of its operations. This policy shall apply to all the Units of the University.

Periodic information system internal assessment should be performed to identify deficiency and improvement opportunities within the existing security framework of the University. These assessments will assess the University's ability to mitigate identified information security risks from people, process and technology perspectives. These assessments will be performed by qualified individuals that have an understanding of the University's information security environment.

When requested and for the purpose of performing internal assessments, any access needed shall be provided to members of internal assessment team. This accesses may include but not limited to:

- User level and/or system level access(es) to any computing or communications device;
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on respective academic units or administrative divisions' equipment or premises;
- Access to work areas (e.g. laboratories, offices, cubicles, storage areas, etc.);
- Access to reports and documents created during internal assessment; and
- Access to interactively monitor and log traffic on networks.

Management response regarding the remedial actions of the identified issues and opportunities for improvement must be obtained.

Reference

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

BS ISO/IEC 27000:2009 – Information technology – Security techniques – Information security management systems – Overview and vocabulary

BS ISO/IEC 27001:2005 – Information technology, Security techniques – Information security management systems – Requirements