

# Lingnan University Information Security Policy

## 1.0 Purpose

Lingnan University's Information Technology resources are a valuable university asset and must be managed accordingly to ensure their integrity, security and availability for lawful educational and research purposes. This document is intended as a high-level security policy statement for use by all university staff, students and users of the university's information technology resources.

The purpose of this policy is to ensure:

- The provision of reliable and uninterrupted IT services;
- The integrity and validity of data;
- An ability to recover effectively and efficiently from disruption; and
- The protection of all the university's IT assets including data, software and hardware.

---

## 2.0 Scope

Within this Policy, Information Technology resources include information assets (e.g. research data, databases, files, training materials, risk assessment documents, business continuity plans); software assets (e.g. applications and systems software and development tools); and physical assets (e.g. computers, communications equipment and media).

The Policy applies to all users of the university's Information Technology resources, including those who install, develop, maintain, administer and/or use those systems and applications.

The University is bound by the regulations and policies of the Hong Kong SAR government. Detailed requirements for Information Security are covered by the Office of the Government Chief Information Officer (OGCIO) at the dedicated website on [Information Security](#).

---

## 3.0 Information Security Policy

### 3.1 *Acceptable Use of University Computing Facilities*

This is described in the policy document '[Acceptable Use of University Computing Facilities](#)'.

### 3.2 *Access Control*

All users of the university's Information Technology resources must be authorised to access the appropriate systems and their resources. Access is controlled and monitored in accordance with university policy. The elements involved in controlling and monitoring access include identification, authorisation and authentication.

#### 3.2.1 Identification

All system users are assigned a unique ID or username to access the university's systems and applications. Usernames are not to be shared, except for designated Group Accounts, authorised by ITSC. Users are responsible for maintaining the security of their own Usernames and all activity occurring under those Usernames. Usernames are issued in accordance with approved standards. In special circumstances, temporary generic accounts may be approved by the Director, Information Technology Services Centre (ITSC) or nominee.

#### 3.2.2 Authorisation

Only those users who have valid reasons (as determined by Heads of Departments/ Units) for accessing the university's systems and information are granted access privileges appropriate to their educational and/or business requirements. Access is granted by means of a computer account, which also serves as identification. Accounts are issued in accordance with approved standards.

### **3.2.3 Authentication**

Authentication ensures an identity. Each Username requires a password for validating identity. Standards apply to all systems requiring authentication. Each password should not be less than 8 characters long, including a mixture of alphabetic and numeric characters. It should be changed at least every 90 days.

### **3.2.4 Account Management**

All Heads of Departments/Units must regularly review their schedule of delegated authority, to determine who is authorised to use the system and their level of authorisation. Heads of Departments/Units must also determine who is authorised to access sensitive university information from off campus or remote locations.

At a minimum, a six monthly review of all system access levels of users should be carried out. The Heads of Departments/Units should ensure any non-compliance as a result of this activity is addressed as a matter of priority. All records of non-compliance must be kept until all matters arising from non-compliance have been resolved.

When employees terminate employment or change positions within the university, the Human Resource Office (HRO) should make the necessary changes to roles and access privileges in the appropriate system and according to established business processes.

### **3.2.5 Privileged Users Access**

Certain system users have high-level access rights; enabling them to access any data stored on the university's Information Technology systems. These staff can be generically termed System Administrators. Staff with high-level access rights should abide by the [System Administrators' Code of Ethics](#). System Administrators found guilty of breaching this Code of Ethics may be subject to disciplinary action handled under the university's normal disciplinary procedures.

Contractor and third-party access are permitted only if agreed to by the Heads of Departments/Units. These parties must comply with access control standards which require, at a minimum, that a unique username is used to identify each user. This ensures that only authorised individuals receive access to systems. All temporary accounts should have an expiration date based on contract completion date.

## **3.3 Asset Security Management**

### **3.3.1 Server and System Backup**

All university information and data must be backed up on a regular basis. Frequency of backup is determined by the frequency with which the data changes and the effort required to recreate the information if lost. Standards apply to the backup of data from all university systems.

### **3.3.2 Personal Computer and Mobile Device Backup**

All critical university information should be stored on centrally maintained corporate networked disk storage. Any other data stored on desktops, laptops or other mobile devices becomes the responsibility of the user to ensure it is backed up on a regular basis. Frequency of backup is determined by the frequency with which the data changes and the effort required to recreate the information if it is lost.

Where university data is stored on portable or mobile devices, it is highly advisable that additional security, in the form of encryption or biometric protection, is implemented to protect the university's information assets.

### **3.3.3 Recovery**

All backups of critical data must be tested periodically to ensure that full system recovery can be achieved. System Administrators must document all restore procedures and test these on a regular basis, at least annually. Backup media must be

retrievable within 24 hours, 365 days a year. Standards apply to the recovery of data from all university systems.

### **3.3.4 Off-Site Storage**

The off-site storage location (which can be “out-of-building”) must provide evidence of adequate fire and theft protection and environmental controls. A formal Service Level Agreement (SLA) must exist with the off-site storage provider and a site visit should be undertaken on an annual basis.

### **3.3.5 Data Retention**

Custodians of university data are responsible for defining and documenting the length of time data must be retained. The retention period, legal requirements, responsible parties, and source of legal requirement should be clearly specified. System Administrators are responsible for ensuring that these requirements are adhered to.

### **3.3.6 Business Continuity**

As part of the [Information Services Risk Management, Business Continuity and Disaster Recovery Policies](#), plans should be prepared and tested for all the university’s major systems. The testing strategy to be implemented will be influenced by the importance of the system to the university’s business operations and the ability to recover the system within agreed timeframes.

A copy of each plan should be stored offsite in a secure manner to ensure that the plan can be implemented in the case of a disaster. A review of any major disruption to information services should be undertaken to identify the cause of the disruption and where appropriate to adjust the plan and/or procedures to minimise the risk of the event occurring again.

### **3.3.7 Security**

All major information assets must be accounted for and have a nominated custodian who is responsible for the implementation and management of this policy in relation to those assets.

#### **3.3.7.1 Physical Security**

Access to secure areas, including data centres, computer rooms, LAN equipment rooms and any associated service facilities, is restricted to authorised university staff, through the use of passwords, locks or Smart Card access-control devices. Access to these facilities is governed by the [Lingnan University Data Centre Access Policy](#). All wiring closets must be secured to prevent any damage and to stop unauthorised attempts to connect to data outlets and to prevent snooping.

#### **3.3.7.2 Data Security**

Different types of data require different levels of security. University data is classified into three categories: Public, Proprietary and Restricted. It is the Heads of Departments/Units responsibility to establish authentication and authorisation guidelines for custodial data. Please note the following...

- Public data can generally be made available or distributed to general public;
- Proprietary data is for internal university use and not for external distribution; and
- Restricted (moderately to highly sensitive) data is to be used only by individuals who require it in the course of performing their university responsibilities, or data, which is protected by HKSAR government legislation. Restricted data can only be deleted with the permission of the Heads of Departments/Units.

Staff should be aware of their legal and corporate responsibilities concerning inappropriate use, sharing or releasing of information to another party. Any third party receiving proprietary or restricted information must be authorised to

do so and that individual or their organisation should have adopted information security measures, which guarantee confidentiality and integrity of that data.

### **3.3.7.3 Software Security**

Software for the purpose of this policy document is defined as the programs and other operating information used by, installed on, or stored on university owned computer systems or storage media (such as disks, backup tapes, CD-ROM, DVDs, etc). This definition also includes portable devices that are directly, indirectly or remotely able to communicate with a university-owned information system.

To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all licensing agreements must be adhered to. All software and other applicable materials must be licensed (as required) in an appropriate manner.

In order to comply with licensing regulations and to prevent software piracy, the purchasing and licensing of software and other applicable materials should, where appropriate, be carried out through IT Customer Services (ICS) in ITSC. Details of the purchaser, approver and installer must be logged, trackable and auditable. Contact the ITSC Helpdesk on ext: 7995 if you are unsure of procedures.

All software, including patches, upgrades or new versions, should be tested, archived and documented before being put into production systems. This transition should be under migration and version control and incorporate change management principles. Control measures should also be in place for maintaining and accessing program and system source libraries.

All operational software should be maintained at current versions or at a level supported by the supplier. In special circumstances, a non-current version of software for a legacy system may be retained for compliance purposes. Processes should also be put in place to ensure that information systems development and operational environments for critical systems are separated logically from each other.

Software development policies and procedures should be co-developed by ITSC's IT Enterprise Services (IES) and the appropriate university business area (e.g. Registry, CO, HRO, etc.), especially for use by project development teams consisting of staff from ITSC and the business area. In particular, attention should be paid to ensure that the security controls of audit trails and activity logs are built into applications for the validation of data and internal processing.

### **3.3.7.4 Internet Security**

Computer devices connected to the Internet face significant risk of unauthorised access or inappropriate use. A number of measures should be taken to mitigate this risk. Standards apply to all Internet capable devices requiring protection.

### **3.3.7.5 Email Security**

All email users should be aware of their responsibilities as described in the [Lingnan University Email Policy](#).

Unsolicited email can become a serious issue for the university, affecting performance of the mail delivery infrastructure and productivity of the user. To reduce the level of unsolicited messages, email that meets one or more of the following criteria will be blocked or rejected:

- Malformed email
- Email with an attachment identified as a significant risk
- Email that exhibits a significant level of unsolicited email characteristics.

### 3.3.7.6 **Mobile Equipment/Wireless Device Security**

With the proliferation of mobile and wireless devices throughout the university, it is essential that special usage policies and procedures be developed governing the use and access of such devices (e.g. PDAs, smart mobile phones, laptops, netbooks, etc). In particular, the university should ensure that the physical security and use of its assets and the sensitivity of information access are clearly addressed in this usage policy.

In addition, and where appropriate, device timeouts should be implemented to lockdown devices and minimise the risk of unauthorised access.

---

## 4.0 **Security Breach Notification and Reporting**

### 4.1 **Security Breaches**

A security breach is defined as any action or event in contravention of the provisions of this Information Security Policy; actions or events that contravene the provisions of policy established by organisations of which Lingnan University is a member (eg. HK-CERT, JUCC, HARNet, etc.); and/or actions or events deemed a security breach by Hong Kong Police Force.

The guidelines listed under “notification” below, should be applied during the course of an actual or potential security breach.

### 4.2 **Notification of a Security Breach**

The following steps are listed in the order that they should be taken. Once a breach is confirmed, the responsible officer should follow these steps as urgently as possible. If a particular step is not appropriate to the breach, then they should be ignored and move to the next step. The steps are...

- The ITSC Director or nominee should be notified immediately.
- If the security breach involves a possible breach of local or international law, then the ITSC Director or nominee will notify the Hong Kong Police Force as appropriate, as soon as is practicable.
- If a university department/unit is involved, then the department/unit should be notified as soon as possible, preferably via the Head of Department/Unit.
- If an organisation or person external to the university is involved in any capacity, then the Hong Kong Computer Emergency Response Team (HK-CERT) should also be contacted, as appropriate.
- If an organisation or person external to the university is involved as a potential victim, then that organisation or person should be advised as soon as possible.

### 4.3 **Reporting a Security Breach**

The person authorised by the ITSC Director to carry out a technical investigation of a security breach must adhere to the processes detailed in the [Lingnan University Security Incident Management Guide](#). A report of the security incident should be prepared for the ITSC Director. Once approved, the report should be submitted to the Head of the relevant Department/Unit outlining where possible the following details...

- General nature of the security breach;
- General classification of people involved in the security breach, such as external client, privileged staff member, etc.;
- Systems involved in the security breach;
- Details of the security breach;
- Impact of the security breach;
- Unrealised, potential consequences of the security breach;
- Possible courses of action to prevent a repetition of the security breach;
- Side effects, if any, of those courses of action.

Remedial action should be taken on the basis of this report, where appropriate. In particular, significant IT risks should be identified as part of the [Information Services Risk Management, Business Continuity and Disaster Recovery Policies](#).

#### **4.4 Unauthorised Access Attempts**

This includes anything from harmless exploration, to hacking in order to gain access to information. Unauthorised access also includes gaining access to computer systems for future use (e.g. extortion).

All unauthorised access attempts must be noted and logged. The Audit Trail/System Access Log must be reviewed regularly, exception reports generated and inspected by the System Administrator and appropriate action taken. A copy of the report of unauthorised access attempts must be produced and kept for future reference.

---

## **5.0 Enforcement**

The university considers any breach of security to be a serious offence and reserves the right to copy and examine files or information resident on or transmitted via the university's Information Technology resources, under the guidelines set out by the [Hong Kong Personal Data \(Privacy\) Ordinance](#). Students deemed to be in breach of security are subject to disciplinary action as outlined in the [Regulations Governing Discipline of Students](#). Staff deemed to be in breach of security are subject to disciplinary action available under [Authorities and Guidelines for the Administration of Disciplinary Actions](#). Offenders may also be prosecuted under local and/or international laws.

ITSC may confiscate computer equipment, temporarily remove material from websites or close any account that is endangering the running of the system or that is being reviewed for inappropriate or illegal use.

---

## **6.0 Awareness and Communication**

It is essential that all aspects of information security, including confidentiality, privacy and procedures relating to system access, should be incorporated into formal staff induction procedures and conveyed to existing staff on a regular basis.

Each employee, on commencement of employment, should be made aware that they must not divulge any information that they may have access to in the normal course of their employment. Staff must also be made aware that they should not seek access to data that is not required as part of their normal duties.

System Administrators should be properly trained in all aspects of system security prior to supporting these systems.

### **6.1 Dissemination of policies to staff and students**

Full details of the university's Information Security policies should be available to the whole university community as easily accessible web documents available online through the university's secure intranet portal.

When students join the university, awareness training in Information Security shall be included in all orientation programs, plus dedicated Information Security training programs will be made available for students to take on a voluntary basis.

Staff orientation should also include Information Security awareness training, plus the distribution of written material covering all their responsibilities.

Regular staff awareness sessions, including periodic testing of staff knowledge on Information Security shall be carried out annually, including new policies and new procedures to deal with information security issues.

## **6.2 Inform all of Policy Updates**

Whenever changes are made to the university's Information Security policies, a campus wide email will be distributed to all staff and students. If there are major changes, special Information Security training sessions shall be organised for both staff and students.

---

## **7.0 Responsibilities**

Information Security is the responsibility of ALL members of the university, but dedicated responsibilities are described in detail below for the following categories...

### **7.1 Heads of Departments/Units**

Heads of Departments/Units are responsible for the security of the IT facilities in their department/unit, including reporting any breach of Information Security in their department/unit or University in general. The head of the Department/Unit may appoint a person to be responsible for the following...

- Secure configuration of computers purchased by the Department/Unit in areas available for use by students and the provision of explicit notices stating the conditions of use of those computers.
- Secure configuration, consistent with these policies, of any servers in operation.
- Making sure that anti-virus software for computers used by staff, visitors and contractors is in operation and has been legally purchased.
- Any other security requirements to meet university regulations and policies.

### **7.2 Staff**

Staff are responsible for...

- Ensuring any computer systems that are assigned for their use are kept physically secure. This requires particular vigilance for computer systems taken off campus.
- Ensuring computer systems assigned for their use have up-to-date and legally purchased anti-virus software active.
- Reporting to the head of Department/Unit any perceived breaches of Information Security at the University.

### **7.3 Students**

Students are responsible for...

- Using university provided computers only for the purpose of pursuing their approved course of study.
- Reporting any perceived breaches of Information Security to a member of staff.

### **7.4 Director, ITSC**

The ITSC Director is responsible for a number of services provided by ITSC, including the...

- Provision of computer systems generally available to students and staff of the University.
- Development and operation of network services interconnecting local departments and units, plus providing connectivity between campuses and the Internet.
- Negotiating of site license agreements for the widespread deployment of anti-virus software and other University wide Information Security software requirements.
- Development, management and ongoing review of the Information Security policies and procedures for the University, through the delegated authority of the Teaching, Learning and Information Services Management Board (TLISMB).
- Coordination and provision of training courses on Information Security for both staff and students, through Information Security Awareness training, dedicated training courses, seminars and other appropriate means.
- Responsiveness to incident reports and coordinate corrective action, as required.
- Distribution of security alerts from vendors and security agencies (such as HKCERT) as appropriate and when necessary.
- Undertaking of Risk Assessments and Business Continuity Planning for important central services.

- Definition of standards and guidelines for the secure operation of networks and computing systems throughout the University, including the selection of anti-virus software to be deployed on university computer systems.
  - Liaison with external security organizations, such as HKCERT and the Hong Kong Police Force.
  - Other Information Security duties, as required by the University.
- 

## 8.0 Privacy Policy

The University fully supports and where possible observes the internationally recognised standards of personal data privacy protection, in compliance with the requirement of Personal Data (Privacy) Ordinance. In doing so, the university will ensure all staff comply with the aforementioned Ordinance with the strictest standards of security and confidentiality, as stated in the [University Privacy Policy](#).

On-line information collection at the University's web page will adhere to the Personal Data (Privacy) Ordinance that states the purpose and use of the information collected.

More information on data privacy is available from [Hong Kong Personal Data \(Privacy\) Ordinance](#).

---

**Approved by:** Chair, Teaching, Learning and Information Services Management Board (TLISMB),  
Lingnan University

**Approval Date :** May 14, 2009

**Review Date:** May 2010

**Contact:** ITSC Director, Lingnan University

**Tel:** 2616 8398

**Email:** [mcdonell@ln.edu.hk](mailto:mcdonell@ln.edu.hk)

---

### Related Policies, Procedures and Forms:

#### Lingnan University

1. [Acceptable Use of University Computing Facilities](#)
2. [Information Services Risk Management, Business Continuity and Disaster Recovery Policies](#)
3. [Lingnan University Data Centre Access Policy](#)
4. [University Email Policy](#)
5. [Lingnan University Security Incident Management Guide](#)
6. [Regulations Governing Discipline of Students](#)
7. [Authorities and Guidelines for the Administration of Disciplinary Actions](#)
8. [University Privacy Policy](#)

#### General

1. [Information Security – website of the Office of the Government Chief Information Officer \(OGCIO\)](#)
  2. [System Administrators' Code of Ethics](#)
  3. [Security Incident Handling for Companies](#)
  4. [Hong Kong Personal Data \(Privacy\) Ordinance](#)
-