Lingnan University

INFORMATION SECURITY POLICY

Version 2.10

Document Classification:	Document Owner:	Publication Date:
Restricted	ITSC	10 Mar 2023

Preface

Background

To minimize the risk of improper management of the information assets of Lingnan University ("the University"), the Information Technology Services Centre (hereafter "ITSC") initiated a review of the Information Security Policies, following the Information Security Management System (ISMS) framework recommended by EDUCAUSE for higher education institutions, which is based on the ISO/IEC 27000 series of information security standards.

These policies are approved by the management of the University.

Corresponding guidelines and operating procedures have been developed, taking into consideration the availability of resources, feasibility and flexibility in operation, and efficiency in administration.

Revision History

Version	Prepared By	Approved By	Date	Revision
1.0	ITSC	TLISMB	14 May 2009	Initial version.
1.2	ITSC	TLISMB	20 Feb 2014	- Added an Appendix on Data Classification and Handling referenced in Section 3.3.7.2. - Revised Mobile Equipment/Wireless Device Security in Section 3.3.7.6.
2.0	ITSC	TLISMB	15 Feb 2017	2nd version to follow ISO 2700x standard.
2.1	ITSC	TLISMB	10 Nov 2017	- Revised password duration requirement on Section 8.3.1
2.2	ITSC	TLISMB	12 Oct 2018	- Modified the requirements of performing periodic review of the Information Security policy in A.5 - Added a section for an organization of Information Security (A.6) - Re-numbered the section numbers - Modified the Asset Inventory requirements in Section 3.3.4 - Added adoption of two-factor authentication in Section 8.4 - Modified the scope of the assessment in Section 17.2 - Modified the periodic vulnerability scanning requirements in Section 17.7 and 17.8 - Modified the software installation policy in Section 18.2 - Modified the Intellectual Property Policy in Section 28.3
2.3	ITSC	TLISMB	25 Apr 2019	- Added source of reference for the account locking on multiple failed attempts in Section 8.3.4
2.4	ITSC	TLISMB	5 Dec 2019	- Grouped All Revision History - Revised all section numbering - Updated team name from Desktop Computing to User Services in Section 1.4 - Added Department Accounts access control in Section 7.5 - Added Contractor and Third-party Accounts access control in Section 7.6 - Revised change password regularly requirement in Section 8.1.5 - Added change default password requirement in Section 8.2.3 - Added shared administrator account restriction in Section 8.2.5 - Added disable inactive administrator accounts in Section 8.2.6 - Added second 2FA authentication method in Section 8.4.1 - Added more prohibited use type in Section 21.1.5

				- Revised Email Quota Checking path and URL in Section 21.2.2 - Revised NDA content and format in Section 22
2.5	ITSC	TLISMB	2 Dec 2020	- Added a guideline on security measures implementation in Clause 12.8. - Revised software audit procedures in Section 18.3 - Added alumni email accounts control in Section 21.3.3 - Added other email account types control in Section 21.3.4
2.6	ITSC	TLISMB	18 Feb 2021	- Revised Intellectual Property Policy in Section 28
2.7	ITSC	ISMB	1 Dec 2021	- Revised the Code of Practice URL in Section 3.8 - Updated the name “Account administrator” to “Custodian” in Sections 7.5 and 7.6 - Added the Hostel staff family member accounts Access Control in Section 7.7
2.8	ITSC	ISMB	28 Feb 2022	- Update the IS organization, replacing “Teaching, Learning and Information Service Management Board” with “Information Service Management Board” in section 1.1 - Update the title of CIO in sections 1.2 and 1.3 - Added handling for staff with connected contract in Section 2.5.4 - Revised the reviewer title from “ITSC Director” to “CIO and University Librarian” in Section 20.9.1
2.9	ITSC	ISMB	5 Dec 2022	- Change document classification from “Internal” to “Restricted” on the cover page - Update of vulnerability assessment remediation timeframe in section 17.3.3 - Update of vulnerability assessment remediation action in 17.4.2 - Remove the non-applicable policy in section 17.5 - Revise the section number of sections 17.6 through 17.8 - Update the link of Intellectual Property Policy in section 28.1
2.10	ITSC	ISMB	10 Mar 2023	- Revised ITSC teams’ names in section 1.4 - Revised the standardized configuration requirements in section 23.6.3 - Added campus network connection requirements in section 23.6.4

A. Information Security Policy Statement

These information security policies provide high-level rules and principles of governance and control of information security for the University. They are based on the most crucial security components of "Confidentiality", "Integrity" and "Availability", and the "CIA triad" of information security. They also follow the Information Security Management System (ISMS) framework defined in the ISO/IEC 27000[1] series on information security standards, and cover the key areas listed below.

Key Areas in ISO 2700x Information Security Standards (ISO control reference number)	
Information Security Policy (A.5)	
Organization of Information Security (A.6)	1. Internal organization
Human Resources Security (A.7)	2. Human Resources Security Policy
Asset Management (A.8)	3. Information Asset Management Policy 4. Information Asset Handling Procedures 5. Security Disposal Policy 6. Removable Storage Usage Policy
Access Control (A.9)	7. Access Control Policy 8. Password Management Policy
Cryptography (A.10)	9. Cryptography Control Policy
Physical and Environmental Security (A.11)	10. Physical and Environmental Security Policy* 11. Clear Desk and Clear Screen Policy
Operation Security (A.12)	12. Operation Security Policy 13. Change Management Policy 14. Back-up & Recovery Policy 15. System Log Management Policy 16. Virus Protection Policy* 17. Vulnerability Assessment Procedures* 18. Software Audit Management Policy* 19. System Audit Policy
Communications Security (A.13)	20. Network Access Control Policy* 21. Email Communication Policy* 22. Confidential Non-Disclosure Agreement

1 ISO/IEC 27000, **Information Security Management System – Family of Standards**, Joint Technical Committee, International Organization for Standardization and International Electrotechnical Commission, 2013.

System Acquisition, Development and Maintenance (A.14)	23. System Acquisition, Development and Maintenance Policy
Supplier Relationship (A.15)	24. Supplier Management Policy
Information Security Incident Management (A.16)	25. Information Security Incident Management and Handling Policy
Business Continuity Management (A.17)	26. Business Continuity Management Policy
Compliance (A.18)	27. Compliance Policy 28. Intellectual Property Policy

* Existing information security policies.

Detailed control objectives are stated as a standard requirement in the corresponding documents. The words 'shall' and 'must' indicate mandatory requirements in the policies, while 'should' indicates a requirement for good practices that should be implemented whenever possible.

Information Security Policy (A.5)

A set of policies on information security shall be defined, approved by management, published and communicated to users, including staff, students, contractors and relevant external third party users. Information Security Officer shall review the Information Security Policies annually or whenever there are significant changes to ensure the continuity of suitability, adequacy and effectiveness. Information Security Officer shall disseminate the Information Security Policies to the appropriate parties to ensure all University personnel understand their applicable security requirements.

Organization of Information Security (A.6)

To establish a structured management framework to initiate, direct, monitor and control the implementation and operation of information security within Lingnan University. Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

Human Resources Security (A.7)

Users, including staff, students, contractors and external third party users, shall understand their roles and responsibilities in reducing risk of human error, theft, fraud or misuse of information assets and facilities.

Appropriate security measures shall be applied throughout an individual's employment within the University, including awareness training during the employment period and security responsibilities and duties after the termination of employment.

They should be made aware of any information security threats and concerns, of their responsibilities and liabilities, and should be equipped to support information security in the course of their normal work.

Asset Management (A.8)

Appropriate levels of protection and accountability shall be maintained for information assets in accordance with the sensitivity, criticality and values of those assets, regardless of the media in which they are stored, the manual or automated systems that process them or the methods by which they are distributed.

Ownership of Information Assets shall be defined and an inventory of Information Assets shall be maintained. Information Assets based on sensitivity, criticality and values have been classified as "**Highly Confidential**", "**Confidential**", "**Restricted**" and "**Public**".

Rules for acceptable use of information assets, return of the assets upon termination of employment and use of removable storage devices shall be identified, documented and implemented.

Roles and responsibilities of different levels of user including "Data Owner", "Data Manager" and "Data User" shall be defined to protect information assets from unauthorised access, modification, destruction or disclosure.

Removable storage device management, and disposal, labelling and handling procedures for information assets should be developed and implemented.

Access Control (A.9)

Access control to information and information processing facilities shall be properly established, documented, reviewed and enforced. Business processes shall be controlled and maintained on the basis of business and security requirements, with appropriate procedures in place.

User access to network resources shall be properly managed, documented and reviewed, including request, authorise, establish, issue, suspend and close, to prevent any possible unauthorised access.

Secure authentication information such as password management shall be established and the use of privileged utility shall be controlled. Access to information and application systems by privileged accounts shall be monitored, logged, restricted and controlled.

Passwords shall be changed periodically; a strong complex password consisting of case sensitive alphanumeric characters must be used. Password history, password aging and account lockout shall be applied to protect the account from password guessing.

Cryptography (A.10)

A policy on the use of cryptographic controls for the protection of the authenticity and integrity of information shall be developed and implemented.

A policy on the use, protection and lifetime of cryptographic keys through their whole lifecycle shall be developed and implemented.

Physical and Environmental Security (A.11)

A policy on the use of "Secure Areas", where data, information, facilities and equipment should be securely housed for the processing of information for the University, shall be defined and developed. The protection of these areas shall include physical entry control, prevention of unauthorised physical access, physical protection against natural disaster, attack or accident, protection against loss or damage of information, and protection against any kind of interference or interruption.

Physical entry control includes access to delivery and loading areas and visitors' visits shall be controlled, supervised, escorted and recorded. Equipment, storage media and cabling shall be protected and maintained both on-site and off-site.

Operations Security (A.12)

Appropriate roles and responsibilities, guidelines and/or procedures shall be defined and documented for the management and operation of information processing facilities. Appropriate back-up and recovery, change management control, capacity management, virus and malware protection and operation control shall be implemented.

Appropriate logging information, security control of software installation, technical vulnerability management and system audit control shall be implemented to maintain the confidentiality, integrity and availability of information in line with third party service delivery agreements.

Communications Security (A.13)

Network resources and services shall be segregated, documented, controlled and protected in a proper manner to protect information in systems and applications. Appropriate controls with policies, procedures and agreements shall be in place to protect the transfer of information through communication facilities.

Appropriate encryption and/or protection shall be in place to protect any sensitive "Highly Confidential" or "Confidential" information being transferred by any kind of electronic messaging, such as email, social media or instant messaging. Non-disclosure agreements with external parties shall be required.

Information Systems (A.14)

Information security elements shall be integral parts of information systems during acquisition, development, testing and maintenance. Appropriate controls on data input, processing and output should be implemented. Cryptographic techniques should be applied to protect the confidentiality, authenticity and integrity of information. Information systems projects and support activities should be conducted in a secure manner.

Supplier Relationship (A.15)

Information security requirements and mitigation of any risks associated with the University's information assets should be addressed in the supplier agreement. Appropriate monitoring and review of supplier services should be implemented and service delivery should be audited on a regular basis.

Information Security Incident Management (A.16)

Incident reporting and handling procedures shall be in place to ensure that information security incidents and weaknesses associated with information systems are communicated effectively to allow timely corrective action to be taken.

Responsibilities and procedures shall be set out for all staff, students, contractors and third party users, whereby they should be made aware of the procedures for reporting different types of incidents and weaknesses that might have an impact on the security of information assets.

Security incidents shall be responded to in accordance with the procedures, and the collection of evidence, such as the identification, collection, acquisition and preservation of information, shall be defined and included. Knowledge obtained from information security incidents shall be used to prevent the occurrence of similar incidents.

Business Continuity Management (A.17)

The information security requirements and the continuity requirements of information security management for critical business processes in the defined adverse situation shall be determined, planned and implemented. Appropriate measures should be defined to verify, review and evaluate the information security continuity in the defined adverse situation. Sufficient redundancy facilities shall be implemented to meet the availability requirement.

Compliance (A.18)

Users shall observe the information security policies and standards, as well as the relevant legal, contractual and regulatory requirements. Procedures shall be implemented to ensure information protection and to comply with corresponding policies, including those dealing with intellectual property rights and with personal data privacy

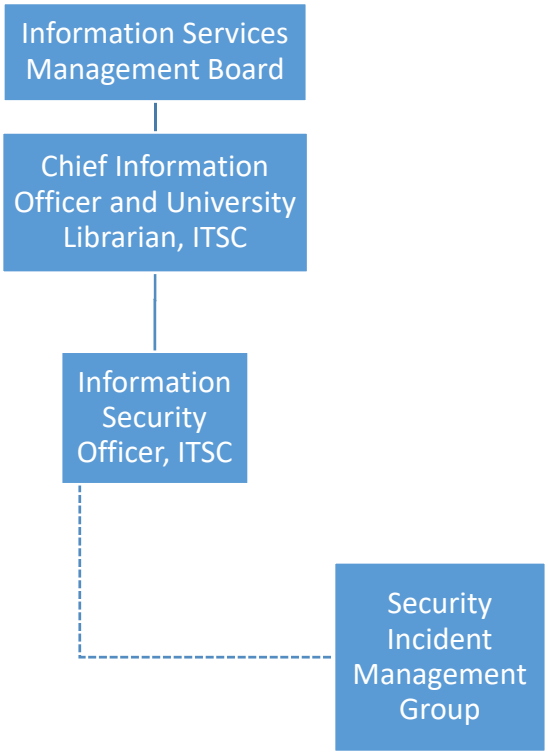
protection.

Independent information security audits should be performed to monitor compliance with this Policy and with the legal, contractual and regulatory requirements.

B. Information Security Policies

1. Internal Organization

To establish a structured management framework as follows to initiate, direct, monitor and control the implementation and operation of information security within Lingnan University. Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.



1.1 Information Services Management Board

The Board makes policy recommendations on the strategic development and advancement of information services of the University. It allocates funds provided by the University for the operation of all departments and programmes in areas related to information technology and library service. It also deals with any other matters relating to information services.

1.2 Chief Information Officer and University Librarian

Chief Information Officer and University Librarian (CIO and University Librarian) is to provide vision and strategic leadership in leveraging the latest information technologies to provide excellent IT services to support the mission and vision of the University. She will direct the development and oversee the management of different units in ITSC and partner with different academic and administrative units of the University to introduce the best IT initiatives to the community.

1.3 Information Security Officer

Reporting to CIO and University Librarian, the Information Security (IS) Officer works closely with other Team Leaders and Senior Executives in the ITSC to ensure the overall information security in campus. The major responsibility of the position is to assist the CIO and University Librarian in overall institutional information security strategy, policy formulation as well as the promotion and enforcement of the said policies. This position will oversee and recommend endpoint security and data loss preventive solutions, information security assessment, planning, implementing and managing security protection measures for the University electronic resources, central IT infrastructure and campus network; as well as handling security breach incidents and subsequent investigations, and University-wide information security awareness promotion.

1.4 Security Incident Management Group (SIMG)

The Security Incident Management Group is responsible for carrying out investigation, management and reporting of IS incidents, IS vulnerability & weaknesses analysis, liaising with different departments on IS compliance and operational issues. The group is led by CIO & University Librarian and consists of Information Security Manager, and all team leaders in the Sections of Application Development, Infrastructure Services and System and User Services.

2. Human Resources Security Policy

2.1 Staff members, students, contractors and third party users shall understand their responsibilities and must be suitable for the roles they are considered for in the 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.

2.2 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 Departments / Units.

2.3 Staff Members during Employment

2.3.1 Staff members shall be aware of information security threats and concerns, and of their responsibilities and liabilities. They are expected to be properly equipped to support the University in the course of their normal work or studies, and to reduce the risk of human error.

2.3.2 The University is responsible for ensuring that all the staff members comply with the Information Security Policies.

2.3.3 All staff members should receive appropriate information security awareness training and regular updates on the Information Security Policies relevant to their job functions.

2.3.4 Staff members who have committed a security breach are subject to disciplinary action.

2.4 Students, Contractors and Third Party Users during Engagement

2.4.1 Students, contractors, and third party users shall be aware of information security threats and concerns, and of their responsibilities and liabilities. They are expected to be properly equipped to support the University in the course of their normal work or studies, and to reduce the risk of human error.

2.4.2 Students, contractors, and third party users should receive appropriate information security awareness training and regular updates on the Information Security Policies relevant to their job functions, whenever it is possible.

2.4.3 The University should communicate with all students, contractors, and third party users to ask them to comply with the University's Information Security Policies.

2.5 On Terminations or Change of Employment / Engagement

2.5.1 Staff members, students, contractors and any third party users shall exit or change their employment / engagement relationship with the University in an orderly manner.

2.5.2 Staff members, students, contractors and any third party users must return all of the University's assets in their possession in a condition acceptable to the University upon termination of employment, or of academic and contractual relationships.

2.5.3 Access rights to information and/or information resources shall be removed or de-activated upon termination of employment, or of academic and contractual relationships.

2.5.4 Staff with a valid connected contract only can apply for account retention before their existing contract expired to keep their data in the system until the new contract commenced. Otherwise, data in the staff account will be removed after the expiry of their employment contract. The applications for account retention shall be endorsed by the Department head and approved by the CIO and University Librarian. The staff account shall be disabled and no access is allowed during the transition period.

3. Information Asset Management Policy

Users including staff, students and external third party users shall be responsible for protecting the University's assets from unauthorised access, modification, destruction or disclosure, whether accidentally or intentionally. To facilitate the protection of assets, users' responsibilities shall be established at three levels as described below: Data Owner (hereafter "Owner"), Data Manager (hereafter "Manager") and Data User (hereafter "User").

3.1 Data Owner

An officer of a business unit where information is created, or one who is the primary user of the information.

Owners shall be responsible for:

- determining the classification for the set of information;
- determining and overseeing the implementation of all the necessary security requirements for a set or sets of information;
- reviewing the appropriateness of classification periodically and regularly;
- defining and implementing appropriate safeguards to ensure the confidentiality, integrity and availability of the information resource;
- monitoring safeguards to ensure their compliance and reporting situations of non-compliance;
- authorizing access to those who have a business need for the information;
- removing access from those who no longer have a business need for the information;
- implementing corrective and preventive action to rectify non-compliance with the information security policies;
- protecting and using a set of information;
- controlling access to information;

Owners may assign administrative and operational responsibility to one or more Data Managers, each responsible for different functions.

3.2 Data Manager

An officer designated by the Owner to control the access to information or an information system by maintaining the safeguards established by the Owner.

The Manager shall provide administration, maintenance and protection of information, including systems and hardware, storage and transmission of information.

The Manager shall ensure the information can only be available to and accessed by the authorised users designated by the owner and shall prevent any unauthorised access, data loss or data leakage to any unauthorised third parties.

3.3 Data User

Users authorised by the Owner to access and work with the information to carry out their job duties while using the safeguards established by the Owner.

The User shall take good care of information assets and shall not disclose them to any unauthorised third parties while taking steps to prevent any possible data loss.

3.4 Building the Asset Inventory

The Information Security Officer shall be responsible for maintaining appropriate protection of organization's IT assets and ensure all information and assets associated with information processing facilities shall be assigned to an owner to establish, maintain and safeguard the assets, review the asset inventory once a year, arrange reassessment of the asset classification, if necessary, and update the asset inventory with newly purchased assets and their classification levels.

3.5 Classification of Assets

The Owner shall use a formal review process to classify information into one of the following four classes: Highly Confidential, Confidential, Restricted and Public.

Highly Confidential

"Highly Confidential" information is information that through unauthorised disclosure, modification or destruction could cause serious damage to the University, or it could cause the University to face legal action or penalties or reduce the University's competitive advantage.

"Highly Confidential" information is highly sensitive and accessible only to a limited number of staff. The Senior Management shall grant access rights on an individual basis, and information shall be subject to strict rules of use.

Examples of "Highly Confidential" information include police/ICAC investigations, legal cases, information on examination misconduct cases, access control data, meeting papers (with sensitive information) of Council and Council Committees, Management Boards and Senate.

No “Highly Confidential” information shall be transmitted over or stored on non-encrypted electronic media or systems.

Confidential

“Confidential” information is important day-to-day operational data or sensitive personal particulars intended for use within the University only. The unauthorised disclosure, modification or destruction of the information might have an adverse impact on the University.

This information shall be accessible to certain groups of staff who have a valid business need. Access rights shall be granted by the information owner on an individual or group basis.

Examples of Confidential information include sensitive personal data (e.g., name, HKID number, passport number, age), contracts that contain non-disclosure provisions, examination papers (before examination), answers (before examination), marking guidelines (before examination), server/database passwords, student and staff information (e.g., personal information, medical information, compensation and benefits information, performance appraisals, records of disciplinary action), meeting minutes of Council and Council Committees, Management Boards and Senate, and departmental budgets and accounts.

Restricted

“Restricted” information is available to some or all the staff who have operational needs to use it. External access to this information shall be prevented. Unauthorised disclosure, modification or destruction of this information may not cause significant harm or embarrassment to the University. Access to this information shall be granted by the information owner.

Examples of “Restricted” information include non-confidential circulars, standards or procedures for internal use.

Public

“Public” information is information that has been made available for public distribution through authorised University channels. This information is available to anyone inside or outside the University. Access to public information is unrestricted.

Examples include marketing brochures, marketing presentations, news releases, prospectuses and annual reports.

3.6 Declassification

The Information Security Officer and Owners shall review annually all classified assets, and reclassify those items which no longer meet the criteria established for such assets.

3.7 Reclassification

The Owner shall change the classification of an asset to match changes in the impact that its unauthorised disclosure, modification or destruction would have. Upon changing the classification, the Owner shall increase, decrease or remove the classification as appropriate and shall notify the Information Security Officer and affected users.

3.8 Other References:

- Data Access Guidelines for Business Intelligence (BI) System (approved by TLISMB in May 2016) (http://www.ln.edu.hk/file/itsc/policy/data-access-guidelines-for-bi-system.pdf)
- Banner System Access, Data Classification and Security Policy (http://www.ln.edu.hk/file/itsc/policy/banner-system-access-security-policy.pdf)
- Code of Practice for Handling Personal Data (https://www.ln.edu.hk/dpp/code-of-practice)

4. Information Asset Handling Procedures

4.1 Labelling Procedures

Different classification of information requires different labelling procedures to ensure a sufficient level of confidentiality, integrity and availability. The following labelling procedure is defined for different medium.

Medium	***Labelling Procedure***
Hard copies	Add a "*Highly Confidential" or "Confidential"* stamp to documents with those classifications.
Emails	Add the word "*Highly Confidential" or "Confidential"* in the subject line for an email with those classifications.
Soft copies	Indicate "*Highly Confidential" or "Confidential"* for documents with those classifications.
Data, databases and business applications	Indicate "*Highly Confidential" or "Confidential"* on screen displays and in reports with those classifications that are generated by IT systems as far as feasible. When printed out, these items should be labelled according to the procedure for hard copy documents.
Other media (floppy disks, CDs, DVDs, videocassettes, USB and electronic removable storage device etc.)	Add a "*Highly Confidential" or "Confidential"* adhesive label on the media with those classifications. Display a message indicating the "*Highly Confidential" or "Confidential"* classification when the information stored on the media is accessed.

4.2 Information Asset Handling Procedures

Different classification of information require different handling procedures to ensure a sufficient level of confidentiality, integrity and availability. The following are different requirements for password protection or encryption for different data classes.

Accessing, Processing and Tracking				
	Highly Confidential	***Confidential***	***Restricted***	***Public***
Granting access rights	Senior management approval [1]	Data Owner approval	Data Owner approval	No restriction
Release to external party	Senior management approval [1] Non-disclosure agreement signed	Data Owner approval Non-disclosure agreement signed	Data Owner approval	No restriction
Processing	Clear desk, clear screen guidelines	Clear desk, clear screen guidelines	No restriction	No restriction
Tracking	Keep records of recipients, copies made, locations, addresses, those who view it and destruction	Keep records, especially of mobile electronic storage devices containing personal identifiable information	No restriction	No restriction

Reproduction, Distribution and Disposal					
		Highly Confidential	***Confidential***	***Restricted***	***Public***
Copy		Senior management approval [1]	Data Owner approval advised	No restriction	No restriction
Fax	Paper	Attended receipt [2]	Attended receipt [2]	No restriction	No restriction
	Electronic	Password protected recipient mailbox	Password protected recipient mailbox	No restriction	No restriction

Paper or postage mail delivery		Sealed opaque envelope with address to specific person, and delivery by hand or by approved courier	Sealed envelope	No restriction	No restriction
Disposal	Paper	Shred or put in a secure disposal bag	Shred or put in a secure disposal bag	No restriction	No restriction
	Electronic storage devices	Follow the secure disposal policy			No restriction

Password Protection or Encryption					
		Highly Confidential	***Confidential***	***Restricted***	***Public***
Storage on fixed devices		Required	Required as far as feasible [4]	No restriction [3]	No restriction
Storage on mobile devices		Required	Required	Required	No restriction
Electronic delivery	Internet	Required	Required	No restriction [3]	No restriction
	Intranet	Required	Required as far as feasible [4]	No restriction [3]	No restriction

Notes:

[1] Senior management of the University refers to the President, Vice-President and Associate Vice-President. They can delegate the power to the Head of Departments/ Units/Deans/Directors to grant access rights, to release to third parties and to copy Highly Confidential data for a particular data item or groups of items. This needs to be done once at the beginning.

[2] Sender should notify the recipient before faxing any Confidential or Highly Confidential document.

[3] No password protection or encryption would be necessary at the document level if there is already password protection on the fixed devices.

[4] Required as far as feasible: some massive data files for individual staff or students that require massive decryption keys that become unmanageable data and encryption keys are examples of exceptions.

5. Security Disposal Policy

5.1 Data Owners are responsible for overseeing information and disk disposal in each department or unit. ITSC shall provide a secure deletion program so that users may thoroughly dispose of electronic storage devices.

5.2 An electronic storage device containing “Confidential” or “Highly Confidential” information should be at least erased by a secure deletion program to ensure all “Confidential” or “Highly Confidential” information is not left on the media for restoration.

Storage Device	***Clear / Wipe***	***Sanitize (if containing “Confidential” and “Highly Confidential” information)***
Non-removable hard drive	1	2 or 3
Tape	3 or 4	3 or 4
Floppy disks	1 or 3	4
Removable storage devices (e.g. USB flash drive)	1 or 3	2, 3 or 4
CD-RW	1	4
CD-ROM / CD-R / DVD	4	4

1 = overwrite, 2 = secure deletion program, 3 = degauss (demagnetize), 4 = destroy

6. Removable Storage Usage Policy

6.1 Users shall ensure that “Highly Confidential” or “Confidential” information stored on any removable storage device (including any mobile device with storage capacity) is properly protected by a data encryption solution provided by the University.

6.2 Authorization from the owner shall be required for storing “Highly Confidential” or “Confidential” information on a removable storage device. The approving officer should assess the need for such storage, the associated security risks and the adequacy of security controls.

6.3 Users shall only store the minimum “Highly Confidential” or “Confidential” information necessary for operational needs on a removable storage device and record the nature and amount of sensitive information stored.

6.4 “Highly Confidential” or “Confidential” information on removable storage devices shall be properly protected and handled. All “Highly Confidential” or “Confidential” information should be removed from the removable storage device immediately after use in accordance with the Information Labelling and Handling Procedure.

6.5 Users shall keep the removable storage device under continuous, direct supervision when in use, and detach the device from computers and store it in a safe location.

7. Access Control Policy

7.1 User Access Management

7.1.1 Access to information shall be managed in accordance with established procedures for requesting, authorizing, establishing, issuing, suspending, closing and regularly reviewing user accounts and access rights.

7.1.2 The University should set up and maintain role-based access control for the network, systems, applications and information under its administration.

7.1.3 User accounts and access rights shall be regularly reviewed to determine their suitability.

7.2 Network Access Controls

7.2.1 Access to the intranet or Internet shall only be provided to users who have a legitimate business need for such access.

7.2.2 Caution shall be exercised when accessing websites of unknown origin, and no programs or executable files shall be downloaded from an unsecured site.

7.2.3 Documents and files downloaded from the Internet shall be scanned with up-to-date antivirus software before use, and downloaded software should be tested on a stand-alone testing machine.

7.2.4 The University network resources and services shall be segregated into a demilitarized zone and internal zones according to the risks faced by and the sensitivity of these resources and services.

7.2.5 External access to administrative, diagnostic and configuration interfaces of network equipment shall require stringent user identification and authentication, and shall only be initiated from a trusted location and by using strong, secured network access and cryptography control (e.g. VPN, registered IP address and registered computer name).

7.3 User Access Controls

7.3.1 Users shall uniquely identify and authenticate themselves for access to systems.

7.3.2 Any software which can override system security shall be removed from operating systems.

7.3.3 After a predefined period of inactivity, user sessions shall be locked and shall require re-authentication to unlock.

7.3.4 The connection period for each session for high-risk applications should be limited.

7.3.5 User access activities should be logged, reported, reviewed and the controls should be appropriately heightened on a regular basis to identify and resolve incidents involving unauthorised activities. Access to log files should be granted on a need-to-know basis.

7.3.6 Faults reported by users or by system programs relating to problems with the systems should be logged and analysed, and any related action should be properly recorded for tracking under the incident and problem management policy.

7.4 Information Systems Access Controls

7.4.1 User shall be provided with access to applications only on a need-to-use basis.

7.4.2 Sensitive applications shall be installed and operated in a dedicated computing environment.

7.5 Department Accounts Access Control

7.5.1 Departments shall apply for the creation of department accounts for communication and access to various resources to complete the work they required.

7.5.2 A full-time staff from the department should be assigned as the custodian of the department account.

7.5.3 The custodian of the department account is responsible for monitoring the usage of the account and serving as the single communication point of the account.

7.5.4 In the event of the resignation of the custodian, a replacement staff should be supplied. Department account without a valid custodian shall be suspended without prior notice.

7.5.5 An expiry date will be set for each department account; custodian should review the usage of the account upon expiration and applied for an extension if needed. If the department fails to apply for an extension of the account, the account will be disabled upon expiry.

7.5.6 The expiry date should be not more than 2 years from the creation date or the last extension date.

7.6 Contractor and third party accounts Access Control

7.6.1 Departments shall apply for the creation of contractor or third party accounts for contractor or external parties to access the systems to complete their assigned tasks.

7.6.2 A full-time staff from the department should be assigned as the custodian of the contractor and third party accounts.

7.6.3 The custodian is responsible for monitoring the usage of the accounts and serving as a single communication point of the accounts.

7.6.4 A replacement staff should be supplied by the Department as a replacement if the custodian has resigned. Contractor and third party accounts without a valid custodian shall be suspended without prior notice.

7.6.5 An expiry date will be set for each contractor and third party account; the expiry date should match with the contract completion date or the project end date. The department needs to apply for an extension if extra time is needed or a new contract is signed.

7.6.6 A contractor or third party account should not access any other systems in the University other than what they need to complete their task.

7.7 Hostel staff family member accounts Access Control

7.7.1 Hostel wardens and senior tutors of Lingnan University shall apply for the creation of accounts for their family members living in Lingnan University hostel for connecting to the University Wi-Fi service and accessing the Internet.

7.7.2 The hostel warden or senior tutor is assigned as the custodian of their family member accounts.

7.7.3 The hostel warden or senior tutor is serving as a single point of contact for their family member accounts.

7.7.4 If the warden or senior tutor no longer works in the hostel or leaves the University, their family member accounts will be terminated immediately without prior notice.

7.7.5 Hostel wardens and senior tutors shall renew their family member accounts every 2 years. Non-receipt of the renewal application will result in termination of the family member accounts.

7.7.6 Wardens and senior tutors shall apply for termination of their family member account should their family member(s) has(ve) moved out from the Lingnan University hostel.

7.7.7 Hostel wardens and senior tutors should apply one account for each family member. Shared account is prohibited.

7.7.8 Family member accounts can only access the Internet within the hostel buildings and should not be able to access any other restricted systems in the University.

7.7.9 The guests of wardens or senior tutors are recommended to use guest Wi-Fi account in case they need Internet access during the visit; sharing the staff account and family member account is prohibited.

8. Password Management Policy

8.1 Password Policy for General User

8.1.1 The same password shall not be used for University accounts and non-University system access (e.g., personal ISP account, option trading, and benefits).

8.1.2 Users shall not disclose passwords to anyone (e.g., supervisors, administrative assistants, secretaries or family) by any means in any circumstances.

8.1.3 Users shall not use the Remember Password feature of applications (e.g., Internet Explorer, Google Chrome and Mozilla Firefox).

8.1.4 Users shall not store passwords in any physical location or on any computer system (e.g., electronic storage devices, mobile phones or tablets etc.) without encryption.

8.1.5 User should change their passwords regularly and shall not re-use a specified number of previous passwords.

8.1.6 If an account or password is suspected to have been compromised, users shall report the incident to the Information Security Officer and change the relevant password.

8.1.7 Password guessing or cracking may be performed on a periodic or random basis by the Information Security Officer. If a password is guessed or cracked, the user shall change it.

8.2 Password Policy for System Administrator(s)

8.2.1 System Administrator(s) shall have two sets of user account: one granted with general user privileges and the other with system privileges which allow the System Administrator to perform daily administration work.

8.2.2 System Administrator(s) shall use the general user account for daily non-system administration work.

8.2.3 The system default administrator or root account password should be changed at the start of using the account and kept in a safe location by the system owner or an authorised person designated by the system owner.

8.2.4 User accounts that have system-level privileges granted through group memberships or programs such as “sudo” shall have a unique password different from all other accounts held by that user.

8.2.5 Each system administrator should have their own system privilege login account whenever possible, shared administrator account should be avoided. Administrators should use their own system privilege account to perform the daily administration work.

8.2.6 The default administrator or root account should be set as disable if the account is not in use.

8.3 Password Rules

8.3.1 A password shall expire and it shall be changed periodically or whenever necessary.

8.3.2 A new password shall be at least 8 alphanumeric characters in length.

8.3.3 A new password shall contain at least one alphabetic (in lowercase or UPPERCASE) and one numeric character.

8.3.4 An account shall be locked after multiple failed attempts according to ITSC's operating guideline for setting the number of failed attempts in the Banner and other related systems.

8.3.5 The last 3 passwords used must not be re-used.

8.4 Adoption of Two-Factor Authentication (2FA)

Two-factor authentication adds a second layer of security protection to Lingnan online accounts. This second form of authentication helps to prevent unauthorized access to an account even if the password is compromised.

8.4.1 All staff and students are required to use the 2FA's mobile app or the ByPass Code as a method of two-factor authentication whenever the computer systems have deployed 2FA as an authentication mechanism.

8.4.2 Staff and students shall register the 2FA accounts via the 2FA services management websites and maintain their records accurately.

8.4.3 Staff and students shall update their 2FA records via the 2FA services management websites as soon as possible in case their phone was lost or a new mobile phone is bought for replacement.

9. Cryptography Control Policy

9.1 Only proven encryption standard algorithms (such as AES, Triple DES, Blowfish and PGP) shall be used to protect any information in the University.

9.2 Any Electronic Certificate (e-Cert) shall be well protected in the proper safeguarded facilities and the e-Cert shall be handled with care during use.

9.3 When using the Electronic Certificate (E-Cert)

- 9.3.1 It shall be used for encryption or digital signature only.
- 9.3.2 It shall be well protected in the proper safeguarded facilities, and shall be handled with care during use.
- 9.3.3 It shall not be shared / exported / distributed.
- 9.3.4 Users shall change the encryption password or pass-phase regularly for a document.
- 9.3.5 Users shall not send the encryption password or pass-phase through the Internet in plaintext.

9.4 The integrity and authenticity of public asymmetric keys (such as e-Cert) shall be established and maintained, and be verifiable.

9.5 Keys and key generation processes shall not be disclosed at the time of selection.

9.6 Leakage of information about the key and errors in its transcription shall be minimized during the installation of the key in the device or during the process that is going to use it.

9.7 Cryptographic keys shall be transmitted in a channel separate from that for encrypted data transfer.

9.8 Cryptographic keys shall be used for a predetermined lifetime and shall be regenerated periodically.

9.9 Cryptographic keys intended for encrypting keys cannot be used for data.

10. Physical and Environment Security Policy

This Physical and Environmental Policy is a sub policy of the Information Security Policy and sets out the principles describing the mechanisms and requirements required to achieve physical and environmental security in the data centre(s) / server room(s) of the University.

10.1 Policy Statement

10.1.1 The University will protect its information systems, information resources and members from environmental hazards or threats, including but not limited to the following:

- Water leakage
- Power surge / loss
- Electric shocks
- Fire
- Typhoon

10.2 Equipment Security

10.2.1 Computing equipment should be placed away from glass windows to avoid the computer equipment being revealed to outsiders and vulnerable to various natural disasters such as typhoons.

10.2.2 Computing equipment should be properly installed in a server room(s) to avoid accidental knocking over.

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

10.2.4 Eating, drinking and smoking must not be allowed near the University's server room(s). Flammable materials must not be brought into the server room(s).

10.3 Cabling Security

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

10.3.2 Wherever possible, power and telecommunication lines should be installed at a high level (e.g. ceiling) or on a raised floor to allow better ventilation, and they should not be routed through a public area without proper protection. In existing premises where overhead cabling cannot be implemented, power and telecommunication lines should be protected by ducting from source to sockets.

10.4 Temperature, Humidity Control and Monitoring

10.4.1 7 x 24 air-conditioning equipment with humidity adjusting functionality must be implemented in the server room(s) of the University. The air-conditioning must be configured to maintain the room temperature and humidity within the normal operating range of the server hardware and other computing devices.

10.4.2 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 about abnormal temperature and humidity should be automatically communicated to the Facilities Management Division (FMD) or ITSC on a timely basis.

10.4.3 Regular tests of air-conditioning equipment, temperature and humidity control and monitoring devices should be conducted at least once a year to ascertain their effectiveness.

10.5 Power Protection

10.5.1 The University shall provide power protection to ensure 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 switch over to an alternative power source immediately upon loss of power.

10.5.2 UPS should be tested by the vendor at least once every three years to ascertain that the battery life can withstand a clean shutdown of the University's critical information systems and can hold the necessary loads until the disaster recovery site is in operation.

10.5.3 Regular monitoring of the output load of the UPS should be performed to avoid and detect overloading issues. Physical access to the UPS facility, including battery and cable connection, shall be restricted to authorised personnel.

10.6 Fire, Smoke and Water Detection and Control

10.6.1 Fire, smoke and water detectors or alternative protection systems shall be properly installed within the server room(s) of the University to protect computing equipment from environmental hazards whenever feasible.

10.6.2 Wherever possible, appropriate segmentation of the fire suppression system should be used so that a fire in one area will not activate the system across the entire server room(s). In addition, regular inspection of the fire suppression system should be performed by the vendor at least once every three years.

10.6.3 Hand-held fire extinguishers should be strategically placed in the server room(s). Signs should be used to clearly indicate the location of hand-held fire extinguishers. Regular inspection of fire extinguishers should be performed by the vendor at least once every three years.

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

10.6.5 Alerts on occurrences of environmental hazards should be automatically communicated to IT operational staff or Facilities Management Division staff immediately.

10.6.6 Regular tests of fire and water detection and control devices should be conducted at least once a year to ascertain their effectiveness.

10.7 Entry Control

10.7.1 Physical access to the data centre(s) or the server room(s) should be controlled and restricted to specifically authorised persons only and their access rights should also be regularly reviewed and updated. All doors of the data centres should be protected against unauthorised access using appropriate access control mechanisms, such as a smart card control system.

10.7.2 Visitors to the University data centres should be escorted and their entrances and exits must be logged. In addition, access should only be granted for specific and authorised purposes. Visitor logs should be provided to detect any unauthorised or inappropriate visits in security audits upon request.

10.7.3 Wherever possible, CCTV equipment should be installed at appropriate locations to monitor the access activities at all entrance(s) of the data centres.

10.8 Evacuation / Activation Process

10.8.1 Adequate training should be delivered to members for correct operating and maintenance of the following equipment and devices:

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

10.8.2 Activation of the above equipment and devices (other than automatic systems such as fire suppression systems) should inform ITSC.

10.8.3 Evacuation criteria and procedures must be established by the University to protect human life in the presence of environmental hazards. Clear evacuation routes and signs should be placed in strategic locations in the server room(s).

11. Clear Desk and Clear Screen Policy

11.1 “Highly Confidential” or “Confidential” information in print format or on mobile computer devices and media shall be stored in suitable locked, fire-resistant cabinets or other secure furniture when not in use, especially outside working hours.

11.2 Computers and printers that are used to access, store, process and print any “Highly Confidential” or “Confidential” information shall not be left unattended without logout and shall be protected by key lock, password, authentication code or other controls when not in use.

11.3 Documents containing “Highly Confidential” or “Confidential” information shall be collected and removed from the equipment immediately after being faxed, printed or photocopied.

12. Operation Security Policy

12.1 All operational procedures should be documented and regularly reviewed and updated.

12.2 All servers should be updated and synchronized with the same time clock to avoid inconsistency in time records.

12.3 Testing activities should not be executed in the production environment.

12.4 The testing environment should be separated from the production environment.

12.5 Appropriate access control based on need-to-know shall be imposed and should be regularly reviewed and updated.

12.6 Back-up solutions shall be applied for both systems and data back-up.

12.7 Other system protection measures such as change control, capacity management, virus protection and malware protection should be implemented.

12.8 To protect the University system in the fast-changing cybersecurity landscape, ITSC may enforce, change or implement new security measures if deemed necessary, to detect, block, tagged, quarantine, remove the source of threats and to stop any attack activities.

13. Change Management Policy

13.1 The University shall maintain a set of IT change management procedures to control all changes to the IT system and the network infrastructure which may affect the confidentiality, integrity, availability, stability and usability of IT systems and services.

13.2 Any changes that affect the IT infrastructure (such as updating or changing the network, servers, firewall and database parameter) or environmental facilities (such as air-conditioning, humidity control, water and fire protection) shall be properly managed through scheduling, coordination, reviews, assessments and approval.

13.3 Formal change requests shall be properly raised, assessed, reviewed, approved and documented by the relevant parties before they can be implemented in the production.

13.4 The implementation processes shall be properly recorded and the implementation results shall be documented and updated on the approved change request documents.

13.5 Unauthorised changes to any of the IT infrastructural or environmental facilities are not allowed.

13.6 Any emergency changes to rectify any production problems shall be documented. Verbal approval shall be received from the management before implementation and formal approval from the management shall be obtained afterwards.

14. Back-up and Recovery Policy

14.1 All machines shall have full system back-up covering all the data as well as system files and data back-up in the machine covering daily activities.

14.2 The full system back-up should be conducted at least once a year and tested for restoration on another machine.

14.3 The data back-up should be conducted on a daily basis with at least the incremental back-up method.

14.4 All back-up jobs shall be recorded and logged.

14.5 Regular restoration tests should be conducted randomly to ensure the back-up media are functioning properly for data restoration.

14.6 The back-up media shall be kept in a secure location to prevent them from fire, water and magnetic problems, as well as from natural disasters.

14.7 The back-up media should be sent to off-site storage regularly to provide sufficient disaster recovery protection.

14.8 A back-up media checklist shall be maintained both on-site and off-site.

14.9 Regular back-up reports should be made giving the back-up status.

14.10 If data restoration is requested, proper authorization from the system owner shall be granted before the data is restored. Such restored data shall be handled as part of the production data.

15. System Log Management Policy

15.1 The appropriate log file (such as audit log, system event log and error log) shall be properly maintained for further audit purposes.

15.2 Log files for all systems, network devices, security devices and applications shall be able to provide user activity information (especially on transaction-related activities), system activity information and any error messages.

15.3 The log information shall be able to cover an agreed period of time (e.g. at least 6 months) for future investigations and access control monitoring.

15.4 The log information shall also include system administrators and/or system privileges account activities on the system to protect both the system administrator and the system.

15.5 Log files shall be well protected against any unauthorised access or tampering.

16. Virus Protection Policy

16.1 Any machine (including PCs and servers, whether using the Microsoft Windows operating system platform, Macintosh or other Unix/Linux operating system platforms) shall have appropriate antivirus software installed under a University software license whenever applicable.

16.2 Machines shall be configured to be updated automatically and regularly with up-to-date virus definition files through a central virus definition distribution server in order to protect them from virus infections or attacks.

16.3 Any removable media that will be used on PCs or servers in the University network must first be scanned to ensure that there is no virus resident in the media.

16.4 All email attachments or downloaded files shall be scanned before opening.

16.5 Users shall not turn off or disable the virus protection software on their machines at any time, and the system administrator shall not allow users to do so.

16.6 Regular virus scanning shall be implemented to ensure machines are free of viruses.

16.7 Anti-spam / anti-virus security solutions shall be used to filter infected files, attachments and spam email messages.

17. Vulnerability Assessment Procedures

17.1 Assessment Requirement

Vulnerability assessment shall be conducted on a regular basis (e.g. once a year for the annual audit review) to check for any non-compliance issues and to check for any unknown security vulnerabilities that may impact on the University in terms of financial loss, image problems or legal non-compliance.

17.2 Scope of the Assessment

The scope of the assessment should include but not be limited to web applications, networks, servers, desktops and WiFi equipment on the campus. ITSC will conduct scanning exercises on a regular basis. Desktop machines with a real IP address can be the victim of a cyber-attack even if the machine does not hold any network services.

17.3 Remediation

17.3.1 The results of scans shall be sent to the system owners and corresponding administrator.

17.3.2 Security vulnerabilities will be classified as “Critical”, “High”, “Medium” and “Low”. A draft report will be sent to the system owner and corresponding administrator so that immediate remedial action may be taken.

17.3.3 The system owner and corresponding administrator shall fix the vulnerability within the timeframe as defined in the assessment report.

17.4 Assessment Result

17.4.1 A final assessment result report should be submitted to the corresponding Head/Dean for record purposes. Alert messages should be sent to the corresponding Head/Dean in the event of long overdue security vulnerabilities.

17.4.2 Services and/or equipment could be forced to be shut down, isolated, quarantined or applied any other appropriate containment and remediation actions if the services and/or equipment failed to compile with the defined requirements of the assessment.

17.5 Detail Scanning Operation Procedures

17.5.1 Network Vulnerabilities Scan

17.5.2 All servers must pass the network vulnerabilities scan.

17.5.3 Web Application Vulnerabilities Scan

- A web application scan should be conducted immediately after a network scan to avoid duplicating manpower for remediation.
- The appropriate user credentials should be provided by the application owner before the web application scan.

- Testing machines should be considered for the first round of scanning to prevent any unexpected impact on the production application.

17.6 Scanning Schedule

17.6.1 Four scanning schedules are suggested, all of which should be arranged and scheduled appropriately to avoid any unexpected interruptions.

17.6.2 It is recommended to split the scanning into several separate batches so that there will be no serious adverse impact on daily operations if the scanning was to encounter problems.

17.7 Precautions and Rescanning

17.7.1 Before scanning starts, the corresponding network firewall and IPS protection should be configured.

- The scanner IP address should be added to the white list for scanning to prevent the packet blockage or dropped by the security devices.
- Protection should be re-enabled as soon as the first scan has been performed.
- A re-scan should be performed without configuring the security devices to check whether the protections are in place.

17.7.2 The scope of scanning should be prepared before scanning takes place.

17.7.3 Credential information may be required for web application, operation systems and network equipment vulnerability scans.

18. Software Audit Management Policy

This policy is designed to assist computer users to manage their computer software assets. Proper software management includes (i) establishing responsibility and software ownership, (ii) maintaining an accurate and updated software inventory, (iii) ensuring licensing compliance and (iv) centrally auditing and logging the installation of software in users' computers owned by the University.

18.1 Licensing and Copyright

18.1.1 Only properly licensed software should be installed on computers owned by the University. Software is categorized as follows:

- Freeware
- University license
- Departmental license (purchase record should be kept by the corresponding department)
- Personal license (purchase record should be provided by the user upon request)

18.2 Software Installation

18.2.1 Users who wish to install software on office computers other than the standard software / applications provided by the University must submit an application to ITSC. After proper endorsement from ITSC, ITSC will install the approved software for the users.

18.2.2 Software shall not be installed in University computers or computing equipment in such a way that may be deemed as inconsistent with applicable copyright laws or licensing agreements. Each individual license shall be installed on one computer only.

18.2.3 University computers shall not be used for copying, storing or transferring to other systems copyrighted or proprietary files, including multimedia and other data files, as well as application and utility software.

18.2.4 Peer-to-peer file sharing applications shall not be installed on University computers on the campus network except when it is a necessity for performing a user's job responsibility and then only with the consent and approval of ITSC and/or the respective Head of Department/Unit.

18.3 Software Audit Procedures

18.3.1 ITSC shall maintain the software inventory by auto-detection and/or inspection of all University computers.

18.3.2 ITSC will perform software audit annually to verify the information and software installed on the University computers. If illegal or unauthorized software was found on the University computer, ITSC shall arrange to remove the software from the computer.

19. System Audit Policy

19.1 The scope of the system audit shall be well planned.

19.2 The audit activities shall be performed periodically to ensure compliance with relevant policies and statutory requirements.

19.3 System audit requirements and activities involving verification of operational systems should be carefully planned and agreed to minimize disruption to business processes.

20. Network Access Control Policy

20.1 The policy is to provide guidance for acceptable use of network resources available to the University community. ITSC will be the sole provider of network resources for the entire University community.

20.2 The University is committed to providing a secure network infrastructure for teaching, learning, research and operational purposes. This policy shall apply to all staff members and students who have access to the network infrastructure, including the data, voice and video network access to the Internet. It shall also apply to all individuals using the network such as, but not limited to, alumni, visitors and contractors.

20.3 Basic Principles

20.3.1 The University network resources provide support for better teaching, learning, research and operations.

20.3.2 The network infrastructure is provided as a corporate service and reasonable access to the Internet is anticipated.

20.3.3 Whenever possible, the University will aim for effective use of network resources and encourage a paperless campus.

20.3.4 The use of network resources, which is funded through the block grant from the University Grants Committee (UGC), shall be governed by the funding principles of the UGC. Any self-funded bodies, such as the Community College or the Student Hostels, shall be allocated network resources according to the levies being charged.

20.3.5 Proper network segregation shall be in place to separate different groups of information services, users, information systems and locations.

20.4 User Rights and Responsibilities

20.4.1 Any person officially affiliated with the University, with a valid username and password, can access the network. It is the responsibility of the user to ensure that network resources are accessed in a fair and responsible manner.

20.4.2 No network address other than those provided by ITSC (TCP/IP) is allowed. IP addresses and other network resources allocated to users by ITSC may be subject to change without prior notice and users are not allowed to use any manually coded IP addresses in their computer.

20.4.3 Users must not configure their computer/network device as a network server of any kind. Users' computers shall not provide any server services without the prior permission of ITSC. For example, web sites for gaming, video/audio streaming, DHCP/BOOTP, FTP, SMTP, NAT, NTP, NFS and remote access service are not allowed. File and print sharing is limited to the Student Hostel network.

20.4.4 Network facilities are provided for academic use (instruction and research) and administrative use. The network facilities must not be used for commercial or personal gain, without explicit approval of ITSC.

20.4.5 Staff members and students may not install wireless access points or other network equipment/devices on the University network. If a wireless access point or network equipment/device is found on the network having been installed without prior approval from ITSC, the equipment will be disconnected and the responsible user account will be disabled.

20.4.6 Any computer/network device connected to the networks shall have security and authentication measures built into them to ensure that unauthorised persons will not be able to gain access to the networks. Service to devices which fail to meet this standard shall be discontinued.

20.4.7 If a staff member or student notices any abuse or misuse regarding University network access, they should immediately report it to the ITSC Helpdesk.

20.4.8 All users shall abide by this policy and all applicable Policies and Procedures, or risk the loss of access privileges and referral to the University authorities for potential disciplinary action.

20.5 Acceptable Use Policy

20.5.1 Since the Internet is mainly provided by JUCC HARNET, all users shall also abide by the 'HARNET Acceptable Use Policy' (see http://ln.edu.hk/itsc/policy/HARNET-acceptable-use-policy/).

20.6 University's Rights and Responsibilities

20.6.1 If there are any problems related to network security, performance and/or availability, ITSC reserves the right to suppress any kind of Internet application service (such as P2P (Bit Torrent), streaming (PP Live), Internet games) without prior notification.

20.6.2 Any users who violate the Rules and Regulations as stipulated in this Policy may lose their network access privileges. Known offenders who violate HKSAR laws or the University's regulations will be reported to the appropriate HKSAR and/or University authorities for further proceedings and/or disciplinary action.

20.7 Authorised Access and Usage of Network Resources

20.7.1 ITSC will restrict access to some low priority Internet applications not related to or rarely related to the purposes of teaching, learning and research, (such as P2P (Bit Torrent), streaming (PP Live), Internet games) to prevent available Internet bandwidth being taken up by these activities.

20.8 Violations of Policy

20.8.1 This policy is legally binding on all staff and students and on other individuals who use the University's network resources. If any staff member or student witnesses any violation of this policy, they should report it directly to ITSC at abuse@ln.edu.hk.

20.8.2 Individuals using the University network resources are prohibited from using the system to commit a criminal act. This includes, but is not limited to, unauthorised access to or attempt to gain access to other systems, the implementation of any virus or virus-type program, downloading and/or distribution of music, movies or any other electronic media for which the legal copyright is not owned, or any use of the system to plan, commit or exploit criminal activities.

20.8.3 Individuals in violation of this policy are subject to a range of sanctions including, but not limited to, the loss of computer or network access privileges, disciplinary action, dismissal and/or legal action. Some violations may constitute criminal offences, as outlined in HKSAR laws, and will be referred to the relevant authorities to be dealt with.

20.9 Exceptions

20.9.1 Exceptions are individually reviewed by the CIO and University Librarian and must follow the following process:

- If staff members want to design special academic network(s) or connect any network equipment/device to University networks in pursuit of their educational or research goals, they must request approval and collaborate with ITSC to ensure that the network is not adversely affected by the equipment or services of the academic network.
- In order to effectively evaluate the request and evaluate existing technology usage, requests for exceptions should detail the purpose of the request and how the current University network is insufficient to address the need.

20.10 Limitations of Liability

20.10.1 The University will make no effort to support individuals found guilty of policy breaches or criminal violations. Any individual accused of misconduct or criminal behavior via University network resources will receive no legal protection. If convicted of any violations, the University reserves the right to impose liability for the consequences of such acts and seek indemnification from the guilty party for damages the University may incur, as appropriate. Failure to comply with the terms of this document will result in denial of access to the University networks.

21. Email Communication Policy

21.1 Purposes and Limitations of the University Email System

Electronic mail services are provided by the University in support of the teaching, research and public service mission of the University.

21.1.1 Users

Users of University email services are limited primarily to University students and staff. Accounts for staff will be available on the starting date of their appointment. However, a staff member who has been confirmed with an appointment at the University, but has not yet reported for duty, may request an early activation of their email service. This request must be endorsed in writing by the Head of Department/Unit.

21.1.2 University Representation

Email users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the University or any unit of the University, unless appropriately authorised to do so.

21.1.3 Security

The University, in general, cannot and does not wish to be the arbiter of the contents of email. Neither can the University, in general, protect users from receiving email that they may find offensive. However, members of the University community are strongly encouraged to use the same personal and professional courtesy and consideration with email as they would with other forms of communication.

21.1.4 False Identity

There is no guarantee that email received is in fact sent by the purported sender, since it is relatively easy for senders to disguise their identity, although it is a violation of University Policy and the Laws of Hong Kong SAR to do so. Furthermore, email that is forwarded may also be modified. As with print documents, in cases of doubt, receivers of email messages should check with the purported sender to validate authorship or authenticity.

University email users shall not employ a false identity. However, email may be sent anonymously provided this does not violate any law or University policy, and does not interfere with normal University business.

21.1.5 Prohibited Use

University email services may not be used for unlawful activities or for commercial purposes that are not under the auspices of the University. Moreover, email services shall not be used for purposes that could reasonably be expected to cause, directly or indirectly, excessive strain on

any computing facilities, or unwarranted or unsolicited interference with other people's use of email or computer systems.

Users should not violate the use of email services by sending or forwarding:

- email chain letters;
- spam, that is exploiting mail list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited email;
- letter-bombs, that is, resending the same email repeatedly to one or more recipients causing interference with the recipient's use of email;
- phishing emails;
- malware or virus;

21.2 Managing your Email Account

21.2.1 Password Protection

Users are requested to change the initial password given to them as soon as possible and to keep passwords confidential at all times. Email accounts provided to individual users should not be shared or transferred. Users are responsible for the use of their email accounts at all times.

21.2.2 Email Quotas, Attachments and Exceeding Quotas

Please find the quota information at the following link:

Lingnan Home > ITSC > Services > Email Services > Checking Email Quota

(https://www.ln.edu.hk/itsc/services/email/email-services/checking-email-quota)

21.2.3 Back-up of Email Data

Users are encouraged to make a regular back-up of their email data onto local or off-line storage (such as writable CD, DVD or USB flash drive). The University does not maintain central or distributed email archives of emails sent or received.

21.3 Termination

21.3.1 Staff

Staff members are required to obtain clearance of their email accounts at the conclusion of their employment with the University. Immediately after their last date of employment with the University, all computer system access and email accounts assigned to the staff will be deactivated with the associated data irreversibly purged. Departing staff may request to set up an auto-reply message for a period of three months with their existing email accounts so that senders can be asked to re-send personal messages to another designated email address. The content of the original email will not be delivered with this auto-reply message.

Under special circumstances and with the written endorsement of the respective Head of Department/Unit or delegated staff member, the departing staff may request extension of their email accounts. This kind of extension will normally be no longer than one month after departure. All applications must be approved by the CIO and University Librarian who may refer the applications to the Human Resources Office or other relevant parties for checking as deemed necessary.

21.3.2 Student

The University email system is for the use of currently enrolled students only. Email accounts and all associated data will be irreversibly purged after 30 days of non-enrolled status. Students who re-enrol after an account has been purged will be provided with a re-activated account, but previously purged emails will not be able to be recovered.

21.3.3 Alumni

Final year students who are graduating will be given an alumni email account upon their confirmation of graduation. It should be noted that it is not possible to transfer the contents of the student current email account to the alumni account. The alumni account be available to University graduates on a continuing basis.

To prevent any unattended or unused account being targeted by hackers, alumni shall renew their email account every 2 years. ITSC will protect the accounts by disabling the account if no response is received in the renewal process. The account will be terminated if no reactivation request is received within 1 year after the account has been disabled.

21.3.4 Other Email Account Types

All other email account types such as department or contractors or third party email accounts that are not specified shall be renewed every 2 years. The account shall be locked if no response is received in the renewal process. The account will be terminated if no reactivation request is received within 1 year after the account has been disabled.

22. Confidential Non-Disclosure Agreement

22.1 An external party shall be aware of and review any corresponding information security policies related to their work with the University, especially in case of an external party who has to handle confidential information pertaining to the University.

22.2 An external party shall agree to and sign a non-disclosure agreement (such as Confidentiality and Non-Disclosure Agreement) before the commencement of their services. The agreement is to restrict the subsequent dissemination and use of the information.

Lingnan University

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

WHEREAS, Lingnan University (hereinafter "*LU*") agrees to furnish _____ (hereinafter "*Recipient*") with certain confidential information relating to any data or information, ideas, patents, inventions or other intellectual property (hereinafter "*Confidential Information*") for the purposes of determining an interest and/or solution to *LU*.

WHEREAS, *Recipient* agrees to review, examine, inspect or obtain such *Confidential Information* only for the purposes described above, and to otherwise hold such *Confidential Information* pursuant to the terms of this Agreement.

For the purposes of this Agreement, "**CONFIDENTIAL INFORMATION**" shall mean any information disclosed by LU, whether in writing, orally, visually or otherwise, including but not limited to business plans, financial data, academic and research information, course information and materials, statistics, operational information, equipment settings, products specification, technical data, know-how, ideas, concepts and vendor relationship of LU or third parties.

Confidential Information excludes, however, information which: (i) is or becomes known or available to Recipient without restriction from a source other than LU with a legal right to disclose the same to Recipient; (ii) is, or without violating the terms of this Agreement becomes, generally available to the public; or (iii) is developed by Recipient independently of the information disclosed hereunder.

BE IT KNOWN that *LU* has or shall furnish to *Recipient* certain *Confidential Information* on the following conditions:

1. *Recipient* agrees to hold *Confidential Information* in trust and confidence.
2. *Recipient* agrees that *Confidential Information* shall be used only for the contemplated purposes, shall not be used for any other purpose, or disclosed to any third party.
3. *Recipient* agrees to use its best efforts to protect the *Confidential Information* or any part thereof, and prevent disclosure of it to any person other than *Recipient's* staff having a need for disclosure in connection with *Recipient's* authorised use of the *Confidential Information*.
4. *Recipient* agrees to take all steps reasonably necessary to protect the secrecy of the *Confidential Information* and to prevent the *Confidential Information* from falling into the public domain or into the possession of unauthorised persons.
5. *Recipient* agrees no copies will be made or retained of any written information or prototypes supplied without the permission of *LU*.
6. *Recipient* agrees that all *Confidential Information* shall remain the property of *LU* and that *LU* may use such *Confidential Information* for any purpose without obligation to *Recipient*. Nothing contained herein shall be construed as granting or implying any transfer of rights to Recipient in the *Confidential Information*, or any patents or other intellectual property protecting or relating to the *Confidential Information*.
7. *Recipient* agrees the obligations of this Agreement shall be continuing until the *Confidential Information* disclosed to *Recipient* is no longer confidential.

At the conclusion of any discussions, or upon demand by *LU*, all *Confidential Information*, including prototypes, written notes, photographs, sketches, models, memoranda or notes were taken, shall be returned to *LU* and shall be destroyed in any storage media of *Recipient* in which it might subsist.

Recipient is permitted to disclose *Confidential Information* to staff members within the *Recipient's* company on a need-to-know basis provided that *Recipient* shall ensure they agree to be bound by the terms of this Agreement.

This Agreement and its validity, construction and effect shall be governed by the laws of HKSAR. IN WITNESS WHEREOF, the parties have executed this Agreement as of the date first written below.

Lingnan University:		Recipient:	
Signature:	_____	Signature:	_____
Name:	_____	Name :	_____
Title:	_____	Title :	_____
Date:	_____	Company :	_____
		Date :	_____

23. System Acquisition, Development and Maintenance Policy

23.1 This policy specifies the minimum security practices to be followed during information system acquisition, development and maintenance, in order to ensure sufficient security in all information systems, and prevent errors, loss, unauthorised modification or misuse of information in applications.

23.2 To ensure that security is built into information systems, the system owner and the Information Security Officer shall identify, justify, agree and document security requirements during the requirements phase of an information system's acquisition or development project.

23.3 Security controls shall be designed into applications systems, including but not limited to:

- 23.3.1 Validation of data input into applications systems to ensure that it is correct and appropriate.
- 23.3.2 Incorporation of validation checks into systems to detect corruption caused by processing errors or deliberate acts.
- 23.3.3 Encryption to safeguard the confidentiality, integrity and authenticity of classified information during transmission or in storage.
- 23.3.4 Message authentication techniques to protect message content from unauthorised changes or corruption.
- 23.3.5 Vulnerability assessment to identify potential risk of information leakage.
- 23.3.6 Validation of output information from applications systems, just before passing it to the target system, to ensure that it is correct and appropriate.

23.4 Access to application system files shall be controlled by the application owner who is responsible for ensuring that:

- 23.4.1 Strict controls are exercised over the implementation of software on operational systems.
- 23.4.2 All application system test data is protected and controlled.

23.5 Development and support environments shall be strictly controlled to maintain the security of application system software and data. These controls can take the following form:

- 23.5.1 Test data, software and hardware shall be distinguished from production data, software and hardware.
- 23.5.2 Modification of vendor-supplied standard software packages or any core system programming of enterprise resource planning systems shall be discouraged.
- 23.5.3 Strict control shall be maintained over access to program source codes, which are usually kept in program source libraries.
- 23.5.4 In dealing with changes resulting from the acquisition, development and maintenance of information systems, the change management policy shall be observed.

23.6 Control of Technical Vulnerabilities

23.6.1 A patch and vulnerability management program should be implemented.

23.6.2 Vulnerability remediation and configuration changes should be implemented to minimize the vulnerabilities.

23.6.3 To maintain the optimal security configurations and facilitate automatic deployment of patches, all computing devices (e.g. computers, network equipment, servers, etc.) acquired for use in the University should be configured by ITSC and loaded with standardized configuration before the device can be used in the University.

23.6.4 Computing devices not set up by ITSC and without loading of standardized configuration are not allowed to connect to the data ports of the campus network as the security of the machine cannot be determined.

24. Supplier Management Policy

24.1 This policy sets out to govern the selection and administration of vendors, consultants, contractors and other service providers external to the University, and to protect the University's information and processing facilities.

24.2 Before allowing an external party to access the University's information or information processing facilities, a security risk assessment shall be carried out to consider the type of access to be provided and any additional security controls that may be necessary.

24.3 The University shall monitor the service provided and review the service report produced by the external party to ensure that the information security terms and conditions of the agreements are being adhered to, and those information security incidents and problems are managed properly.

24.4 When there is a need to change the service specification and/or level, the security risk assessment should be re-performed and service contracts renegotiated.

25. Information Security Incident Management and Handling Policy

25.1 The University shall assign a responsible person (e.g. Information Security Officer) and establish a security incident response team and incident response procedures to manage overall information security incidents and to ensure a quick, effective and orderly response to information security incidents.

25.2 Information security events shall be reported through appropriate management channels as quickly as possible.

25.3 Users who are using the University's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

25.4 Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

25.5 Information security incidents shall be responded to in accordance with the documented response procedures.

25.6 Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

25.7 The University shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

26. Business Continuity Management Policy

26.1 This policy aims to ensure that the University has a documented and tested Business Continuity Plan (BCP) that describes how the University business will be conducted if critical systems are disrupted by a disaster affecting the University's operations.

26.2 The University shall establish and manage a process for developing, implementing and maintaining business continuity throughout its information processing facilities and critical business operations.

26.3 A BCP Coordinator shall assist in managing the BCP programme for the University in order to fulfil corporate and regulatory requirements.

26.4 The BCP Coordinator shall conduct a Business Impact Analysis (BIA) regularly to determine the criticality of the University's business processes, applications, systems and platforms, and the need for a BCP. The BIA results will be presented to the corresponding committee for review and approval.

26.5 The BIA results shall be reviewed annually to ensure the results are still appropriate.

26.6 The BCP Coordinator shall assist IT system managers to prepare formal BCPs for disaster protection, detailing how critical data and systems will be recovered if a disaster occurs. They will review, test and update these plans annually to ensure the currency of strategies, plans and solutions.

26.7 The BCP Coordinator shall work with the infrastructure and data centre operation in making appropriate provisions for the back-up and replacement of physical facilities, computer hardware/software or communications networks that support the processing of critical systems. This shall be done in a time frame consistent with the criticality of data and systems, and shall be consistent with the recovery time objectives specified by the University.

26.8 The ability to use override facilities shall be severely restricted, and these facilities will be used only to remedy extraordinary conditions that are not otherwise resolvable.

26.9 IT system managers shall clearly define the specific circumstances when security controls may be overridden or compromised to maintain the continuity of business operations. Advance approval from the BCP Coordinator shall be obtained.

26.10 Whenever system controls have been overridden, a log shall be generated showing the changes made and the privileged commands used. The Information Security Officer shall promptly review these logs and related particulars to ensure that the override facilities were used properly and correctly.

27. Compliance Policy

27.1 Users shall comply with laws, statutory, regulatory or contractual obligations and the Information Security Policies and standards.

27.2 Users who breach any laws, statutory, regulatory or contractual obligations and security requirements of information systems containing personal data (e.g. Personal Data Privacy Ordinance, Electronic Transactions Ordinance), shall be subject to disciplinary actions.

27.3 The management shall ensure that all security procedures within their area of responsibility are carried out correctly in accordance with the policies and standards as described in the University's Information Security Policies.

27.4 The internal audit mechanisms should be in place to monitor and measure compliance with the University's Information Security Policies.

28. Intellectual Property Policy

28.1 In general, intellectual property arising out of any work done as part of the duty of a member of staff resides with the University. Please refer to "Policy on Research, Knowledge Transfer and Intellectual Property" (https://www.ln.edu.hk/orkt/forms-and-policies/policies-and-useful-links) of Lingnan University for details.

28.2 The Intellectual Property Rights are protected under the laws of Hong Kong, all users shall comply with the law. For more details please refer to the website of the Intellectual Property Department of HKSAR (https://www.ipd.gov.hk/eng/home.htm).

- End -