Baseline Information Security Policy

P-1

VERSION 1.2

Contents

1 Document Control

1.1 Document Status

Document Name	Baseline Information Security Policy
Document Code	P-1
Author	IT Security Team
Version Number	1.2
Document Status	~~Draft for Internal Review~~ / ~~Release for Consultation~~ / Approved
Superseded Version	N/A

1.2 Document Status and Review

Version Number	Revision Date	Summary of Changes	Authored By
1.0	23-JAN-2015	Official release	IT Security Team
1.1	14-FEB-2017	PolyU logo updated	IT Security Team
1.2	20-MAY-2022	Sections "Outsourcing and Public Cloud Security" and "Internet of Things (IoT) Devices" are added	IT Security Team

2 Introduction

2.1 Purpose

The purpose of this Baseline Information Security Policy (Policy) is to ensure that the information managed by the Hong Kong Polytechnic University (the University) is appropriately secured in order to protect against the possible consequences of breaches of confidentiality, failures of integrity or interruptions to the availability of that information.

2.2 Usage

Departments and Offices shall establish appropriate security measures are implemented as detailed in this Policy.

2.3 Scope

This Baseline Information Security Policy constitutes the minimum information security requirements that shall be observed and followed by all those with access to the University Information Systems, including Staff members, students, visitors and Third Party Suppliers. These security requirements apply to any Information Systems attached to the University Campus Network and any Information Systems supplied by the University.

3 Definitions and Conventions

3.1 Definitions

The following are the definition of the terms used in this Policy.

Term	Definition
Business Owner	"**Business Owner**" is usually the User representative from the primary business functions of User departments leveraging the web application for supporting their business function.
Campus Network	"**Campus Network**" is set of interconnected local area networks serving the University.
Computer Equipment Room(s)	"**Computer Equipment Room**" is a dedicated room for housing computer and networking equipment.
Data Centre(s)	"**Data Centre**" is a centralized data processing facility that houses Information Systems and related equipment. A control section is usually provided that accepts work from and releases output to Users.
Departmental Computer Liaison Officer	"**Departmental Computer Liaison Officer"** is the single point of contact between departments and Information Technology Services Office on all IT-related issues including departmental IT requirements, IT security and software asset management.
Information System(s)	"**Information System**" is a related set of hardware and software organized for the collection, processing, storage, communication, or disposition of information. It usually comprises server, workstation, network equipment and application.
Personal Data	"**Personal Data**" is defined under the Personal Data (Privacy) Ordinance to mean any data: • Relating directly or indirectly to a living individual; • Form which it is practicable for the identity of the individual to be directly or indirectly ascertained; and • In a form in which access to or processing of the data is practicable.
Portable Computing Devices	"**Portable Computing Device**" is a mobile device capable of storing or processing digital information. Examples of Portable

	Computing Devices are portable USB, smart phones, tablets and laptops.
Sensitive Information	A data classification scheme is defined for classifying University data into four categories to ensure the data is protected with appropriate security controls: Level 0 – Data can be accessed by the Public Level 1 – Data is restricted to the University staff members and students Level 2 – Data is the information that, if made available to unauthorized parties, may adversely affect individuals or the business of the University Level 3 – Data is the information that is legally regulated or its data confidentiality is required by contractual obligation "**Sensitive Information**" is all the University's information that classified as level 2 or above.
Strong Authentication	Refers to the authentication method which is stronger than traditional User name and simple password. For instance, two-factor authentication based on something the User owns in addition to what the User knows is a form of Strong Authentication. Strong password such as enforcement of complex password and periodic password change is another way of implementing Strong Authentication.
Staff	"**Staff**" are people employed by the PolyU irrespective of the employment period and terms.
Third Party Suppliers	"**Third Party Suppliers**" are all external parties that provide service to the University in respect of Information Systems and business activities.
Un-trusted Network	"**Un-trusted Network**" is any network that is external to the Campus Network which is not under the University's management.
User(s)	"**Users**" are the personnel, including Staff members, students and Third Party Suppliers, who have access to the University's Information Systems or information.

3.2 Conventions

The following is a list of conventions used in this document:

- **Shall** - the use of the word ‘shall’ indicates a mandatory requirement.
- **Should** - the use of the word ‘should’ indicates a requirement for good practice, which should be implemented whenever possible.
- **May** - the use of the word ‘may’ indicates a desirable requirement.

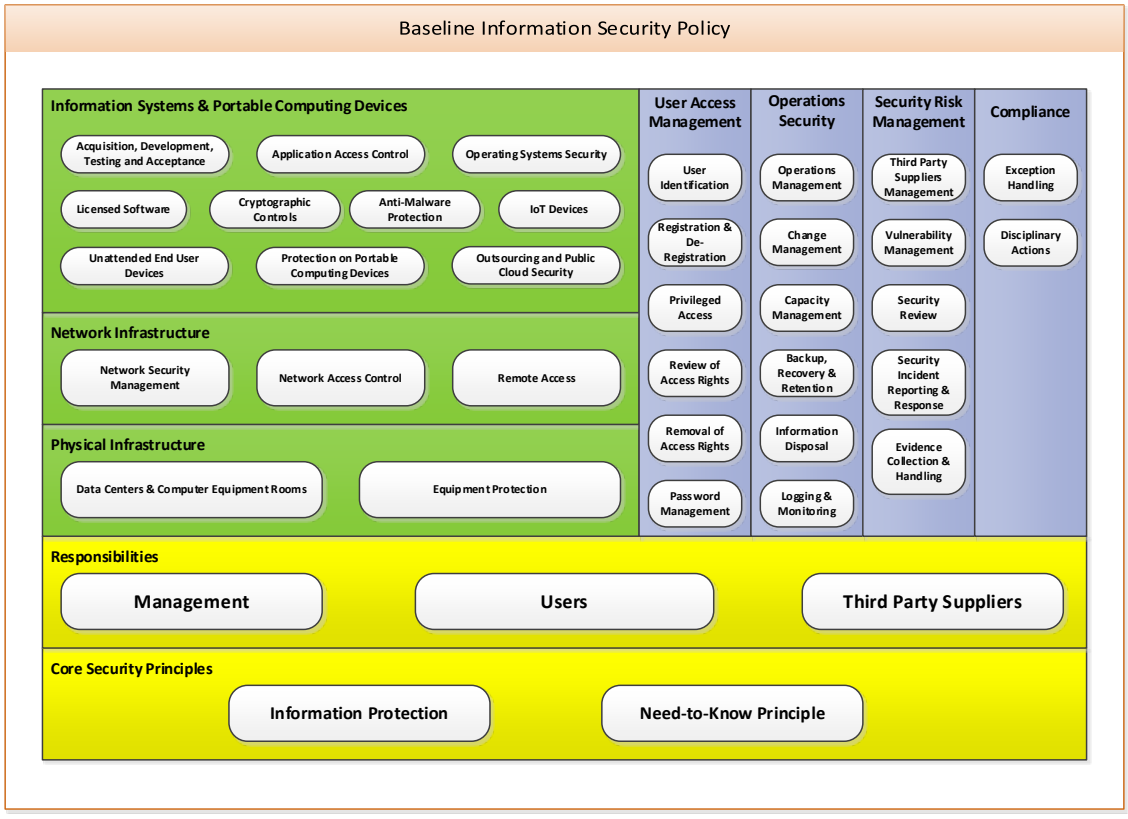
4 An Overview of Baseline Information Security Policy

This Policy is developed based on core security principles which are depicted in the Section 5 - "**Core Security Principles**" of the document. Information security is the responsibilities of every member in the University community including management, Staff members, students and Third Party Suppliers. The information security responsibilities of these parties are stipulated in Section 6 - "**Roles and Responsibilities**" of this Policy.

This Policy stipulates the minimum information security requirements that shall be observed and followed by all those with access to the University Information Systems, including Staff members, students, visitors and Third Party Suppliers. These security requirements apply to any Information Systems attached to the University Campus Network and any Information Systems supplied by the University. These requirements are depicts in the following sections:

- Section 7 – "User Access Management"
- Section 8 – "Physical Infrastructure"
- Section 9 – "Network Infrastructure"
- Section 10 – "Information Systems & Portable Computing Devices"
- Section 11 – "Operations Security"
- Section 12 – "Security Risk Management"

Section 13 – "Compliance" of this Policy depicts how exception and non-compliance of the Policy are handled. The following diagram shows the topics covered in various main sections of the Policy.



5 Core Security Principles

5.1 Information Protection

5.1.1 University's information shall be protected from unauthorized use, access, disclosure, modification, loss or deletion. Appropriate level of safeguards necessary to provide protection is relative to the value, legal requirements, sensitivity and criticality of the information.

5.1.2 Security shall be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

5.1.3 Information security is the responsibility of every member of the Staff and students in the University community.

5.1.4 Information security risks shall be identified and appropriate corresponding controls shall be incorporated throughout the Information System lifecycle (i.e. acquisition, development, testing, and maintenance / support).

5.2 Need-to-Know

5.2.1 The dissemination of information shall be no wider than is required for the efficient conduct of business in hand and restricted to those who are authorized to have access.

6 Roles & Responsibilities

6.1 Management

6.1.1 Management shall provide support for the development, implementation and ongoing maintenance of information security processes and infrastructure within the University.

6.1.2 A Departmental IT Security Officer shall be appointed by individual departments to coordinate all IT security related matters. This role may be assumed in alignment with other duties such as the Departmental Computer Liaison Officer role.

6.2 Users

6.2.1 Users with access to University information are responsible for protecting the information from unauthorized access, modification, duplication, destruction, or disclosure whether accidental or intentional.

6.2.2 Users are accountable and liable for all activities performed on Information Systems with their User accounts and should exercise all due diligence with respect to keeping their identity and password information safe and secure.

6.3 Third Party Suppliers

6.3.1 Third Party Suppliers who are engaged in the University's projects and operations shall be subject to equivalent information security requirements and have the same information security responsibilities as University's Users.

6.3.2 Third Party Suppliers shall treat as confidential all information supplied by the University in the course of business with the University which is designated as confidential by the University or which is by its nature clearly confidential. Third Party Suppliers shall not divulge any University information to any person except to their own employees on a need-to-know basis.

6.3.3 Third Party Suppliers must attest to these responsibilities as part of the contract of supply process.

7 User Access Management

7.1 User Identification

7.1.1 User accounts should be uniquely assigned to individual User for access to the University Information Systems.

7.1.2 Shared or group accounts shall only be created with business justification. Shared or group account shall have a documented owner who is responsible for all activities performed using the User account.

7.2 User Registration & De-registration

7.2.1 Formal registration and de-registration processes shall be implemented for granting and revoking access to all Information Systems.

7.3 Privileged Access

7.3.1 The allocation and use of privileged access rights should be restricted and controlled.

7.3.2 Privileged access rights should be assigned to a User account different from those used for regular business activities. Regular business activities should not be performed by privileged User accounts.

7.4 Review of User Access Rights

7.4.1 User access rights should be reviewed regularly and after changes of User's role in the University.

7.5 Removal or Adjustment of Access Rights

7.5.1 Access to the University's information and Information Systems shall be modified or removed as soon as possible after changes of User's role in the University.

7.6 Password Management

7.6.1 Users are responsible for their own password security. Passwords shall be kept in strict confidence and never appear on screen or in printed form.

7.6.2 Users shall not capture or otherwise obtain others' passwords and decryption keys.

7.6.3 Passwords shall never be stored in clear text on Information Systems. Compensating controls shall be applied to reduce the risk exposure of Information Systems to an acceptable level if encryption is not implementable.

7.6.4 Passwords should be encrypted when transmitting over an Un-trusted Network. Compensating controls shall be applied to reduce the risk exposure of Information Systems to an acceptable level if encryption is not implementable.

7.6.5 All vendor-supplied default passwords shall be changed before any Information Systems is put into operation.

7.6.6 Passwords shall be promptly changed if they are suspected of / are being compromised.

7.6.7 Passwords should be changed regularly.

8 Physical Infrastructure

8.1 Data Centres & Computer Equipment Rooms

8.1.1 Data Centres and Computer Equipment Rooms shall be housed in secure areas commensurate with identified risks and protected by a defined security perimeter.

8.1.2 Data Centres and Computer Equipment Rooms shall be protected by entry controls to ensure that only authorized personnel are allowed access.

8.1.3 All Data Centres and Computer Equipment Rooms should be monitored at all times by authorized personnel.

8.1.4 Guidelines for working in Data Centres and Computer Equipment Rooms shall be established. Personnel authorisation processes should be explicitly documented and individual authorisation renewed periodically. All personnel working in these secure areas, including Third Party Suppliers, shall adhere to the Code of Practices.

8.1.5 Physical security for Data Centres and Computer Equipment Rooms shall be designed and applied taking into account of relevant health and safety regulations and standards.

8.2 Equipment Protection

8.2.1 Equipment that stores or processes the University information shall be protected from physical and environmental security threats in order to prevent unauthorized access to information and/ or loss or damage.

8.2.2 Equipment containing University Sensitive Information and licensed software shall be securely destroyed, deleted, or overwritten prior to disposal or reuse.

8.2.3 Preventive maintenance of equipment and communication facilities shall be performed to ensure continued availability and integrity.

8.2.4 All University owned equipment and non-public information in the possession of Staff or Third Party Suppliers shall be returned to the University upon termination of employment and must be returned upon termination of contract unless the contract provides otherwise.

9 Network Infrastructure

9.1 Network Security Management

9.1.1 Network security controls and practices to provide adequate protection against intrusion into the University Information Systems shall be implemented, maintained, documented, and followed.

9.1.2 Network management and security monitoring activities shall be conducted on a regular basis. Information including network traffic and protocols shall be logged for monitoring and detecting irregularities.

9.1.3 Internal network information such as network diagram and network addresses shall be properly maintained and not released to external parties without the approval of Director of Information Technology or delegates.

9.2 Network Access Control

9.2.1 Network segmentation shall be implemented to protect Information Systems storing different types of Sensitive Information.

9.2.2 Assessment shall be performed to determine how access shall be granted across different network segments.

9.2.3 Connection of any equipment to the Campus Network that can affect the network's normal operation shall be prohibited.

9.2.4 Information Systems connected to the Campus Network shall be equipped with adequate security mechanisms protecting against cyber-attack.

9.2.5 Any external network shall not be connected to the Campus Network without the approval of Director of Information Technology.

9.3 Remote Access

9.3.1 Proper and necessary protection mechanisms including firewall and authentication processes shall be implemented for remote connections to safeguard the Campus Network from external attacks.

9.3.2 Remote access to the Campus Network shall require Strong Authentication.

9.3.3 Remote access shall be restricted to allow access only to specifically approved Information Systems or functions.

10 Information Systems & Portable Computing Devices

10.1 Acquisition, Development, Testing and Acceptance

10.1.1 Every Information System shall have a Business Owner.

10.1.2 New Information System or enhancements to existing Information System shall include security requirements. These requirements shall be identified prior to the development or acquisition of Information System and agreed and approved by the Business Owner of the system.

10.1.3 Information Systems shall be developed using secure coding practices to prevent common coding vulnerabilities and to minimize security errors.

10.1.4 Test data shall be carefully selected, protected and controlled commensurate with its sensitivity. The use of test data extracted from production systems or operational data containing Sensitive Information should be avoided. If genuinely required, the process should be reviewed, documented and approved by the Business Owners of concerned Information Systems and where possible any data should be 'masked' so as to remove personal information.

10.1.5 Development, test and production operational facilities shall be subject to physical or logical separation to achieve segregation of the processing environments. Transfer of Information Systems from development to operational status shall be based upon documented rules and in accordance with established change management procedures.

10.1.6 Strict control shall be maintained over access to program source code and libraries to reduce the potential corruption of Information Systems.

10.2 Application Access Control

10.2.1 Security capabilities within applications shall be enabled to restrict access to University information to authorized Users only.

10.2.2 Wherever feasible, additional authentication controls such as the use of two-factor authentication techniques should be employed on Information Systems for protecting University Sensitive Information.

10.3 Operating Systems Security

10.3.1 Information Systems shall be managed in accordance with the principle of least functionality with all unnecessary services or components removed or restricted.

10.3.2 Information Systems shall be reviewed and tested to ensure that there is no adverse impact on operation or security as a result of any changes or upgrades to the underlying operating system.

10.4 Cryptographic Controls

10.4.1 Wherever feasible, Sensitive Information stored or transmitted by Information Systems shall be protected by cryptographic controls.

10.4.2 Cryptographic controls employed by Information Systems shall use internationally recognized strong algorithms.

10.5 Anti-Malware Protection

10.5.1 Anti-malware protection shall be enabled on Information Systems to protect against malware attack.

10.5.2 Virus signatures, malicious code definitions as well as their detection and repair engines shall be updated regularly and whenever necessary.

10.5.3 Users shall not intentionally write, generate, copy, propagate, execute or involve in introducing computer viruses or malicious codes.

10.6 Licensed Software

10.6.1 Only licensed software shall be used on University's Information Systems.

10.7 Unattended Information Systems

10.7.1 Users shall ensure that unattended Information Systems have appropriate protection. If there has been no activity for a predefined period of time, to prevent unauthorized system access attempt, re-authentication should be activated or the logon session and connection should be terminated.

10.7.2 User workstations should be switched off, if appropriate, before leaving work for the day or before a prolonged period of inactivity.

10.8 Protection on Portable Computing Devices

10.8.1 Wherever feasible, Portable Computing Devices shall be password protected. Cryptographic controls with internationally recognized strong algorithms should be employed to protect the University's information stored on the devices.

10.8.2 Users shall not leave Portable Computing Devices storing University's information unattended in public locations.

10.8.3 All Portable Computing Devices storing University's information shall be kept in a secured location when not in use.

10.8.4 Users should not store Sensitive Information on Portable Computing Devices.

10.9 Outsourcing and Public Cloud Security

10.9.1 When considering public cloud services, users shall assess the overall security risk of the potential cloud providers following the relevant security requirements stipulated in the Security Questionnaire for Public Cloud Services.

10.10 Internet of Things (IoT) Devices

10.10.1 The IoT deployment shall not pose any threats to the existing IT environment of the University.

10.10.2 Wherever feasible, proper security measures stipulated in the Deployment Guideline for IoT in the University shall be implemented in the IoT deployment.

11 Operations Security

11.1 Operations Management

11.1.1 Operational and administrative procedures for Information Systems shall be properly documented, followed, and reviewed periodically.

11.1.2 Wherever feasible, sufficient segregation of duties shall be applied to avoid execution of all security functions of Information Systems by a single individual.

11.2 Change Management

11.2.1 Effective mechanisms shall be adopted to ensure that changes to Information Systems are authorized, controlled and recorded.

11.2.2 Changes affecting existing security protection mechanisms shall be carefully considered.

11.3 Capacity Management

11.3.1 Usage of an Information System and its resources shall be monitored and managed in accordance with capacity requirements to ensure the required availability and efficiency of systems.

11.4 Information System Backup, Recovery and Retention

11.4.1 Essential information shall be backed up routinely and restore tests should be carried out regularly.

11.4.2 The retention period for essential information shall be determined for every Information System, taking into account any requirement for archive copies to be permanently retained.

11.4.3 Personal Data associate with an individual shall only be collected and retained for pre-declared legitimate business purpose and in accordance with the Personal Data (Privacy) Ordinance.

11.4.4 Personal Data shall not be transferred out of the University unless there is a written consent from the Business Owner. Security controls shall be implemented to protect such type of Personal Data.

11.5 Information Disposal

11.5.1 Information shall be securely destroyed when it is no longer needed or its retention period has expired.

11.6 Logging & Monitoring

11.6.1 Event logging mechanisms shall be established and activated on Information Systems to provide evidence in case of security incidents.

11.6.2 Log information shall be protected from unauthorized modification and retained for at least SIX months but no longer than the retention life of the information stored on the system.

11.6.3 A centralized time synchronization system shall be utilized to synchronize all Information Systems.

12 Security Risk Management

12.1 Third Party Suppliers Management

12.1.1 Users shall impose service agreement terms requiring Third Party Suppliers to compile with legislative, regulatory and the University's data protection requirements, and monitor their compliance.

12.1.2 Access to University's information and Information Systems by Third Party Suppliers shall be controlled and such controls shall be agreed to and defined by way of contractual obligation with the Third Party Suppliers.

12.1.3 Third Party Suppliers accessing University Sensitive Information shall be required to sign a confidentiality agreement to protect the University's information.

12.2 Vulnerability Management

12.2.1 Information Systems should be protected from known security vulnerabilities by applying the latest security patches provided by vendors or implementing other compensating security measures.

12.3 Security Review

12.3.1 Security risk assessment shall be performed in the early stages of an Information System project for identifying appropriate and cost-effective security measures required for Information Systems.

12.3.2 Privacy impact assessment shall be performed for an Information System involving collecting, handling and storing of Personal Data in accordance with the Personal Data (Privacy) Ordinance.

12.3.3 Security vulnerability assessment shall be performed before production launch of an Information System.

12.3.4 Any security flaws identified during security vulnerability assessment shall be remediated before the production launch.

12.3.5 Information Systems should regularly review for compliance with the University's information security policies and standards.

12.4 Security Incident Reporting & Response

12.4.1 All Users shall report any security breaches to ITS Helpdesk as quickly as possible to limit the impact of the security incidents to the University.

12.4.2 Information Technology Services Office may take necessary actions during a security incident in order to protect the Campus Network as a whole, including temporary disconnection of the implicated devices or systems from the Campus Network or User account suspension in the event of a security incident.

12.4.3 During a security breach investigation, the Director of Information Technology may appoint an investigator to examine information stored in or transmitted by implicated University Information Systems in accordance with the Personal Data (Privacy) Ordinance.

12.5 Evidence Collection & Handling

12.5.1 The use of digital forensic and anti-forensic tools shall be limited to trained personnel who are authorized by the Director of Information Technology.

12.5.2 The methods used to collect and acquire potential digital evidence shall be clearly documented in detail and, as far as practically possible, be reproducible or verifiable by personnel with the knowledge in handling digital evidence.

12.5.3 Digital evidence shall be preserved to ensure its usefulness in any investigation. The preservation process shall involve safeguarding potential digital evidence and digital devices that may contain potential digital evidence from tampering or contamination.

12.5.4 The chain of custody shall be maintained throughout the lifetime of the evidence and preserved for TWELVE months after the end of the investigation.

12.5.5 Only personnel authorized by the Director of Information Technology, through the IT Security Manager, shall access digital evidence.

13 Compliance

13.1 Exception Handling

13.1.1 All Users shall observe and comply with the Baseline Information Security Policy. Requests for exceptions to this Policy shall be submitted in writing to the Office of Director of Information Technology with appropriate business justification and the compensating controls for minimizing the risk associated with the exception request.

13.1.2 All exceptions to this Policy shall be reviewed on annual basis.

13.2 Disciplinary Actions for Security Breach

13.2.1 Any inappropriate use of IT services or facilities and breach of the baseline information security policy shall be reported to the Director of Information Technology and the Head of the Department concerned and/or the University's disciplinary authority for appropriate actions. Interim suspension of access to University's IT facilities and services may be a necessary consequence of a security breach.

~~~~~~End of Document~~~~~
~~~~~~