Personal Data Protection and Security Measures

Data and Security Team
April 2018

The University of Hong Kong
Information Technology Services
Agenda

➢ Data Protection Principles
➢ Data Management Roles
➢ Data Classification
➢ Good Practices for IT Security
Data Protection Principles
University’s Data

➢ Data is one of the most valuable assets of the University

➢ Data can be any information (including fact, opinion, statistics, record and research information) that is stored in computer, USB drive, Cloud storage and on paper.
Risk to Data Protection

| Data Quality | Data are of high quality if they are fit for their intended uses in operations, decision making and planning. |

Which is against ...

- misuse
- destruction
- alteration
- theft
- misinterpretation
- inappropriate access restriction
Data Protection Principles

Confidentiality

Refers to ensuring only authorised persons can access the data

Data/information confidentiality

Integrity

Refers to maintaining the accuracy and consistency of data/information over its entire life cycle, and is the opposite of data corruption

Data/information integrity

Availability

Refers to ensuring data and the functions of associated information systems are available and protected from service disruption

Data/information availability
Data Management

Roles

See the Information Security and Data Management ("ISDM") Policy
3-Level Defence Governance Structure

3rd level
- Internal Audit Officer (IAO)
- Independent Assessor

2nd level
- Data and Security team
- University Data Protection Officer (for personal data issues)

1st level
- Data Owner
- Data Steward
- Data Custodian
- Data User

Compliance

Assess, Support and Ongoing Compliance Monitoring

Day-to-day data operation and security protection
**Data Management Roles**

Proper delegation of accountabilities and responsibilities is required, and the followings are collectively known as **1st line of defence**.

- **Data Owner**
- **Data Steward**
- **Data Custodian**
- **Data User**
Data Management Roles

Data Owner

Definition

• The **head** of an administration office / faculty / department / school / centre or the **Principal / Chief Investigator** (PI or CI) of a research programme or project (“unit”)

• The **decision maker** with respect to data collected and/or used

• Example: Dean of Faculty

Key Responsibilities

• Interpret and implement **information security and data management policies, standards and guidelines**

• **Delegate this responsibility** (but not **accountability**) to a Data Steward where appropriate
Data Management Roles

Data Steward

Definition

• Any appropriate individual assigned by a Data Owner

• Example: Faculty Secretary

Key Responsibilities

• **Facilitate the interpretation and implementation** of information security and data management policies, standards and guidelines to meet the needs of the University for the use of data

• **Work with Data Owners** to assure that data is appropriately classified, managed and protected

• **Identify and implement procedures and controls** for data protection

• Work with the University’s data protection / information security personnel to enforce the procedure and controls

• Play the role of or cooperate with the **University’s Personal Data Protection Coordinators**
Data Management Roles

Data Custodian

Definition
• Organisational functions or individuals that are entrusted to operate on university data/information on a need basis as part of their assigned functions or employment or contractual duties
• Example: IT function of the Faculty

Key Responsibilities
• Be familiar with the University’s governance and classification structures in relation to data/information management and information security
• Comply with all related policies, standards, guidelines and procedures issued by the University associated with data/information management and information security and equip themselves with necessary knowledge and skills to enable such compliance

Data User

Definition
• Organisational functions or individuals that are entrusted to access and use university data on a need basis as part of their assigned employment or contractual duties or functions
• Example: Officers of the Faculty
Data Classification
**Data Classification Scheme**

01 **Restricted**
- Very sensitive in nature and strictly restricted by the University, the government or any agreements
- Example: Sensitive information concerning a pending criminal investigation

02 **Confidential**
- Intended for use by specific group of authorised personnel within the University and business partners
- Example: Student and staff information (e.g., Contact phone)

03 **Internal**
- Non-sensitive operational data that is intended for use within by members of the University and authorised services providers
- Example: Internal policies

04 **Public**
- Approved by the appropriate University authority for public consumption
- Example: Press releases
Good practices for IT Security
Workstation (PC)

➢ Use strong password, at least 10 characters with combinations of alphabet and numeric
➢ Enable PC login password and screen saver password
➢ Screen lock or logout your PC when unattended
➢ Do not install Peer-to-Peer (P2P) software on PC that handles confidential data
➢ Physically secure the notebook PC, tablet PC
➢ Avoid using public computer to access confidential files
➢ Using VPN or other secure channel for remotely access from the outside of the university
Storage

Data could be stored on personal PC, file server, mobile phone, Network Attached Storage (NAS), Cloud storage, files and folders... etc.

- Apply access control
  - Require user ID and password
  - Read, write, deny access
  - Logging

- Use encryption

- Backup regularly
Physical Security

• DON’T leave your PC unattended without physical protection.

• Protection measures:
  – Lock your office door.
  – Use cable chain lock.
  – Enable screensaver.
Removable Storage

➢ Use encryption and password protected
➢ Erase the data after use (best reformat the USB drive)
➢ Don’t leave USB drive unattended
➢ Keep it safe
➢ Don’t use USB drive from unknown source
➢ Only store sensitive data on portable devices or media when absolutely necessary
➢ For storing personal data, adhere to the absolute necessary principle, seek permission and take protection measures (encryption) - see the Code of Practice
➢ Report to supervisor if lost USB drive that contains sensitive data

Guidelines on Electronic Communications and Storing Personal Data on Portable Storage Devices, Personally-owned Computers and Public Cloud Services
(http://www.its.hku.hk/about/policies/personal-data-guidelines)
Removable Storage

➢ Data Leakage Prevention ("DLP") Protection (See Code of Practice)
➢ USB PSDs are required to be initialized before any write access of the device and only read access is allowed.

- Logon HKU Portal
- Search for “DLP”
- Click on the link “DLP for PSD”
Email & File Protection

Information Rights Management (IRM) Solution

• allows individuals to set access permissions to files and email messages.

• only authorized person is granted access (permission) to an IRM-controlled document.

• Prevent content from unauthorized forwarding (applicable to mail message), editing, printing, faxing, saving, or copying (cutting and pasting) the content

• Support major platforms: Windows(Full features), MacOS, Android, iOS


• Training: http://www.isdm.hku.hk/communication
Cloud storage

Before uploading data to Cloud storage, you should consider:

➢ Privacy and confidentiality
➢ Data Encryption
  ▪ uploaded to, downloaded from, and stored in the cloud
➢ Exposure of data
  ▪ to cloud operator, local and foreign government or agency
➢ References
  ▪ Guidelines for Using External Web 2.0 Services
    (http://moodle-support.hku.hk/teacher/web20guide)
  ▪ PCPD Information Leaflet – Cloud Computing
    (https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf)
Social Networks

Online Social networking sites are useful to stay connected with others, but you should be wary about how much personal information you post.

• “Stay Smart. Mind Your Digital Footprint” – by PCPD
• Privacy and security settings
• Once posted, always posted
• Keep personal information personal
Mobile Security

“New Technology, old Privacy and Security issue”

➢ **Lost or stolen mobile devices**
  - Enable screen lock
  - Encrypt the data, such as email and documents
  - Use Remote Wipe and Anti-Virus
  - Beware of automatically login of company email & file server

➢ **Malware and virus**
  - Steal bank details, company data, personal identities & email addresses

➢ **Beware of apps sources and access rights**
  - Install from trusted sources only
  - Beware of app requests of excessive permissions of devices
Phishing is the act of attempting to acquire information such as usernames and password by pretending from a trusted entity, e.g. ITS or other department of the University

➢ Signs of a phishing email:
  • Unofficial “From” address
  • Urgent actions required
  • Generic greeting
  • Link to a fake website, sometimes with legitimate links

➢ What to do if you received phishing email
  • Delete these suspicious emails
  • Don’t reply or click any link on them
Phishing email

Sample of phishing email

Non-HKU Hyperlink
Http://evil.com/cheat_u/login.htm
Ransomware

Ransomware is malicious software which encrypts files and waits for a paid ransom, and in some cases, normal use of the infected computers cannot be resumed even a ransom is paid.
Ransomware typically propagates in the form of a Trojan horse which enters a computer through

- a downloaded file
- emails with malicious attachments
- malicious website
- network vulnerability

Your PC is locked and files are encrypted:
To get the key to unlock your PC and decrypt files, you have to pay HK$10,000.
Security Measures for Protecting PC

1. Regularly backup your PC data and keep a recent backup copy off-line.
2. Ensure anti-virus software is installed on your PCs and keep it up-to-date with the latest virus signature.
3. Keep the operating systems of your PCs up-to-date.
4. For suspicious emails, attachments/files and unsolicited web sites, please do not open them.
5. Do not enable macros in document attachments received via email.
6. Limit the privilege & access right of shared network drives.

Refer to HKU ITS web site
http://www.its.hku.hk/faq/infosec/awareness/ransomware
Thank You