Agenda

➢ Why Data Protection?
➢ HKU Policies and Guidelines
➢ ISDM Policy
➢ Data Classification
➢ Good Practices for IT Security
Why data protection?

- DPP4
- Academic freedom
  => Very open firewalls
- Security is only as good as your weakest leak
HKU ITS Policies & Guidelines

• [http://www.its.hku.hk/about/policies](http://www.its.hku.hk/about/policies)

• Good advice on Information Security (IS)

• Regulations on what should not be done
  – Campus Network & HARNET acceptable use policy
  – e.g. NOT add network device to Campus Network

• Privacy Policies
  – Personal Data Guidelines
  – Using External Web 2.0 Services for University Purposes

• Password Policy
ISDM Policy in a nutshell

➢ Information Security and Data Management Policy
➢ Launched in May 2017
➢ Define roles and responsibilities in a decentralized environment (three lines of defence, more in the next slide)
➢ The Council is the sponsor of the Policy
➢ See more https://isdm.hku.hk
# ISDM governance structure

<table>
<thead>
<tr>
<th>University-Wide Data/Information Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Technology Policy Committee</strong></td>
</tr>
<tr>
<td>Strategic oversight: information security, data management &amp; information tech.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sub-committee on Information Security and Data Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversight of operations in relation to information security and data management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Governance</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd Line</td>
</tr>
<tr>
<td>Internal Audit</td>
</tr>
</tbody>
</table>

| 2nd Line |
| University Data Protection Officer (Personal Data Privacy Advisory) |
| Data & Security Team of ITS (Data* & Information Security Compliance) |
| Task Force on Mgmt. of Research Data & Records (Research Data Mgmt. Advisory) |

| Assess, support and ongoing compliance monitoring |

| 1st Line |
| Central Administrative Offices, Faculties, Departments/Schools/Centres, Research Teams |
| Data Owners and Data Stewards Processes, Procedures and Systems |

| Data Custodians, Data Users |
| Day-to-day handling of data and security |

* Including Personal Data Privacy
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.

Strict requirements are imposed.
Workstation (PC)

➢ Use strong password, at least 10 characters with combination 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 your notebook PC, tablet PC
➢ Avoid using public computer to access confidential files
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 - AIP

• 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
    (https://intraweb.hku.hk/local/its/web2guidelines/)
  ▪ 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 receive phishing email
  • Delete these suspicious emails
  • Don’t reply or click any link on them
  • Report to ithelp@hku.hk
Phishing email

Sample of phishing email

Dear User,

We noticed a violation of our services on your E-mail account and for this reason, your E-mail account will be closed if you fail to resolve the issue within the next 48 hours.

This will only take a moment. Click the "RESOLVE" link below and enter the requested details to complete the process.

RESOLVE

© 2012 The University of Hong Kong.

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

• I’m aware that <substitute password formerly used by recipient here> is your password
• ... placed a malware on the porn website ... While you were watching the video, your web browser acted as a RDP (Remote Desktop) and a keylogger which provided me access to your display screen and webcam... gathered all your contacts from your Messenger, Facebook account, and email account.
• $<money> is a fair price for our little secret.
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.
Protecting PC from ransomware

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