Joint Universities Computer Centre Limited
(“JUCC”)
Information Security Awareness Training- Session Three

Data Handling in University

Information Classification and Handling

Agenda

- Background
- People-Process-Technology (PPT)
- Information Classification
- Data Handling
- Fundamental Security

What is Data?

- Data is one of the universities most valuable assets.
- Because staff need to handle sensitive and confidential information, it is necessary to educate employees how to properly secure data.
- Universities have an increasing dependency on information in the form of computer data for its day to day operations.
- The risk of data being misused or accidentally/ deliberately modified or damaged increases.

Background Information

Who is Affected?

- Anyone who creates or handles sensitive or critical data.
    - Sensitive and critical data exists throughout the University

What to Know?

- How to recognise critical data
- What precautions are needed to take when “handling” them.

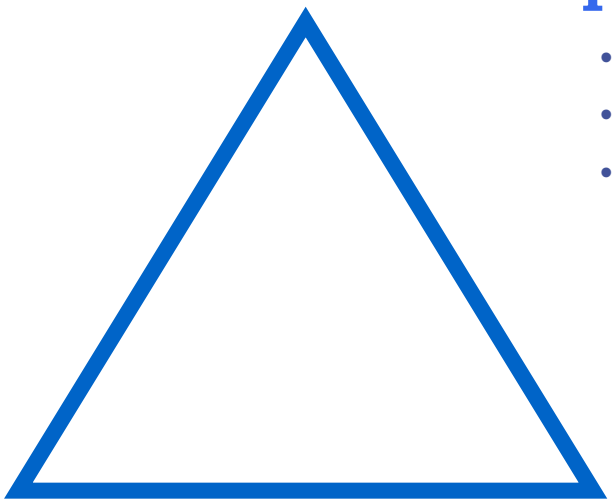
Challenges - Implementing data classification in Universities

- Certain types of data must be specially handled so that the University can maintain its operations whilst fulfilling its legal or moral obligations.
- This requires control mechanisms that are safe and easy to use. Controls are required to protect the:
  - **Confidentiality** of data, where sensitivity warrants this;
  - **Integrity** of data, to ensure its completeness and accuracy; and,
  - **Availability** of data, so that it is accessible as and when required.

HOWEVER…

Challenges – Implementing data classification in Universities

- *However*, management/ information security team may not have knowledge of:
  - What data exist in campus;
  - Where they are;
  - Who owns the them;
  - What level of protection is required; and
  - How to protect them



People

- Data Owners
- Data Custodians
- Data Users

Process

- Information Classification Policies
- Data Handling Guidelines
- Third-party Data Handling Requirements

Technology

- Data Classification System
- Data Loss Prevention Solutions
- Document Management System

Responsibilities in Information Classification

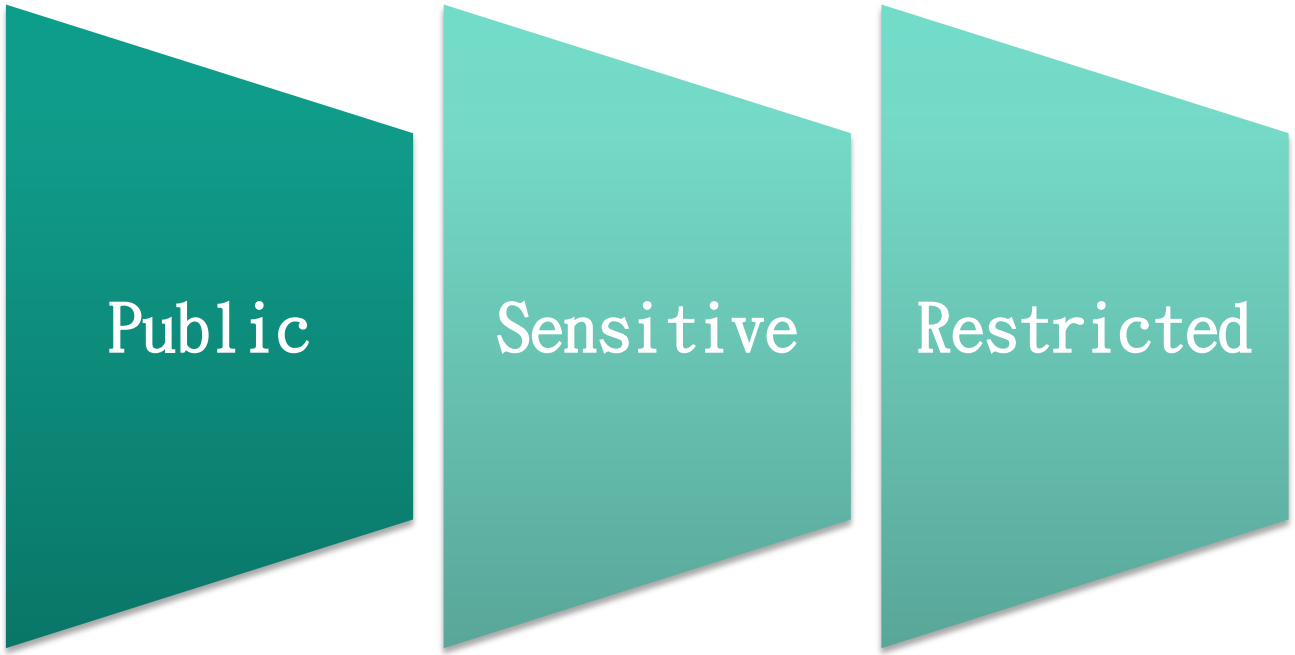
- **Management** – provides framework and defines classifications
- **IT** – provides appropriate infrastructure and training
- **Data owner** – identify & classify data and apply controls

** Data owners are people with the best knowledge of how to identify and classify the data they own **

Three-level Classifications:

For the purpose of handling data appropriately, data is classified by data owners into categories- classification level.

One set sample classification levels common used is:

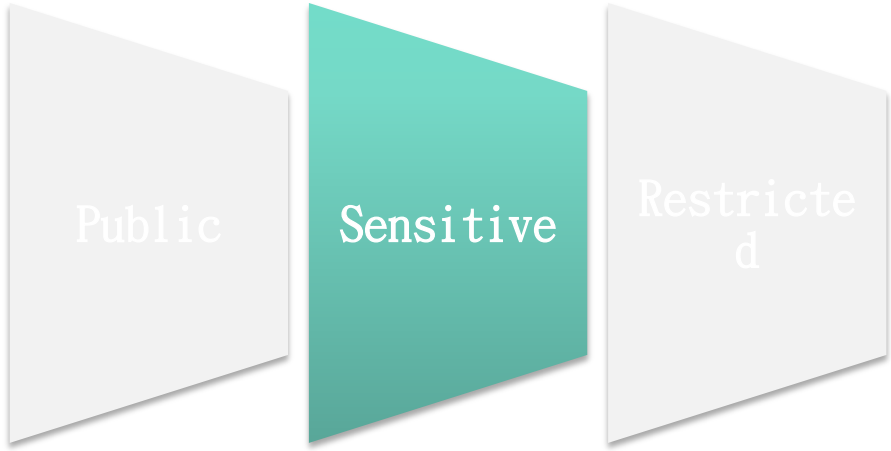


Public

- Information which may or must be open to the general public.
- It is defined as information with no existing local, national or international legal restrictions on access.
- Example: reports containing generalised information (e.g. summary reports, enrollment reports, degrees conferred reports, etc), or any report that contains only directory information.

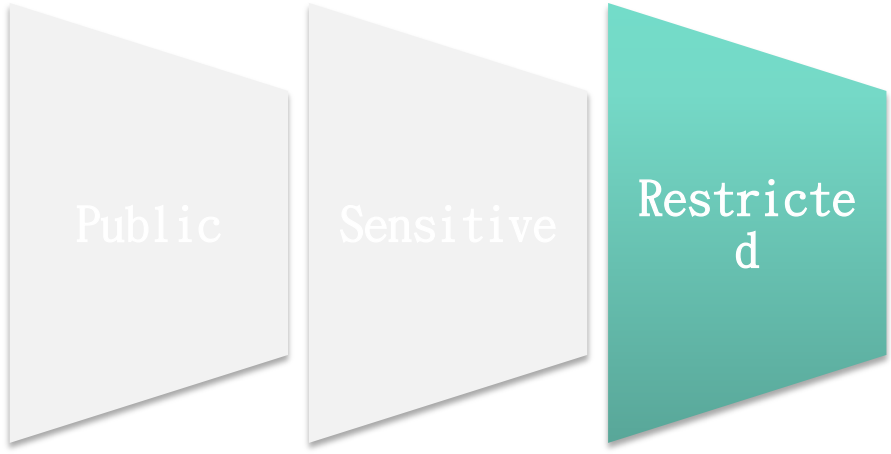
Sensitive

- Information whose access must be guarded due to proprietary, ethical, or privacy considerations.
- This classification applies even though there may not be a civil statute requiring this protection.
- Example: Student ID; Electronic signature.



Restricted

- Information protected because of protective statutes, policies or regulations.
- Data which data owner exercised their right to restrict access.
- Example: Business confidential, secret design/ formula



Data Handling

- "Handling" information relates to when you
  - View
  - Update
  - Delete
  - Transfer (digital and paper)
  - Mail
  - Store
  - Destroy

} DATA

- Therefore, it is important you understand how to handle these situations based on the data's classification. Depending on how the data is classified, different level of precautions for handling may be required.

Examples

- Creation and Access
- Disclosure
- Storage
- Copying and Transmitting
- Printing
- Backup

Use of Privately Owned Equipment

- Privately owned equipment is not to be used to create or access Restricted Data unless a secure form of remote access is used for this purpose (e.g. Secured VPN)
- Anyone accessing Restricted Data via the secure means of remote access is responsible for ensuring that:
  - The computer that they are using is not a public computer;
  - the input of their user ID and password is not observed when logging on to initiate a remote session;
  - sensitive information cannot be viewed by others;
  - restricted data are not downloaded;
  - restricted data are not printed out;
  - open sessions are not left unattended;
  - sessions are properly terminated.

Use of University Owned Equipment

- Sensitive and Restricted information is safer if it is encrypted.
- If University equipment is used to create information classified as Restricted which is not encrypted, you must:
  - Make sure that the equipment is not a public computer
  - The equipment is physically secured from unauthorised access
  - Using of the equipment requires adequate user authentication (e.g. login password)
- You must delete any residual unencrypted data from any University equipment that you have used to create Restricted files as soon as possible.

Disclosure

- You may reveal Restricted information only to those who need it to carry out their official University work.
- Data users should be aware of the classification and the controls needed to protect it. (e.g. use of classification label if appropriate)
- Classified data is not to be provided to any third party unless a confidentiality undertaking has been signed by both parties.
- Disclosure of Sensitive or Restricted information should be made via secure channels such as VPN or network storage with proper access control.

Storage

- For Sensitive or Restricted data, unless the data is encrypted, you must save it :
  - on the Storage Area Network (SAN) assigned only to authorised users;
  - in private storage areas on the Local Area Network (LAN); or
  - in shared storage areas on LANs that are only accessible to authorised users.
- You must not store this sort of data on unencrypted local hard disks.
- The storage device must be physically secured
  (i.e. network storage physically secured in monitored data-centre or local storage of computer physically secured from unauthorised access)
- You may make back-up copies of Restricted data for disaster recovery provided that the backup media (e.g. backup tapes) are physical secured and only authorised operators are assigned with access to the backup media.

Storage

- Where you use removable media to transport or present Sensitive or Restricted data, the following controls apply:
  - You must keep the removable media with you at all times or secure it under lock and key where this is not practical.
  - For media containing data classified as Restricted, you must:
    - Return it during normal working hours;
    - destroy the data after use; or
    - store it outside normal working hours in encrypted format

Copying and Transmitting

- You may only copy Sensitive or Restricted data to removable media for approved special use such as:
  - Transporting the data to a research sponsor or another University involved in collaborative working; and
  - presentation of the data
- Only copy the minimum amount of Restricted data for the required purpose
- Securely delete or destroy the copy as soon as you can after their special use.
  - *Simple deletion under common operating systems does not remove the content of the files. File erase tools should be used to completely delete the file.*
- Keep the number of copies of Restricted data to as few as is operationally practical.
- All copies are to be tracked by the data owner/ custodian and treated

E-mail

- Sensitive or Restricted information may be sent as a encrypted/ password protected attachment to an e-mail
- The recipient is informed of the password by a different method such as over the telephone.
- Do not send the password in the same e-mail that contains the password protected attachment.
- Recipients should be aware of the classification, the protection required and manage the data in accordance with the protection requirements.

Fax

- Particular care required for sending classified documents by fax.
  - Make sure the recipient is standing by at the receiving end to collect the fax as it is printed;
  - The sender must be certain that the number dialed is correct and is not misdialed.

Post

- When sending Restricted documents through the post, make sure that the outer envelope does not show the classification label.
- When sending Restricted documents through the internal mail system, always use sealed envelopes.

Copying and Transmitting

- When sending Restricted documents by post, they must always be double enveloped.
  - Use a trusted delivery service so that you can check that the documents were delivered;
  - address the **inner** envelope to the intended recipient and include the wording RESTRICTED in the centre, top and bottom, and on both sides;
  - use clear sticky tape to ensure the flap of the outer envelope is well sealed;
- Write only the recipient's name and address on the front of the outer envelope along with the 'return to sender if undelivered' details on the flap. You must not indicate the confidential nature of the contents on the outer envelope.

Printing

- Restricted documents may only be printed with the permission of the document's author.
- When making copies of Restricted documents:
  - Use secure print function or make sure someone is collecting the print-out once the copies are printed;
  - keep the number of copies as low as possible; and
  - treat all copies in the same way as the original.

Backup

- Backup of Sensitive or Restricted information should be made in encrypted format. Password for the encrypted content should only be known to the data owner or in parts by multiple IT operation staff.
- If encryption for backup is not feasible, data owner should be informed of the risk of unencrypted backup. Backup media should be physically secured and access to the backup media should be restricted to the data owner or by authorised IT operation staff

Fundamental Security

Data handling procedures are created to protect classified data. However, the effectiveness of a well-defined handling procedure depends on the fundamental security of information.

There are numerous ways in which data can be compromised. Below are ways to secure your workstation, email, passwords and internet access.

Workstation

- Lock workstation when away from desk
- Shut down the workstation each night
- Lock the office door

Password

- Always use strong passwords and keep them secret.
- Do not log in for other people for access to the computer system or e-mail system.
- Do not save passwords in files on workstation or mobile phone.
- Do not write the password on paper.
- Change the password regularly

Email

- Check your e-mail “Sent Items” and “Deleted Items” daily for sensitive data.
- Do not open email attachments that you aren’t expecting. Especially avoid attachments ending in .exe, .vbs, .pif, .scr, .com, or .bat,
- Don’t open suspicious attachment even if it looks like it is sent from someone you know as many viruses can forge, or spoof, the sender’s name from names found in address books.
- Do not email Restricted data.
- Never comply with requests for personal information from an e-mail unless you initiated the contact.

Internet

- Do not download software such as screensavers, games, or other programs from unverified sources.
- Delete temporary Internet files.
- Turn off auto-complete. It stores information such as usernames and passwords.

Physical

- Sensitive and Restricted data should be stored in secured locations (i.e. locked filing drawers and cabinets).
- Access to department office should be restricted to authorised personnel only.

Conclusion

- With well defined classification and handling policy and expensive document management technology, after all, it is still PEOPLE who:
  - Identify and classify information
  - Handle the data
  - Operate the technology

Users should always be aware of the importance of data and thus the classification and handling requirements.

Q&A

?

Copyright Statement