DATA CLASSIFICATION & HANDLING

WHERE are your data?

We come across data almost every second, every day – whether we create, process or store it. Data is growing at an exponential rate: from hard copy documents on paper to digital photos on campus computers to the terabytes of research data generated across the university. A single piece of information may repeat on all sorts of devices. How do we as individuals in the university environment keep up with our growing data management needs?


Computer Lab


Notebook


Library


External Harddisk


Paper


Printer


USB Storage Device

WHO is responsible for Data Handling?

MANAGEMENT
- Provides framework
- Defines classification

YOU

DATA OWNER
- Identifies & classifies data
- Applies Controls

IT DEPARTMENT
- Provides appropriate infrastructure and training

WHY do we need to classify data?

1. To manage the risk of losing valuable data assets by focusing our effort in protecting sensitive data
2. To help understanding the criticality and dependency of data in the university for the day to day operations
3. To effectively and efficiently implement appropriate data protection
4. To make sure students and staff know how to properly secure data according to the data type

FRAMEWORKS in Data Classification

DATA CLASSIFICATION - a tool for categorization of data. It helps you understand the following:

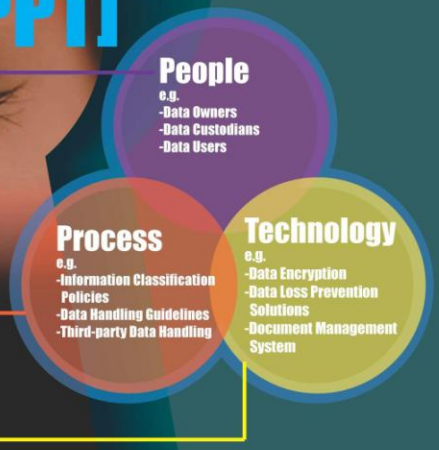
- the criticality of different types of data
- the impact to you and to the university when you lose it
- the proper way of handling each type of information
- the access rights to each type of data
- the owner and user of each type of data

People | Process | Technology [PPT]

There are different aspects when you try to implement a security management framework. PPT is one of the frameworks that allows you to do so. In considering implementation of effective data classification, we need to know...

- who will handle data,
- with what technologies, and
- undergo what processes.

It is important to know how to identify them and how they interact and interrelate to each other.



TAG YOUR OWN DATA

Data Classification Example

PUBLIC
Information which may or must be made available to the general public.
Information with no existing local, national or international legal restrictions on access.

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.

RESTRICTED
Information protected because of protective statutes, policies or regulations.
Data which data owner exercised their right to restrict access.

HOW TO HANDLE AND PROTECT YOUR DATA

Generate

DO'S
- determine the classification of the information once it is generated
- select a suitable encryption mechanism for sensitive information when it is created
- When creating unencrypted restricted information, make sure the equipment is physically secured from unauthorised access
- implement user authentication to sensitive information

DON'TS
- do not create unencrypted sensitive data on a public computer

USE

DO'S
- ensure that your user ID and password input is not observed when accessing sensitive information
- sensitive information should not be viewed by people other than yourself
- terminate remote access sessions immediately after use
- collect print-outs of sensitive information from the printer immediately

DON'TS
- do not access sensitive information unless a secure form of remote access is used for this purpose
- do not use a public computer to access sensitive information
- avoid downloading or printing out sensitive data
- do not leave sensitive information on your desk or your screen unattended
- Never give your username and password to anyone

Destroy

DO'S
- delete all unnecessary copies of sensitive information
- use data erase tools to completely delete sensitive data from the storage device
- shred paper based sensitive information
- prevent dumpster diving, e.g. do not let anyone find valuable information in discarded papers

DON'TS
- do not use simple deletion under common operation systems because deleted data can be retrieved
- do not simply dispose of sensitive information in the trash bin.

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

Transfer

DO'S
- consider additional encryption for sensitive data during the transfer process
- only copy minimum sensitive information to removable media for approved special use
- inform the recipient of the classification of information before distribution

DON'TS
- do not copy more than the minimum amount of sensitive data
- do not demote the classification of information unless you are the data owner.

Archive

DO'S
- archive sensitive information in an encrypted format or encrypt the archive media
- store the password in parts, only the data owner should know the full password
- maintain the archived information with proper physical and environmental security
- Pay attention to the security of storage media in transport

DON'TS
- do not make excessive copies of sensitive information

Transform

DO'S
- reveal sensitive information only to those who need it to carry out their official University work
- be aware of the classification and controls needed when transforming data
- transformation of sensitive information should be made via secure process with proper access control

DON'TS
- do not provide classified data for transformation to any third party unless a confidentiality undertaking has been signed by both parties

Storage

DO'S
- restrict access to sensitive data
- physically secure storage devices
- encrypt all sensitive data
- make sure authentication mechanism is in place
- back-up copies of sensitive data for disaster recovery only if the backup media are physically secured

DON'TS
- do not store sensitive data on an unencrypted storage device
- do not keep sensitive data after usage

Don't Forget the Fundamental Security

Data handling procedures are created to protect data. However, the effectiveness of a well-defined handling procedures depend on the fundamentals of information security.

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

Computers

- Lock screen/computers when away from your desk
- Shut down the computer each night
- Lock the office door

Password

- Always use strong passwords and keep them confidential
- Do not log in for other people using your own user account
- Do not save passwords in electronic files on computers or mobile devices
- 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 to ensure sensitive information is not retained in unexpected locations.
- Do not open suspicious email attachments
- Avoid sending sensitive data through email. Check the name of the recipients very carefully before sending
- Never comply with requests for personal information from an e-mail unless you initiated the contact
- Validate URL links in email and be aware of phishing websites

Internet

- Do not download software from unverified sources, such as unknown software download centre
- Delete temporary Internet files
- Turn off online form auto-complete function. It stores information such as usernames and passwords

Physical

- Sensitive data should be stored in secured locations
- Access to areas storing sensitive data should be restricted to authorised personnel only

PEOPLE –

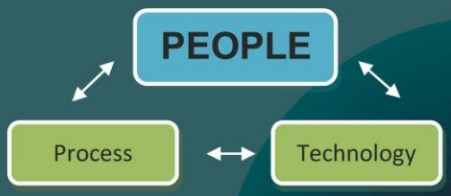
Your Involvement in Data Classification and Handling

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, thus be sensitive to data classification and handling requirements.

HUMAN FACTORS IN INFORMATION SECURITY



YOU as Part of the System

Information security is not only related to computer systems.

Why it is not just about Technology?

- Technology is vulnerable
- Organisation may not be able to adequately address all technical security concerns
- Technology is expensive
- People implement and operate technologies

PEOPLE- always the weakest link

CORE Principles of Information Security

- **CONFIDENTIALITY**- is keeping sensitive information protected
- **INTEGRITY**- is keeping information intact and valid
- **AVAILABILITY**- is keeping information available and accessible

How Human Nature Infringes Security?

MISTAKE	CARELESS	FRAUD	CURIOSITY
Inputting the wrong value Creating erroneous routine in application	Forgetting to log off Sharing passwords	Deliberate spreading of viruses Creation of hidden backdoors in application	Clicking links in email from unknown sender Installing software from unknown publisher

SCENARIO#1

Computer System Authentication – Security vs. Your Convenience

- Password policy defined the requirements for password length, complexity and expiration dates
- The password policy was implemented within the application used by general departmental users
- Validation and expiration reminders was implemented to help users in observe the password policy requirements
- However... due to the frequent password change, user wrote the password on a memo and stuck it on the screen!

Will you hang your key next to your door?

HUMAN FACTORS IN INFORMATION SECURITY

System Security Patch – Security vs. Your Technical Knowledge

- Software vendor identified system vulnerabilities
- System security patch and proof-of-concept were announced by vendors
- Security patch was not installed by the administrator due to the large amount of security updates available
- Virus was developed utilising the identified vulnerability
- Virus outbreak in campus network!

SCENARIO#2

Malicious Email – Your Awareness vs. Your Curiosity

- Security awareness training was conducted for educating people not to open email attachments from suspicious senders
- Virus writers managed to find ways to leverage general users' curiosity by coming up with interesting subject line, body text and file name

SCENARIO#3

Information Security Roles and Responsibilities

- Understand importance of information security
- Establish information security direction and allocate sufficient budget for information security management
- Follow up on security breaches
- Involve information security team in management meetings

MANAGEMENT

- Obtain up-to-date security trends and latest threats and vulnerabilities
- Acquire up-to-date technical information and system related security updates
- Timely implemented security updates to systems and report to the security management team

OPERATION TEAM

- Obtain up-to-date information regarding security trends, latest security threats and system vulnerabilities
- Conduct adequate security awareness training to users
- Review and update security policies and communicate these changes to users
- Report and escalate security incidents to management
- Build the technical competence of operation team
- Understand the security on campus and identify potential weaknesses

IS TEAM

- Understand their roles in information security
- Attend security awareness training
- Be skeptical when dealing with suspicious emails and Internet contents
- Use a strong password and maintain confidentiality
- Report security incidents to the Information Security Team

USERS