ISMS Induction

Information Security Management System

.

Agenda

- What is information?
- Data & Information
- How is information transmitted?
- The life cycle of information
- Introduction to ISMS and its importance
- Information security
- Impact of security breaches
- Information Security policies at THBS
- Security policies in SDLC
- Secure coding practices
- Handling security incidents
- Best Practices - Do’s & Don’ts

What is information?

- Information is an **asset**
- Information has **value** to an organization
- Information needs to be suitably protected

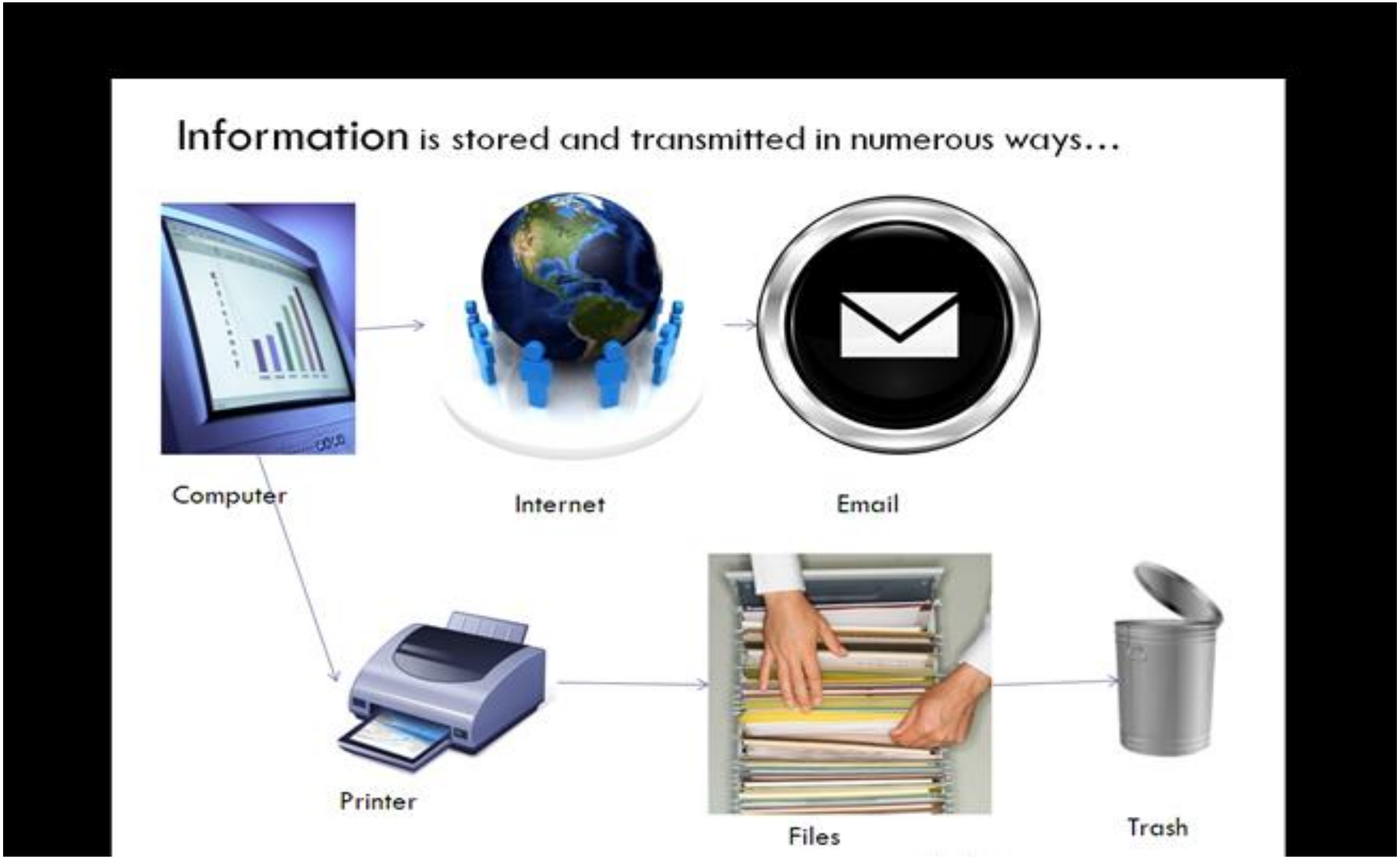
Example's for Information

- Financial Records
- Customer Details
- Employee Records
- Project/Work Details
- Business Partners Records
- Current & Future Business Plans etc.

Data VS Information

Data	Information
Data can be any character, number, images, word, text which is not organized	Information are organized and presented in a context to make it useful.
Data alone may not be significant.	But information is always important by itself.
Data is based on records, observations etc.	Information is based on analysis of data.
Data is unorganized and does not depend on information.	Information is organized and depends on data.

How is information transmitted?



Information is stored and transmitted in numerous ways…

The life cycle of information

- Created
- Stored
- Processed and refined
- Transmitted
- Destroyed
- Corrupted
- Lost
- Stolen

Introduction to ISMS

- **Information Security Management System**
- ISMS is a set of policies concerned with information security management or IT related risks

ISMS mainly focus on protecting **3 key aspects** of the organization:

1) Confidentiality: The information is not available or disclosed to unauthorized people, entities or processes.

2) Integrity: The information is complete and accurate, and protected from corruption.

3) Availability: The information is accessible and usable by authorized users.

Why ISMS & Security Risk

Why ISMS:

- Information Security that can be achieved through **technical** means **is limited**.
- Security also depends on **People, Process, Policies** and **Procedure**.
- Security is not a once off exercise but an **ongoing process**.

Information Security Risk & ISO 27001:

- ISMS mandates that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.
- ISO 27001 provides a framework for implementing ISMS

Business importance of ISMS

- Business continuity
- Minimization of damages and losses
- Competitive edge
- Profitability and cash-flow
- Respected organization image
- Legal compliance

Information security

- The architecture where an integrated combination of appliances, systems and solutions, software, alarms, and vulnerability scans work together
- Information security is achieved using several strategies
- Essential to protect vital processes and systems
- Has to be monitored 24x7
- Involves people, processes, technology, policies, procedures.

Information security is the responsibility of every employee in the organization rather than one department

Impact of security breaches

- Loss of reputation
- Financial loss
- Loss of intellectual property
- Legislative breaches leading to legal actions (Cyber Law)
- Loss of customer confidence
- Costs of business interruption

Loss of goodwill

IS policies at THBS

The policies are available in MIS at-

https://my.thbs.com

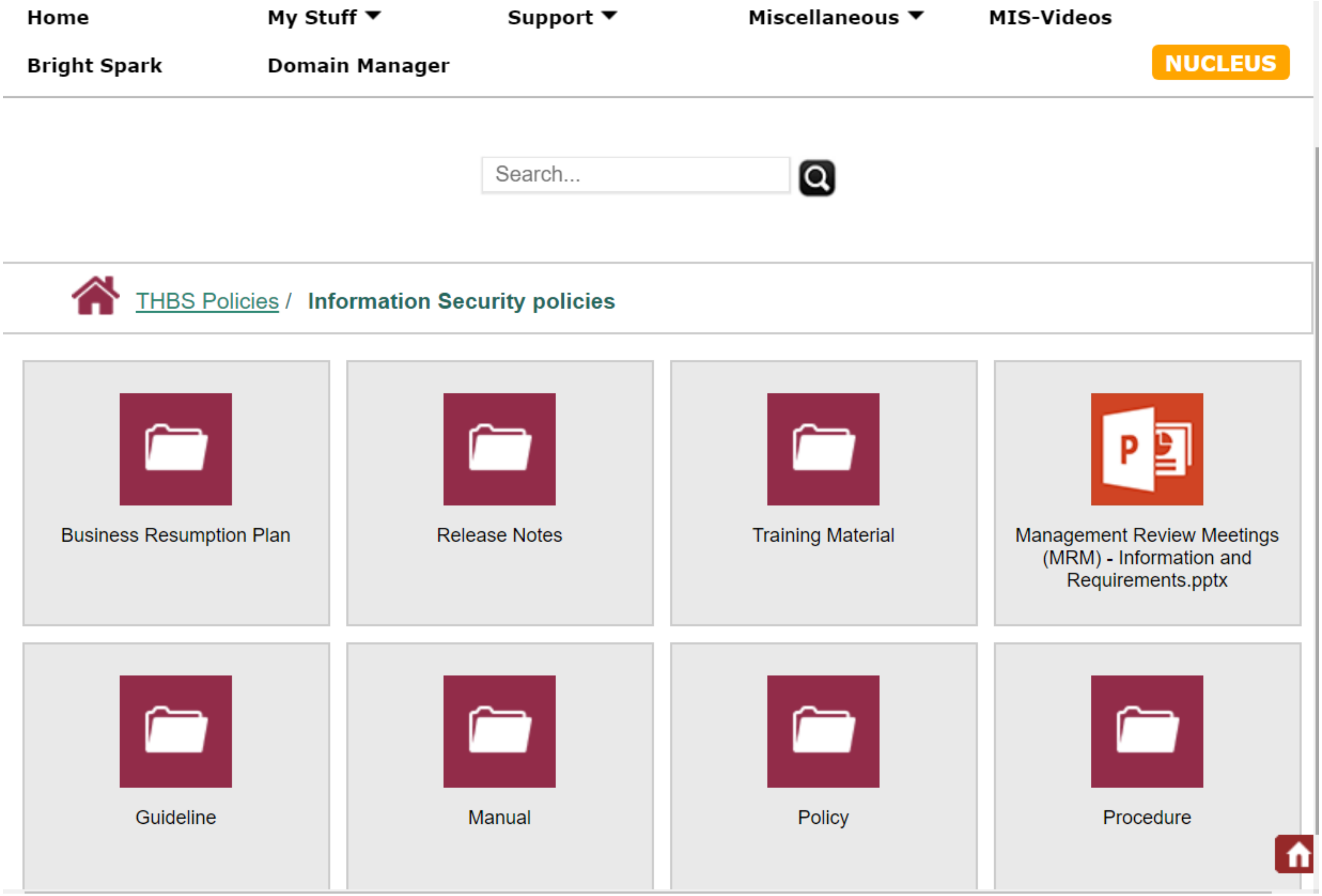
↓

Miscellaneous

↓

Information Security Policies

IS policies at THBS



THBS Policies / Information Security policies

- Business Resumption Plan
- Release Notes
- Training Material
- Management Review Meetings (MRM) - Information and Requirements.pptx
- Guideline
- Manual
- Policy
- Procedure

Security policies in SDLC

Each phase of the SDLC is required to map with the security activities explained below:

Requirements Gathering

Security Requirements

Setting up Phase Gates

Risk Assessment

Design

Identify Design Requirements from security perspective

Architecture & Design Reviews

Threat Modelling

Security policies in SDLC

Coding

Coding Best Practices

Perform Static Analysis

Testing

Vulnerability Assessment

Fuzzing*

Deployment

Server Configuration Review

Network Configuration Review

***Fuzzing** or fuzz **testing** is an automated software **testing** technique that involves providing invalid, unexpected, or random data as inputs to a program.

Secure coding standards & practices

Secure coding standards are rules and **guidelines** used to prevent **security** vulnerabilities. Used effectively, **secure coding standards** prevent, detect, and eliminate errors that could compromise software **security**.

Secure coding practices

To reduce or nullify the security vulnerabilities in our products and services our delivery teams are following the popular secure coding practices like **OWASP**. Also, **Data Protection Impact Assessment(DPIA)** is incorporated to ensure GDPR compliance along with other measures for application security & data privacy protection.

Handling security incidents

- Report security incidents (IT and Non-IT) to the helpdesk through
  - E-mail : **security@thbs.com**, **ciso@thbs.com**
  - Telephone : **080 4182 7244**
  - Anonymous reporting through drop boxes
- Do not discuss security incidents with anyone outside the organization
- Do not attempt to interfere with, obstruct or prevent anyone from reporting incidents

Do’s

- Wear identity cards and badges inside the office premises
- Check identity of any strangers inside the office premises
- Attend to visitors only in the discussion rooms available in the reception areas
- Always use at least 8 character passwords with a combination of alphabets, numbers and special characters, while avoiding common dictionary words and names
- Use Internet services and official email only for business purposes
- Follow mail storage guidelines to avoid blocking of emails
- Ensure that your desktops have the latest antivirus updates
- Collect the printouts as soon as you print

Do’s

- Ensure that your system is locked when you are away
- Always store laptops/ media in a lockable place
- Ensure that sensitive business information is under lock and key when unattended
- Ensure back-up of sensitive and critical information assets
- Understand compliance issues such as

  - Cyber Law

  - IPR, Copyrights, NDA

  - Contractual obligations with customer
- Verify credentials, if the message is received from an unknown sender
- Always switch off your computer before leaving for the day.

Don’ts

- Do not bring visitors in the operations area without prior permission
- Do not practice *piggybacking*
- Do not use pen drives, zip drives, iPods, or other storage devices unless authorized
- Do not use internet for viewing, storing or transmitting unauthorized material
- Do not use Internet for hacking other computer systems
- Do not use Internet to download/upload commercial software or copyrighted material.

Don’ts

- Do not use official email ID for any personal subscriptions
- Do not send unsolicited mails of any type like chain letters/hoax
- Do not send mails to clients unless you are authorized to do so
- Do not open any mail or attachment which is suspected to be a virus or received from an unidentified sender

Assessment

- Please click on the following link to take up an online test to gauge your understanding of ISMS. This is **mandatory** and will not take up more than 15 minutes of your time

- **testmoz.com/1930324**

Thank You