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

Information Security- Perspective for Management  
Information Security Management Program – Concept and Implementation
Agenda

- Information Security Management
- Information Security Fundamentals
- The Standard - ISO27001
- ISO27001 – 11 Domains
- Information Security Change Management
- Information Security Change Management - Example
Information Security Management

**Information** Security Management

- **Physical Information**
  - e.g. paper forms / answer scripts / proposals / project progress reports …

- **Electronic Information**
  - e.g. financial data (accounting system)
    student information (registry system)
    payroll information (HR system) …
Information Security Management

“Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction”

(Wikipedia)

Information security exists to: “ensure adequate and proportionate security controls that adequately protect information assets and give confidence to customers and other interested parties. This can be translated into maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image.”

(ISO27001)
Information Security Management

- The risks associated with information
- The corresponding controls in place to manage those risks
- Controls:
  - Technology measures
  - Organisational structures
  - Procedures
  - Policies
  - Plans
- Industry standard for information security management – ISO27001
Why manage information security?

Data Loss Statistics
Why manage information security?

Data Loss Statistics

![Data Loss Statistics Chart]

Source: KPMG International, October 2010
The core principles of information security:

- “Confidentiality” is keeping sensitive information against unauthorised access
- “Integrity” is keeping information intact and valid
- “Availability” is keeping information available and accessible
• Information security is not only related to computer systems.
• People are always the weakest link.
• A complete framework is required to manage information security.

“JUCC is committed to improve the security environment of the universities in all 3 perspectives”
Types of Information Security Controls

- Administrative
  - Logical
  - Physical

- Detective
- Corrective
- Preventive

Limitations
- No 100% assurance
- Breakdown e.g. misunderstand/ mistake
- Involve human judgement
- Management override
- Collusion
Control Implementation - Cost vs Loss

Cost of Loss

Cost of Control

Total Cost

Optimised Level of Control
Standard- ISO27001

• Information Security Management System (ISMS) standard

• Published by International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

• Requires management:
  • Systematically **examine** the organization's information security risks, taking account of the **threats, vulnerabilities and impacts**;
  • **Design and implement** a coherent and comprehensive suite of information security controls and/or other forms of **risk treatment** (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
  • Adopt an overarching **management process** to ensure that the information security controls continue to meet the organization’s information security needs on an **ongoing basis**.

(Source: Wikipedia)
ISO27001 - 11 Domains

1. Security Policy
2. Organisation of Information Security
3. Asset Management
4. Human Resource Security
5. Physical and Environment Security
6. Communication and Operations Management
7. Access Control
8. Information System Acquisition, Development and Maintenance
9. Information Security Incident Management
11. Compliance
ISO27001- 11 Domains (cont’d)

- Security Policy
  - Security *policy document* approved and communicated
  - Regular *review* of the policy document

- Organisation of Information Security
  - Clear direction and visible *management support*
  - *Managed implementation* of security controls
  - Information security *responsibilities* defined
ISO27001 - 11 Domains (cont’d)

- Asset Management
  - Information, software & physical asset inventory
  - Information classification
  - Information handling procedures

- Human Resource Security
  - Employment checks
  - Confidentiality/ non-disclosure agreements
  - Information security training
  - Disciplinary process for security violation
ISO27001- 11 Domains (cont’d)

• Physical and Environment Security
  • Physical protection of premises/ facilities
  • Protection against natural disasters
  • Protection against communication interception
  • Clear desk policy

• Communication and Operations Management
  • Operating procedures
  • Security requirements for contractors
  • Detection and prevention of malicious software
  • Data backup
  • Network, email, portable media and disposal management procedures
ISO27001- 11 Domains (cont’d)

• Access Control
  • User registration/ deregistration process
  • Password controls
  • User access review
  • Remote access control
  • Audit logging

• Information System Acquisition, Development and Maintenance
  • Data validation
  • Message authentication
  • Cryptography management
  • Control over testing data
  • System change controls
  • Prevention against covert channels
ISO27001- 11 Domains (cont’d)

• Information Security Incident Management
  • Incident prioritisation & classification
  • Channels for incident reporting
  • Incident escalation procedures
  • Contacts of regulatory bodies and law enforcement agencies

• Business Continuity Management
  • Business continuity framework
  • Established business continuity plans
  • Regular business continuity test
ISO27001- 11 Domains (cont’d)

- Compliance
  - Defined compliance requirements
  - Procedures implemented to comply with requirements (e.g. personal data/ privacy protection)
  - Regular compliance checks
Information Security Management – ISO27001

Plan-Do-Check-Act (PDCA)
A model adopted by ISO27001

**Act**
- Security improvement plan;
- Review and update of ISMS components, such as policy and procedures.

**Check**
- Review of incidents and lessons learnt;
- Self internal compliance audits;
- Review of risk assessment and action required.

**Plan**
- Risk assessment, risk treatment and risk acceptance.

**Do**
- Incident reporting and management;
- Regular updates of news and trends of information security;
- Regular information security training or awareness program to staff member.
Managing Changes
in Information Security Management
Managing Changes in Information Security Management

Managing Changes

Managing changes is essential in information security management as a structured approach to shifting/transitioning individuals, teams, and organisations from a current state to a desired future state.

Examples of change:
• Missionary changes
• Strategic changes
• Operational changes (including Structural changes)
• Technological changes
• Changing the attitudes and behaviors of personnel

(Wikipedia)
Information Security Change

• Includes changes to policy, direction, strategy and operations relating to information security

• May affect a large number of personnel in an organisation

• May face resistance from change audience

• Should be well managed
Managing Changes in Information Security Management

**Process**

- Evaluate the **current situation**
- Assess the scope of change
  - **Need** for change
  - **Capability** to change
- Define the **objective, goal and process**
- Develop the change management **plan**
- **Communicate** the change to stakeholders and relevant personnel (the plan, reasons and benefits)
- **Execute** (including training to personnel)
- **Counter resistance**
- Progress **tracking**, evaluation & fine-tuning
Example

To Implement password expiry requirement (e.g. 90 days) across the institution

- **Current Situation:**
  No password expiry on systems, users are not used to changing and remembering new passwords.
  Passwords are easily cracked by brute-force attack.
  Unauthorised access identified due to leakage of username and password.

- **Need for Change:**
  Improve access security.

- **Capability to Change:**
  System – Ready for password expiration requirements.
  Users – Resistance towards implementation of password expiry.
Example

• **Objective & Goal:**
  Implement consistent password expiry requirement across the university for all information systems

• **Change Management Plan:**
  Timeline, budget, performance indicators, instructions, technical support, contacts

• **Communication:**
  Early communication to staff and students, explaining the new processes, as well as the benefits and needs

• **Counter Resistance:**
  Understand the source of resistance, provide training and counseling

• **Progress Tracking:**
  Monitor the helpdesk request raised by users and fine tune parameters such as the expiration period (e.g. from 90 days to 180 days for the first phase of implementation)
Summary

• Information security management framework is **essential** for the overall security of data in the university.

• Defining sound information security management is the **responsibility** of university’s management.

• Information security changes should be **well managed**.
All material in this document is, unless otherwise stated, the property of the Joint Universities Computer Centre ("JUCC"). Copyright and other intellectual property laws protect these materials. Reproduction or retransmission of the materials, in whole or in part, in any manner, without the prior written consent of the copyright holder, is a violation of copyright law.
A single copy of the materials available through this document may be made, solely for personal, noncommercial use. Individuals must preserve any copyright or other notices contained in or associated with them. Users may not distribute such copies to others, whether or not in electronic form, whether or not for a charge or other consideration, without prior written consent of the copyright holder of the materials. Contact information for requests for permission to reproduce or distribute materials available through this document is listed below:
copyright@jucc.edu.hk
Joint Universities Computer Centre Limited (JUCC),
Room 223, Run Run Shaw Building,
c/o Computer Centre, The University of Hong Kong,
Pokfulam Road, Hong Kong