ICT CENTRE

Information Security Tips

Director ICT Centre

Introduction

- This Tips are based on ISO/IEC 27001 Standard
- This standard provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System (ISMS)
- ISO/IEC 27001 is a framework that helps an organization protect information such as financial data, intellectual property or sensitive customer information
- It helps an organization to identify risks and puts in place appropriate security measures

ISO/IEC 27000 Series

- ISMS Family of Standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
- Provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS)

ISO/IEC 27000 Series

ISO/IEC 27000	Overview and Vocabulary
ISO/IEC 27001	Requirements
ISO/IEC 27002	Code of Conduct
ISO/IEC 27003	Implementation Guide
ISO/IEC 27004	Measurements
ISO/IEC 27005	Risk Management
ISO/IEC 27006	Certification Guide
ISO/IEC 27007	Management System Auditing
ISO/IEC TR 27008	Technical Auditing
ISO/IEC TR 27008	Security Controls
ISO/IEC 27010	Inter-organizational Comm
ISO/IEC 27011	Telecomm Organizations
ISO/IEC 27013	Integrated Implementation
ISO/IEC 27014	Info Security Governance
ISO/IEC TR 27015	Financial Services
ISO/IEC 27017	Cloud Services
ISO/IEC 27018	Cloud Privacy
ISO/IEC TR 27019	Process Control in Energy
ISO/IEC 27031	Business Continuity
ISO/IEC 27032	Cybersecurity
ISO/IEC 27033 1-6	Network Security
ISO/IEC 27034 1-2	Application Security
ISO/IEC 27035	Incident Management
ISO/IEC 27036 1-3	Security for Supply Chain
ISO/IEC 27037	Digital Forensics
ISO/IEC 27038	Redaction Of Digital Docs
ISO/IEC 27039	Intrusion Prevention
ISO/IEC 27040	Storage Security
ISO/IEC 27041	Investigation Assurance
ISO/IEC 27042	Analyzing Digital Evidence
ISO/IEC 27043	Incident Investigation

ISO/IEC 27001:2013

- Clause 1: Scope
- Clause 2: Normative references - contained in ISO/ IEC 27000
- Clause 3: Terms and definitions - ISO/IEC 27000
- Clause 4: Context of the Organization
- Clause 5: Leadership
- Clause 6: Planning
- Clause 7: Support
- Clause 8: Operation
- Clause 9: Performance Evaluation
- Clause 10: Improvement

ISO/IEC 27001:2013

Clause 4: Context of the Organization

- This is the clause that establishes the context of the organization and the effects on the ISMS
- The starting point is to identify all external and internal issues relevant to your organization and your information or information that is entrusted to you by 3rd parties
- Establish all interested parties and stakeholders and how they are relevant to the information
- Identify requirements for interested parties which could include legal, regulatory or contractual obligations.
- Show how you establish, implement, maintain and continually improve the ISMS in relation to the standard

ISO/IEC 27001:2013

Clause 5: Leadership

- Top management need to establish the ISMS and information security policy, ensuring it is compatible with the strategic direction of the organization
- Top management need to make sure that Info Sec Policy is available, communicated, maintained and understood by all parties
- Top management must ensure that the ISMS is continually improved and that direction and support are given

ISO/IEC 27001:2013

Clause 6: Planning

- Outlines how and organization plans actions to address risks and opportunities to information
- Focuses on how an organization deals with info security risks
- Guide - ISO 31000, the international standard for risk management
- Organizations are required to produce a "Statement of Applicability" (SoA)
- The SoA provides a summary of the decisions an organization has taken regarding risk treatment, the control objectives and controls included/excluded and why
- The need to establish information security objectives

ISO/IEC 27001:2013

Clause 7: Support

- This is all about getting the right resources – people and infrastructure to establish, implement, maintain and continually improve the ISMS
- It deals with requirements for competence, awareness and communications to support the ISMS
- The organization also needs to ensure that internal and external communications relevant to info security and the ISMS are appropriately communicated
- Organizations need to determine the level of documented information that is necessary to control the ISMS

ISO/IEC 27001:2013

Clause 8: Operation

- This clause is all about the execution of the plans and processes
- Execution of the actions determined and the achievement of the info security objectives
- Any changes, whether planned or unintended need to be considered here and the consequences of these on the ISMS
- Performance of information security risk assessments at planned intervals
- Implementation of the risk treatment plan

ISO/IEC 27001:2013

Clause 9: Performance Evaluation

- This clause is all about monitoring, measuring, analyzing and evaluating an organization's ISMS to ensure that it is effective and remains so
- Internal audits and management reviews will need to be carried out at planned intervals

ISO/IEC 27001:2013

Clause 10: Improvement

- This is concerned with corrective action requirements - how an organization reacts to nonconformities, take action, correct them and deal with the consequences
- An organization is required to show continual improvement of the ISMS

Way Forward

- An ISMS Leader has been appointed
- 15 ISMS Champions have been appointed across campuses
- Training of Implementers (Process Owners)
- Conducting awareness training for identified employees
- Creating Risk Registers and Risk Management Action Plan
- Documenting ISMS Policy and Procedures
- Establishing information assets and securing them
- Launching the ISMS based on the ISO/IEC 27001:2013