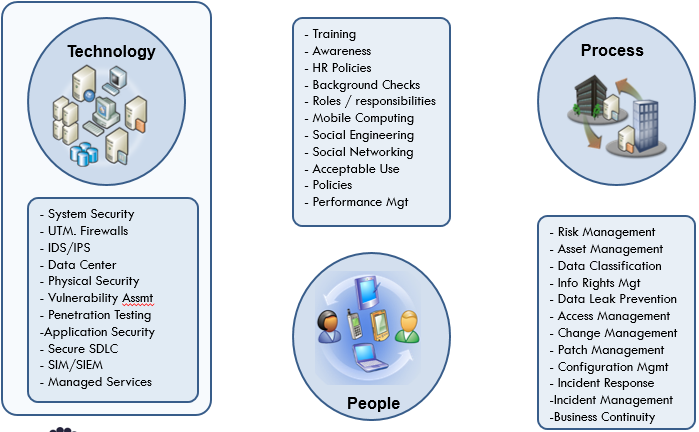


**Information Security Management include:**

* Define Scope and Boundaries of the ISMS
* Define the Security Policy
* Define a Risk Assessment Approach of Organisation
* Identify the Information Assets and their Risks
* Analyze and Evaluate the Risks
* Identify and Evaluate options for Treatment of Risk
* Select Control Objectives and Controls for treating Risks
* Formulate Risk Treatment Plan and Implement RTP Plan
* Implement Control to meet Control Objectives
* Define how to measure effectiveness of the Controls
* Implement Training and Awareness Program
* Implement of procedures and other controls capable of detection
* Security Events / Incidents.
* Promptly Detect errors in result of Processing
* Identify Security Breaches and Incidents
* Regular Reviews of Effectiveness of the ISMS
* Measure the Effectiveness
* Review Risk assessment at planned intervals
* Conduct Internal Audits
* Implement the identified improvements
* Take appropriate corrective and Preventive actions.
* …

**Information Security Management involve:**



**Security Policy:**

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Information security policy document

Review of the information security policy

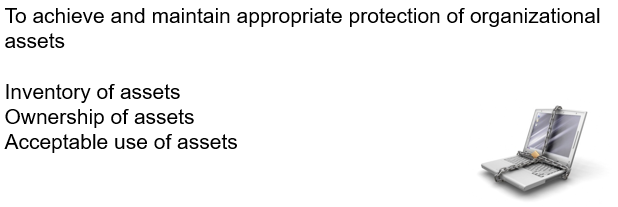
**Information Security within the Organization:**

* Management commitment to information security
* Information security co-ordination
* Allocation of information security responsibilities
* Authorization process for information processing facilities
* Confidentiality agreements
* Contact with authorities
* Independent review of information security

**Information Security with External Parties:**

* To maintain the security of organizational information and information processing facilities that are accessed processed, communicated to, or managed by external parties
* Identification of risks related to external parties
* Addressing security when dealing with customers
* Addressing security in third party agreements

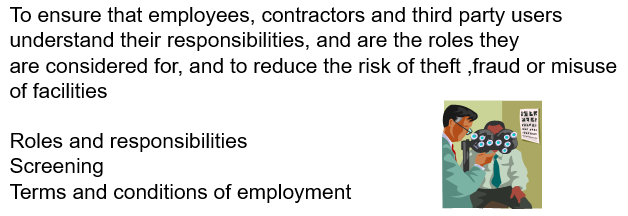
**Information Security with Asset Management:**



**Information Security Classifications:**



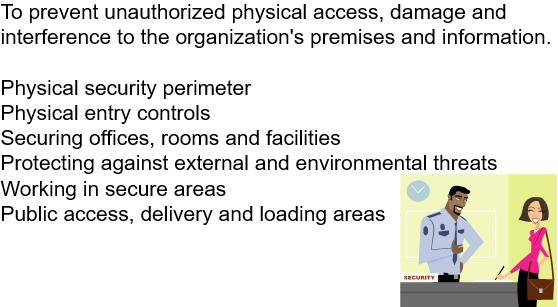
**Information Security and Human Resources:**



Additional Human Resource Specific Considerations:

* Management Responsibilities
* Information security awareness, education and training
* Disciplinary process
* Termination responsibilities
* Return of assets
* Removal of access rights
* …

**Physical and Environmental Security:**



Additional Considerations:

* Equipment sitting and protection
* Supporting utilities
* Cabling security
* Equipment maintenance
* Security of equipment off-premises
* Secure disposal or re-use of equipment
* Removal of property
* …

**Network Security:**

To ensure the protection of information in networks and the protection of the supporting infrastructure

Network controls

Security of network services

**Media Security:**

To protect unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities

* Management of removable media
* Disposal of media
* Information handling procedures
* Security of system documentation
* …

**Electronic Commerce Security:**

To ensure the security of electronic commerce services and their secure use.

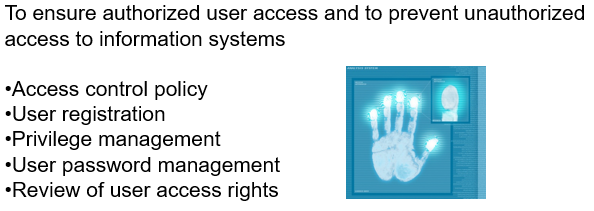
* Electronic commerce
* On-line transactions
* Publicly available information
* …

**Security Implementation: Monitoring**

To detect unauthorized information processing activities.

* Audit logging
* Monitoring system use
* Protection of log information
* Administrator and operator logs
* Fault logging
* Clock synchronization
* …

**Security Implementation: Access Control**



NOTE: We have a separate chapter on this subject.

**Security Implementation: Technology**

To prevent errors, loss, unauthorized modification or misuse of information in applications.

* Input data validation
* Control of internal processing
* Message integrity
* Output data validation
* …

To protect the confidentiality, authenticity or integrity of information by cryptographic means.

* Policy on the use of cryptographic controls
* Key management
* Security of system files
* Control of operational software
* Protection of system test data
* Access control to program source code

To maintain the security of application system software and information. Implement change control procedures. (We have a separate chapter on the subject).

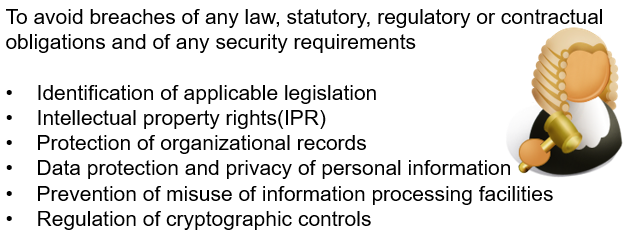
* Technical review of applications after operating system changes
* Restrictions on changes to software packages
* …

**Security Implementation: Incident Management**

To ensure information security events and weakness associated with information systems are communicated in a manner allowing timely action to be taken.

* Reporting information security events
* Reporting security weakness
* Responsibilities and procedures
* Learning from information security incidents
* Collection of evidence
* …

**Information Security: Law Compliance**



**Additional Thoughts:**

* What’s is your approach to handle so many passwd?
* Intrusive electronic monitoring on employees a legal issue?
* What are the ways safeguard a file transfer to a client? (Fundamental question/issue):
  + Md5 the file, checksum/signature.
  + FTP Site for temporary file transfer?
* Ideas for “bullet” proof information/data security:
  + Cut the wire-internet connection?
  + Operate in a missile silo-mode? (USB-only data transfer-update?)
  + DIS-information? (Confuse the hackers by vast amount bogus info. The US version of a story…)
  + …
  + Is information useful, if NOT shared?
  + There is no absolute information security.
  + What is your damage control, recovery plan?
* Cloud Computing and information Security: Your concerns? Who is going to be the last one to migrate?
* …