**Domain 5 Risk Management**

**5.1 Policies Personnel**

**Policies**

* Policies form foundation of any security program
* Policies define

1. How IT approach security
2. How users approach security
3. How certain situations are handled

**Policy Document Types**

* Policies – general management rules
* Standards – specific mandatory controls, based on given policy
* Guidelines – recommendation/good practices
* Procedures – instructions on how to implement policy/standard

**Policy Elements**

* Overview
* Purpose
* Scope
* Target audience
* Definitions
* Version
* Implementation dates
* Compliance/exceptions
* Policy statements

**Common Policies**

* Acceptable Use Policy (AUP)
* Access Policy
* Authentication Policy
* Backup & Recovery Policy
* Data Classification Policy
* Email/Messaging Policy
* Social Media Policy
* Physical Security Policy
* Incident Response Policy
* Mobile Device Policy
* Network Security Policy

1. Wireless Policy
2. Remote Access

**Acceptable Use Policy (AUP)**

* Describes how employees in organisation can use company systems & resources
* Includes rules of behaviour/code of conduct for users to behave in manner that is legal, ethical & within cultural expectations of the organisation
* Should also outline consequences for misuse

**Standard Operating Procedure (SOP)**

* Standard set of instructions for workers to carry out routine operations
* Aim to achieve efficiency & consistent output

**Agreement Types**

* Non-Disclosure Agreement (NDA) – protects against sensitive information disclosure
* Business Partner Agreements (BPAs) – specifies partner financial & fiduciary responsibilities (profit sharing)
* Service-Level Agreements (SLAs) – specifies nature & level of service by provider (uptime)
* Memorandum of Understanding (MOU) & memorandum of Agreement (MOA)

1. Outlines terms & details of agreement

* Interconnection Security Agreement (ISA)

**Personnel Management**

* Mandatory vacations
* Job rotation
* Separation of duties
* Clean desk
* Background checks
* Onboarding
* Terminations/exit interviews
* Role-based awareness training – based on job responsibilities
* Continuing education