5.1 Leadership and commitment

- Ensure information security policy and objectives are **established**
- Communicate **importance** of information security management and **conformance** to ISMS requirements
- Ensure information security is integrated in the organisation processes
- Ensure that the ISMS achieves desired **outcomes**
- Ensuring availability necessary human and financial **resources**
- Promote continual **improvement** of the ISMS

5.2 Policy

- Tailored to the organization
- Includes the information security objectives
- Shows the management commitment
- Must be high level policy
- Must be communicated
- Must be reviewed regularly
- Must have an owner

Example of Policy of a Bank

- **Objectives**
  - Protect the organization's information asset, customer data and transactions
  - Ensure Confidentiality, Integrity, Availability of Information
  - Meet Regulatory and legislative requirements
- CEO **commitment and support**
- Ownership : Board of directors
- Responsibilities : IT Security department, CISO, employees
- Policy is communicated by the CISO
- Should be reviewed every year

HealthBridge Policy

- **Purpose**: establish and maintain effective ISMS
- **Scope**: applies to all employees, contractors, and third-party providers
- **Objectives**: protect sensitive info, ensure compliance, improve ISMS
- **Roles**: CISO oversees ISMS, all responsible for compliance
- **Risk management**: regular risk assessments, prioritize security controls
- **Information security controls**: access controls, encryption, training, incident response, testing
- **Compliance**: comply with all applicable laws, regulations, and standards
- **Monitoring and review**: monitor and review ISMS effectiveness and compliance
- **Review Frequency**: Policy reviewed and updated annually or as needed

5.3 Organisational roles, responsibilities and authorities

- **Assign** and **communicate** responsibilities and roles for Information security
- Assign the responsibility for
  - Ensuring the ISMS is **conforms** to ISO 27001 requirements
  - Reporting the **performance** of the ISMS
- Documentation is not required

Example of Roles in the ISMS

- Information Security Officer
  - Definitions, Supervision, coordination of ISMS activities
  - Communication of information related to the ISMS
  - Should have managerial, communication and technical skills
- IT Administrator
  - Responsible of security devices and technologies
  - Supervision of access rights
- Internal Auditor
  - Performs audits
  - Assesses compliance with ISO 27001 requirements

Roles and Responsibilities at HealthBridge

- CISO responsible for overall information security management.
- IT Security Manager responsible for day to day ISMS operations.
- IT Department responsible for implementing technical controls
- HR Manager manages employee security training.
- Legal department ensures compliance
- Employees must follow security policies and report incidents.