

Management Responsibilities

[Organization Name]

[Version no.]

Objective: To define the roles and responsibilities of senior management in the development, implementation, and maintenance of the information security management system (ISMS) in accordance with ISO 27001.

Scope: This policy applies to all personnel and other interested parties involved in the management and protection of information assets within the organization.

Policy Statement:

1. Roles and Responsibilities:

- a. Senior management is responsible for providing direction and oversight of the ISMS.
- b. Senior management is responsible for ensuring that the ISMS is developed, implemented, and maintained in accordance with ISO 27001.
- c. The information security manager is responsible for the development, implementation, and maintenance of the ISMS.
- d. The information security manager is responsible for reporting to senior management on the performance of the ISMS.
- e. Senior management is responsible for ensuring that adequate resources are allocated to the development, implementation, and maintenance of the ISMS.
- f. Senior management is responsible for ensuring that the information security policy is communicated to all personnel and other interested parties.

2. Information Security Management System (ISMS):

- a. Senior management is responsible for ensuring that the ISMS is aligned with the organization's objectives and risk management strategies.

- b. Senior management is responsible for ensuring that the ISMS is integrated into the organization's business processes.
- c. Senior management is responsible for ensuring that the ISMS is continually improved to meet changing business needs and security threats.

3. Communication and Training:

- a. Senior management is responsible for ensuring that the information security policy is communicated to all personnel and other interested parties.
- b. Senior management is responsible for ensuring that personnel are trained on their roles and responsibilities in the ISMS.
- c. Senior management is responsible for ensuring that personnel are trained on the relevant security controls and procedures.

4. Compliance:

- a. Senior management is responsible for ensuring that the organization complies with all relevant legal, regulatory, and contractual requirements related to information security.
- b. Senior management is responsible for ensuring that the organization complies with the requirements of ISO 27001.

5. Performance Measurement:

- a. Senior management is responsible for monitoring and measuring the performance of the ISMS.
- b. Senior management is responsible for reviewing the effectiveness of the ISMS and taking appropriate action to address any identified deficiencies.

6. Responsibility:

Senior management is responsible for complying with this policy and ensuring that all personnel and other interested parties are aware of their roles and responsibilities in the development, implementation, and maintenance of the ISMS.

7. Compliance:

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment or contract.

Review: This policy will be reviewed annually or as necessary to ensure its continued relevance and effectiveness in defining the roles and responsibilities of senior management in the development, implementation, and maintenance of the ISMS in accordance with ISO 27001.