

[Company]

AWARENESS AND TRAINING POLICY

Training, awareness, and education on information security

1 Document Version Control

Last Modified				Last Modified By				Document Changes			
0.1	[DATE]										Document first created

2 Document Contents Page

1	Document Version Control.....	2
2	Document Contents Page.....	3
3	Information Security Awareness and Training Policy.....	5
3.1	Purpose.....	5
3.2	Scope.....	5
3.3	Principle.....	5
3.4	Information Security Awareness and Training Topics.....	6
3.5	New Starters.....	6
3.6	In Role Employees.....	7
3.7	Training and Competency Register.....	7
3.8	Training and Awareness Plan.....	7
3.9	Assessment and Acceptance.....	8
4	Policy Compliance.....	9
4.1	Compliance Measurement.....	9

4.2 Exceptions 9

4.3 Non-Compliance 9

4.4 Continual Improvement..... 9

5 Areas of the ISO27001 Standard Addressed..... 10

3 Information Security Awareness and Training Policy

3.1 Purpose

The purpose of this policy is to ensure all employees of the organization and, where relevant, contractors receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.

3.2 Scope

All employees and third-party users.

3.3 Principle

Management is committed to information security throughout the organisation and awareness, training, and education.

3.4 Information Security Awareness and Training Topics

The topics covered:

- stating management's commitment to information security throughout the organization
- the need to become familiar with and comply with applicable information security rules and obligations, as defined in policies, standards, laws, regulations, contracts, and agreements
- personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and external parties.
- basic information security procedures (such as information security incident reporting) and baseline controls (such as password security, malware controls and clear desks)
- contact points and resources for additional information and advice on information security matters, including further information security education and training materials.

3.5 New Starters

Information Security training is provided to new starters [REDACTED]

[REDACTED]

[REDACTED]

[Redacted]

3.6 In Role Employees

General Information Security training is conducted for employees at least annually.

Information Security awareness is provided [Redacted]

[Redacted]

3.7 Training and Competency Register

A register of information security training and competency is maintained for employees.

3.8 Training and Awareness Plan

A communication plan includes training and awareness campaigns for the year.

The training and awareness plan is based on legal and regulatory requirements, business need and risk.

3.9 Assessment and Acceptance

Employees are assessed on their understanding of information security and formally sign that they have received training.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.