Information Security Policy

Template aligned with ISO 27001:2022 Clause 5.2

This template provides a structured framework for establishing your organisation's information security policy. It covers purpose, scope, principles, roles and responsibilities, and compliance requirements. Customise each section to reflect your organisation's context.

Prepared by: Nuvencia — Information Security Advisory

Author: Jaouhar Mosbahi, CISSP, CCSP, ISO 27001 LI/LA

Version: 1.0 — February 2026

Classification: Template — Customise for your organisation

This template is provided by Nuvencia for guidance purposes. Organisations should customise it to reflect their specific context, risk appetite, and regulatory requirements.

© 2026 Nuvencia. All rights reserved.

Table of Contents

1. Purpose

2. Scope

3. Information Security Objectives

4. Security Principles

5. Roles and Responsibilities

6. Risk Management

7. Acceptable Use

8. Incident Management

9. Compliance and Legal Requirements

10. Policy Review and Maintenance

11. Document Control

© 2026 Nuvencia. All rights reserved.

1. Purpose

This Information Security Policy establishes the framework for protecting the confidentiality, integrity, and availability of information assets within [Organisation Name]. It defines the organisation's commitment to information security and sets the direction for the Information Security Management System (ISMS).

[Guidance: Customise the purpose statement to reflect your organisation's specific security objectives and business context.]

2. Scope

This policy applies to all information assets owned, controlled, or processed by [Organisation Name], including but not limited to:

- All employees, contractors, and third-party personnel
- All information systems, applications, and infrastructure
- All data in any format (digital, physical, verbal)
- All locations where organisational information is processed or stored
- Cloud services and third-party platforms used for business operations

[Guidance: Define your ISMS scope boundaries clearly. Reference your Statement of Applicability (SoA) for detailed control applicability.]

3. Information Security Objectives

The organisation's information security objectives are to:

- Protect information assets against unauthorised access, disclosure, modification, or destruction
- Ensure business continuity and minimise the impact of security incidents
- Comply with applicable legal, regulatory, and contractual requirements
- Maintain and continuously improve the ISMS in accordance with ISO 27001:2022
- Foster a culture of security awareness throughout the organisation

[Guidance: Add measurable security objectives with KPIs. Example: 'Achieve less than 3% phishing simulation compromise rate by Q4.']

4. Security Principles

The following principles guide all information security decisions:

Confidentiality: Information shall be accessible only to authorised individuals who have a legitimate business need.

Integrity: Information shall be accurate, complete, and protected from unauthorised modification.

Availability: Information and systems shall be accessible to authorised users when required.

Accountability: All users are responsible for their actions regarding information assets.

Defence in Depth: Multiple layers of security controls shall be implemented to protect against threats.

Least Privilege: Access rights shall be granted based on the minimum level required to perform job functions.

© 2026 Nuvencia. All rights reserved.

5. Roles and Responsibilities

Role	Responsibility
Senior Management	Provide leadership commitment, allocate resources, approve policies, and conduct management reviews
CISO / Security Lead	Develop and maintain the ISMS, manage security operations, report to senior management, coordinate incident response
IT Department	Implement and maintain technical security controls, manage access rights, perform system hardening
All Employees	Comply with security policies, complete security training, report incidents and vulnerabilities
Third Parties	Comply with contractual security requirements and organisational policies when accessing information assets

[Guidance: Add specific names or teams for each role in your organisation.]

6. Risk Management

The organisation shall maintain a risk assessment methodology and risk register to identify, analyse, evaluate, and treat information security risks. Risk assessments shall be conducted at planned intervals and when significant changes occur. Risk treatment plans shall be approved by risk owners and monitored for effectiveness.

7. Acceptable Use

All users must use information assets responsibly and in accordance with the organisation's acceptable use guidelines. Prohibited activities include unauthorised access, sharing credentials, installing unapproved software, and transmitting sensitive data through unapproved channels.

8. Incident Management

All security incidents, suspected incidents, and vulnerabilities must be reported immediately through the designated reporting channel. The incident response team shall investigate, contain, eradicate, and recover from incidents following the Incident Response Plan.

9. Compliance and Legal Requirements

The organisation shall comply with all applicable legal, regulatory, and contractual requirements including but not limited to:

- General Data Protection Regulation (GDPR)
- Industry-specific regulations applicable to the organisation
- Contractual obligations with clients and partners
- ISO 27001:2022 requirements

[Guidance: List the specific regulations and contractual obligations applicable to your organisation.]

10. Policy Review and Maintenance

© 2026 Nuvencia. All rights reserved.

This policy shall be reviewed at least annually or when significant changes occur in the organisation, its threat landscape, or regulatory environment. Reviews shall be conducted by the CISO and approved by senior management.

11. Document Control

Field	Value
Document Owner	[CISO / Security Lead]
Approved By	[CEO / Board / Senior Management]
Version	1.0
Effective Date	[Date]
Next Review Date	[Date + 12 months]
Classification	Internal

© 2026 Nuvencia. All rights reserved.