Information Security Policy

Information Security

Version 1.0

Prepared By:
Hrushikesh Mehendale

Reviewed By:
Shruti Deshpande

FlaggGRC

Document Control

Last Modified	Reason For Change	Suggested By	Approved By
1 March 2025	Document created	Hrushi M	Shruti D
25 Mar 2026	Document reviewed, no change	Hrushi M	Shruti D
6 Oct 2026	Document reviewed, no change	Hrushi M	Shruti D

Purpose

The purpose of this policy is to set out information security policies that apply to the organization for protecting the confidentiality, availability and integrity of information.

Scope

All the staff, vendor staff and the client users.

Management Statement

“At FlaggGRC Techlabs LLP, we recognize the critical importance of information security in protecting our data, customer information, and business operations. As a responsible organization, we are committed to establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS) in accordance with ISO 27001 and other applicable legal, regulatory, and contractual requirements.

As the management of FlaggGRC, we take full responsibility for ensuring that our ISMS is aligned with the strategic objectives of our organization. We will provide the necessary resources, leadership, and support to uphold the highest standards of information security, ensuring trust and confidence among our stakeholders.”

- Hrushikesh Mehendale, Chief Executive Officer

Strategic Direction

At FlaggGRC, we are a growing company committed to information security. Our corporate clients trust us to handle confidential and sensitive data, and we take this responsibility seriously.

We are building a security-first culture, not just for compliance but to proactively manage risks, protect client data, and strengthen our security posture.

ISO 27001 certification is a key part of our operations, helping us identify, assess, and mitigate security risks while ensuring a secure and compliant environment.

With strong leadership, employee awareness, and continuous improvement, we aim to be a trusted partner in secure governance, risk, and compliance solutions.

Objectives

To turn our strategic vision into action, we have defined clear, realistic and measurable objectives as documented in the Information Security Objectives document. The intention is to establish a comprehensive baseline covering key areas.

📄Information Security Objectives

Defining Information Security

We define information security as follows:

- **Confidentiality** - Access to information should be granted only to authorized individuals with a legitimate need.
- **Integrity** - Information should be complete and accurate.

FlaggGRC

- **Availability** - Information is available whenever needed.

Policy Framework

The information security management system is based on the following set of policies, in conjunction with this policy:

- Acceptable Use Policy
- Access Control Policy
- Asset Management Policy
- Authentication Policy
- Business Continuity Policy
- Change Management Policy
- Clear Desk and Clear Screen Policy
- Configuration Management Policy
- Continual Improvement Policy
- Cryptography Policy
- Documents & Records Policy
- Equipment Siting & Protection Policy
- Event Logging & Monitoring Policy
- External Authorities Contact Policy
- Human Resources Policy
- Identity Management Policy
- Incident Management Policy
- Information Classification & Handling Policy
- Information Security Audit Policy
- Information Security Awareness Training Policy
- Information Security Objectives Policy
- Information Transfer Policy
- Intellectual Property Rights Policy
- Malware & Data Leakade Protection Policy
- Management Review Policy
- Network Security Policy
- Organization Context
- Physical & Environmental Security Policy
- Privacy Policy
- Redundancy in Information Processing Facilities Policy
- Remote Work Policy
- Risk Management Policy
- Roles & Responsibilities Policy
- Scope of ISMS Policy
- Secure Software Development Policy
- Segregation of Duties Policy

FlaggGRC

- Software Installation Policy
- Special Interest Groups Contact Policy
- Storage Media Policy
- Third Party Supplier Security Policy
- Threat Intelligence Policy
- User Endpoint Security Policy
- Vulnerabilities Management Policy
- Web Filtering Policy

Roles & Responsibilities

Everyone plays a role in keeping information secure. Management provides direction and resources for security. The CISO ensures security policies are followed and improved. The IT team manages access, safeguards systems, and responds to threats. HR and Admin handle security in hiring, training, and office safety. All employees, contractors, and vendors must follow security policies, report issues, and help protect company and client data. The roles and responsibilities are detailed in the Roles & Responsibilities document.

📓Roles & Responsibilities Register

Availability of Policies

Policies shall be made easily available to the staff and to third party users.

Training & Awareness

A training plan shall be in place to communicate the policies, processes and concepts of information security. A training plan shall be in place and documented. Training needs are identified and relevant training requirements are captured via the competency matrix.

📄Information Security Awareness Training Policy
📓Competency Matrix

Monitoring

A monitoring plan shall be in place to monitor the implementation of policies, processes and concepts of information security. The monitoring plan shall be documented as an Information Security Audit Policy document.

📄Information Security Audit Policy

FlaggGRC

Legal and Regulatory Obligations

The company shall be committed to complying with the applicable legal and regulatory obligations. A separate Legal Register shall be maintained for the same.

Compliance Measurement

The management and CISO shall ensure compliance to this policy by setting the right tone from the top, appropriate provisioning of resources, comprehensive training programs and periodic monitoring activities.

Policy Compliance

Exceptions

Any exception to this policy shall be approved and recorded by the CISO in advance and reported to the Management Review Team.

Non-Compliance

Any staff found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment.

Continual Improvement

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

FlaggGRC