Compliance Procedure

Version 1 - Approved by Rishabh

Contents

1. Objective
2. Scope
3. Compliance with Legal Requirements
4. Safeguarding Organizational Records
5. Independent Reviews of Compliance with Security Policies & Standards
6. Technical Compliance Checking
7. Intellectual Property Rights
8. Information Systems Audit
9. Corrective & Preventive Actions (Applicable & Mandatory Only if ISO 27001 is Implemented)
10. Document Security Classification
11. Non-Compliance
12. Responsibilities
13. Schedule
14. Version History

1. Objective

The objective of this procedure is to establish the methods by which management of regulatory and legal compliance requirements for the systems that are in the scope of the Information Security Management System (ISMS) that is implemented.

2. Scope

This document is applicable to all employees, contractors, and relevant third-party service providers of the organization that operate within the scope of the Information Security Management System (ISMS). The ISMS covers the company's SaaS product, supporting infrastructure hosted on AWS and GCP, source code and artifacts stored in GitHub, business email and collaboration in Google Workspace, and any employee devices used to access organizational systems.

3. Compliance with Legal Requirements

3.1 Identification of Applicable Legislation

- The Information Security Officer, together with the Legal team and Engineering team, is responsible for identifying legislation, regulations, and contractual requirements applicable to the organization's SaaS operations (including but not limited to SOC 2, ISO 27001, and GDPR).
- The Information Security Officer shall maintain and update the registry of applicable legislation and regulatory obligations as part of the ISMS documentation, and will review these updates at least annually or when triggered by significant legal, product, or infrastructure changes.
- Advice on statutory, regulatory, and contractual requirements shall be sought from the Legal team and Engineering team as needed to ensure controls and procedures align with obligations.
- The Information Security Officer, with input from Engineering and Legal, shall ensure implementation of required controls and that responsibility for those controls is assigned.
- Periodic reviews of compliance shall be conducted by the Engineering team in conjunction with the Information Security Officer; frequency of reviews will be at least annually and additionally when product, infrastructure (AWS/GCP), or regulatory changes occur.

3.2 Data Protection & Privacy of Personal Information

- Data protection and privacy shall be maintained in accordance with identified legislation and contractual requirements, including GDPR obligations for personal data processed by the SaaS product and business operations.
- Applicable legislation, regulations, and contractual privacy requirements shall be communicated to employees, contractors, and any third parties involved in processing personal information.
- The Information Security Officer shall provide guidance to Business Heads on responsibilities and procedures for handling personal data, including lawful basis, data subject rights, and data retention requirements.

- Access to personal information shall be granted on a need-to-know and role-based basis, implemented through access controls in AWS, GCP, Google Workspace, and application-level permissions managed via GitHub access and internal identity processes.

4. Safeguarding Organizational Records

All organizational records, including customer data, operational logs, configuration artifacts, and employee records, shall be classified and handled in accordance with the Data Classification Policy. Electronic records stored in AWS and GCP or in SaaS services (e.g., Google Workspace, GitHub) shall rely on the respective vendor-managed controls for durability and access control, supplemented by the organization’s access management and backup configuration reviews.

4.1 Prevention of Misuse of Information Processing Facilities

Information processing facilities, including cloud accounts, development repositories, and employee devices, must be used in accordance with the Acceptable Usage Policy. Use of personal devices to access organizational systems requires adherence to the organization's device security requirements (e.g., disk encryption, OS updates, approved endpoint protection) as defined in device management procedures.

5. Independent Reviews of Compliance with Security Policies & Standards

- The organization will continuously monitor and periodically review compliance with the listed policies and procedures, prioritizing controls relevant to SaaS operations and cloud infrastructure (AWS, GCP).
    - Human Resources Security
    - Asset Management
    - Physical and Environmental Security
    - Communications and Operations Management
    - Systems Acquisition, Development, and Maintenance
    - Supplier Management
    - Access Control
    - Network Security
    - Security Incident Management
    - Compliance
- The Information Security Officer shall ensure security procedures are tracked using the organization’s compliance documentation and tracking mechanisms.
- The HR team is responsible for security training and awareness for employees and contractors.
- Each department shall review compliance within its area; where non-compliance is identified, managers shall: determine root causes, evaluate corrective actions to prevent recurrence, implement corrective actions, and notify the Information Security Officer as appropriate.
- The Information Security Officer shall conduct or coordinate an organization-wide compliance review at least annually and more frequently as required by regulatory or operational changes.

6. Technical Compliance Checking

A minimum of one annual technical assessment (e.g., external vulnerability assessment or penetration test) shall be performed by a competent third-party in coordination with the Engineering team to identify vulnerabilities in cloud infrastructure (AWS, GCP), production systems, and web applications. Continuous automated scanning and monitoring tools shall be used to supplement annual testing, and findings shall be reported to the Information Security Officer for remediation tracking.

7. Intellectual Property Rights

Care must be taken by the Engineering team and the Information Security Officer that all third-party software and services are appropriately licensed and do not violate any copyrights or intellectual property rights.

8. Information Systems Audit

8.1 Preparing & Conducting Audits

- The organization uses automated compliance monitoring tools to perform continuous monitoring of controls where available; in addition, an annual audit of the control environment shall be performed to ensure continued compliance. Audits should consider:
  - Completeness of inventory of assets and systems.
  - Adherence to procedure SLAs.
  - Review of the list of vendors.
  - Review of Information Security Risks.
- Audits may be performed by the Information Security Officer, internal auditors, or independent external auditors. Audit results must be communicated to Senior Management and reviewed at least annually.

8.2 Audit Reports, Findings & Non-Conformance Closures

- The auditors should perform the audit and record the non-conformances and their observations/ suggestions in the Internal Audit Report.
- Any corrective actions that need to be taken must be documented in a corrective and preventive action (CAPA) register maintained by the Information Security Officer.
- The internal audit report, along with the CAPA register, must be presented to Senior Management for review and acceptance.
- The respective departments or functions should initiate corrective and preventive action on the non-conformances and close them within the committed closure time.
- At the end of the committed time frame, the Information Security Officer should verify the closure of the non-conformances.

9. Corrective & Preventive Actions (Applicable & Mandatory Only if ISO 27001 is Implemented)

The process for corrective and preventive actions should be initiated whenever a condition warrants an investigation to determine if corrective or preventive action is required.

9.1 Corrective Actions

- Corrective actions shall be documented in the CAPA Register when non-conformances are identified during internal or external audits, security incidents, management reviews, or reported deviations in service delivery. Corrective action should be initiated as a result of, but not limited to, the following:
  - Non-conformances identified during internal audits or external audits.
  - Action items from management reviews of information security effectiveness.
  - Reported security incidents.
  - Reported deviations in the provision of services.
- Problems identified by employees pertaining to security weaknesses.
- Violation of security policy and security objectives.

9.2 Preventive Actions

- The Information Security Officer shall maintain a summary of corrective and preventive actions taken; detailed records shall be retained in the CAPA Register.
- Preventive action should be determined from the analysis of appropriate data to detect trends and identify causes that may result in future non-conformances.
- The Information Security Officer shall verify the effectiveness of corrective and preventive actions for affected departments and report results to Senior Management.
- The results of corrective and preventive actions should be reviewed by the Senior Management during meetings with the Information Security Officer.

10. Document Security Classification

Company Internal. Please refer to the Data Classification Policy for more details.

11. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

12. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation. Engineering is responsible for implementing technical controls in AWS, GCP, and GitHub; Legal is responsible for regulatory and contractual interpretation; HR is responsible for employee and contractor

onboarding and training; third-party vendors (e.g., cloud providers, GitHub, Google Workspace) are responsible for their managed controls per contractual agreements.

13. Schedule

This document shall be reviewed at least annually and whenever significant changes occur to product, infrastructure (AWS/GCP), applicable legislation (e.g., GDPR), or organizational structure. Reviews shall be coordinated by the Information Security Officer.

End of Compliance Procedure. For version history, please see the next page.

Version History

	Version	Log	Date
1	Current	Policy version approved by Rishabh	13 Mar, 2026
1		New policy version created	13 Mar, 2026