Information Security Policy

|  |  |
| --- | --- |
| Owner |  |
| Approver |  |
| Last Reviewed |  |

# Scope and applicability

This policy applies to all [Company Name] information assets, including customer-sourced data, regardless of the format or processing, shared or stored. The information assets include but are not limited to information in printed or written materials, stored and transmitted electronically, shown in presentations, or spoken in conversation.

Information security is the responsibility of anyone who has access to a company's information assets, including employees, partners, consultants, agents, vendors, distributors, and contractors who use or are granted access to [Company Name] facilities or information systems. Collectively these human resources shall be referred to as "[Company Name] Personnel" in all company's security policies.

# Policy

[Company Name] defines security objectives and principles to minimize risks, avoid threats, and manage vulnerabilities to ensure business stability and agility. [Company Name] reviews security objectives and principles at least annually to reflect internal and external factors and requirements of the interested parties.

## Security objectives

The primary goal of [Company Name]'s information security is preserving the confidentiality, integrity, and availability of all forms of [Company Name]'s information assets. Other

company's security goals for stable, effective, and long-lasting company operation are:

 Provide secure and reliable products and services to [Company Name]'s clients;

 Establish secure relationships with third parties whose services are used by [Company Name] or who process [Company Name]'s information;

 Comply with the applicable legislation in information security;

 Implement the ISMS according to the leading security standards;  Protect [Company Name]'s intellectual property.

Responsible managers in their documentation, formulate information security objectives for their functions and levels. These objectives should be consistent with the information security policy.

## Security principles

To achieve the security objectives, [Company Name] establishes the security principles. The responsible personnel use them to design and implement security policies, procedures, and controls. They are:

 Compliance with the applicable legal requirements, contractual requirements, and other obligations for the protection of the information, including personally identifiable information;

 [Company Name]ʼs top management has the leading role in establishing, promoting the importance, and controlling the effectiveness of the security;

 All necessary resources are timely provided for proper security operation;

 All the personnel is responsible for complying with the security requirements;

 Personnel responsible for the design and implementation of the security have the necessary expertise and continuous education;

 Employees and third parties are regularly informed about security requirements;

 For implementing security controls, a risk-based approach is used to maximize business opportunities and minimize adverse consequences;

 Security architecture and controls embrace defense in-depth concept;

 Security controls focus on uniformity with minimization of exceptions and non- standardization and are automated whenever possible;

 Security controls are periodically reviewed to ensure efficacy and compliance with security policies and objectives.

## Security roles, responsibilities and competence

[Company Name]’s executive management commits to preserving its information assets and products' confidentiality, integrity, and availability. For the security implementation and operation, [Company Name] defines and assigns the following security roles and responsibilities cross the company:

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| GRC | Responsible for [Company Name]ʼs compliance with the leading security standards and practices. |
| Engineering | Responsible for the secure design and development of [Company Name]ʼs product and production environment. |
| IT | Implements technical measures in the corporate IT environment, monitors information security events and responds to incidents. |
| Legal | Determines the legislation requirements that could impact [Company Name]ʼs security. |
| System owners | Responsible for secure administration and maintenance of the information systems used in [Company Name]. |
| Information assets owners | Define the criticality and protect [Company Name]ʼs information assets. |
| Risk owners | Responsible for risk assessment and treatment in their functional area. |
| Information security auditors | Internal or external specialists periodically audit [Company Name]ʼs security design and operational effectiveness and who are independent of the security activities. |
| [Company Name] Personnel | Comply with [Company Name]'s information security requirements to protect the company's information assets. |

Additional internal information security roles are defined in other information security documents.

Third parties' responsibilities for [Company Name]'s information security are defined in the agreements. [Company Name] is responsible for reviewing the third parties' security before authorizing any relationship with them.

[Company Name] defines the security responsibilities of its users in the System Description of the SOC 2 report and agreements and public documents on the website.

[Company Name] ensures that all staff involved in information security are competent based on appropriate education, training, skills, and experience. The skills required are determined and regularly reviewed together with an assessment of existing skill levels within [Company Name]. If necessary, training needs are identified and maintained.

## Security awareness

[Company Name] personnel accept the Acceptable Use Policy and Code of Conduct during the onboarding process to acknowledge their obligations related to information security. In addition, they also pass the security training during onboarding and repeat it annually. For more details please refer to the Security Awareness Training eligibility page.

Additional important information about [Company Name]ʼs security is communicated to personnel via the companyʼs internal communication channels and meetings.

## Information ownership

Information assets are provided to assist [Company Name] Personnel in facilitating company related business. All information composed, sent, received, and stored on information systems remains, at all times, the property of [Company Name].

At the same time, business unit heads define the criticality of the [Company Name]ʼs information assets in their area of responsibility and implement their proper protection from information security risks with the support of the other teams such as GRC, IT and Engineering.

## Risk management

The risk assessment defines the suitable security measures to protect [Company Name]ʼs information assets from security and fraud risks.

Risk management takes place at several company levels, including:

 Management planning – risks to achieving information security and general companyʼs objectives are assessed and reviewed at the quarterly Board meetings and during the annual and quarterly OKRs planning process.

 Information security risk assessments are conducted by the GRC team annually or upon significant change to the business, IT systems or [Company Name]ʼs products.

 Risk assessment of changes to [Company Name]ʼs products via the change management process is managed by the Engineering team.

 As part of major projects to achieve business change, e.g., new information systems and business processes, respective business unit heads are responsible.

## Incident management

Engineering and IT teams constantly monitor the security of the production and corporate IT environments to prevent security incidents. The company has a management process to respond to information security events proactively.

## Other security processes

Access to the resources is denied by default, aligned with the concept of least privilege, and dictated by business requirements.

[Company Name]ʼs IT infrastructure is configured in a way that ensures its continuity in case of disaster via usage of Google Cloud services and periodic data backups. More details are provided in the Disaster Recovery Plan.

# Compliance with the policy

[Company Name] Personnel are responsible to understand and comply with the policies, procedures, and controls established by [Company Name] for their respective business units. Failure to comply with them may subject the individual to disciplinary action, up to and including termination of employment.

# Communication about security

The Legal and GRC teams are responsible for determining the need for internal and external communications relevant to the [Company Name]ʼs security. The Marketing team helps with writing the right messages externally. Other security documents may define specific requirements for communication about security.

**Revision history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Approved by** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |