Document ID: E3	Document name: Information Security Policy
Version: 0.5	Owner: CEO
Date: 01-01-2023	Classification: Public

LOGO

COMPANY NAME

Information Security Policy

[ORGANIZATION]
Version: 0.5
Approved by management: NOT YET APPROVED

1 Context and goals

[ORGANIZATION DESCRIPTION]

This policy document describes the information security management system (or ISMS) that our company uses. Anyone in our company (or at key positions at suppliers) that is handling confidential or sensitive data should be aware of this policy and act in accordance with it. Also, if anyone observes something in our company that is not in line with this policy, he or she should report this immediately. This can be done either by informing our information security officer, or to any member of the security team. The entire management team of our company has been involved in creating this policy and is fully committed to making sure we are compliant.

2 Scope

The scope of the [ORGANIZATION] ISMS is:

> Information security related to ... [e.g. development and delivery of a platform for XYZ]

Within this scope, we provide the following main activities and provides the following services to customers:

- A
- B
- C

The following departments are in scope of this policy

- A
- B
- C

- D

At this point in time, no departments or business activities have been specifically declared out of scope of this policy. Our company has the following office locations and working locations that are in scope of this policy:

- Main office: [ADDRESS]
- B
- C

[ORGANIZATION] does/does not directly manage any data centres. Amazon Web Services/Azure/Google Cloud/IBM is used as provider of IT infrastructure.

3 Stakeholder analysis

The management team is responsible for maintaining regular contact with stakeholders, understanding the information security requirements and expectations from stakeholders and making sure that the ISMS is aligned with the stakeholder requirements and expectations. The resulting information is documented in the stakeholder analysis, which will be updated annually. The stakeholder analysis will cover at least:

- Customers
- Users
- Regulatory requirements such as GDPR

The most recent stakeholder analysis can be found in the Register stakeholders and communication.

4 Leadership

The entire management is aware of the information security policy and is committed to support this effort on an ongoing basis. [MGMT_REP] is the management representative that interfaces directly with the security team.
There is an information security team that is responsible for implementing and maintaining information security.

All other staff of the company is regularly updated by the information security team and is responsible for following policies and guidelines.

5 Resources, awareness and training

Management is responsible for making sure employees executing information security tasks are knowledgeable on the subjects they work on.
They receive security awareness training after onboarding, and after that again at least once a year. Staff involved in product design and development or staff with additional security responsibilities will receive additional training suitable to their role.

6 Operations

[ORGANIZATION] has a register of goals, [LINK DOCUMENT]. These goals are established by top management, and reviewed on an annual basis. When establishing these goals, top management makes sure to include the organizational context and stakeholder requirements.

7 Performance evaluation

The management team will review that effectiveness of the ISMS annually in a management review. If needed, external support will be sought by external partners, such as additional technical advice, independent security testing, or audits by independent parties.

8 Continuous improvement

The management is committed to contiuously improving the information security management system.