Maze Feedback AS

Maze Security Policy

Top Level Information Security Policy

3.6

15.11.2018

Top Level Information Security Policy for Maze Feedback AS

About this document

This is the top-level information security policy which defines the overall goals and framework for information security in Maze Feedback AS, and the subsidiaries under its control (hereafter called Maze).

Goal

The goal of information security in Maze is to protect its information assets and to minimize security risks in a cost-efficient manner, by preventing and reducing their potential impact from internal, external, deliberate and accidental threats.

Information security is a business enabler and provides competitive advantage that allows us to enter and maintain markets and situations that would otherwise be too risky or not accessible. By minimizing net losses resulting from information security breaches, it supports our financial bottom line. It also enhances our corporate image as a trustworthy, open, honest and ethical organization.

Scope

This policy applies to the information assets (such as the Maze-application, customer setup and information, processes and services (development, setup, operations and support), all employees, locations, networks and IT-infrastructure (Data Center Remote Access, employee equipment, source code/database) of Maze, as further described in the ISMS.

Information security principles

Information security practices in Maze is guided by the following principles:

- **Confidentiality** of information (*e.g.* preventing unauthorized access and disclosure of sensitive corporate or personal information)
- **Integrity** of information will be maintained (*e.g.* ensuring that human errors or programming bugs do not reduce the completeness or accuracy of our data)
- **Availability** of information assets and related services will be maintained (*e.g.* minimizing unplanned system downtime and consequently interruption of critical business processes, and ensure business continuity/Disaster Recovery).
- **Privacy** of information will be maintained.
- **Legislative and regulatory requirements** will be met (Norwegian Law (such as The Norwegian Privacy Act), GDPR (EU)) and we will conform to suitable standards (such as ISO 27001).
- **Continuous improvement of information security** is part of our business culture and processes.
- **Training** for human assets within scope will be available.
- **Actual or suspected information security breaches** will be reported to the Information Security Team and will be thoroughly investigated.
- **Sub-policies policies, procedures and guidelines** exist to support this policy, including virus/malware control measures, password routines, and IT technical security measures.
- **We invest** wisely in proven information security controls where justified based on lifecycle cost/benefit assessment and risk analysis.
- **The Information Security Team** is responsible for maintaining the ISMS and is an internal center of excellence providing leadership, guidance and support on all matters relating to information security.

- **All managers** are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.
- **Compliance** with the Information Security Policy is mandatory. **In other words, information security is everyone's responsibility.**

Monitoring and reviewing

The Information Security Team will regularly measure and review the effectiveness of our information security efforts, and report back to management on significant findings.

Approved

Policy approved by Senior Management on November 15, 2018.
Signed: Frode Berg, CEO