

# Maze Feedback AS

# Maze Security Policy

Top Level Information Security Policy

3.8

28.09.2020

## Top Level Information Security Policy for Maze Feedback AS

### About this document

This top-level security policy 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 our information assets and optimize security risks in a cost-efficient manner, by preventing and reducing the potential impact from internal, external, deliberate and accidental threats.

At the forefront of our security measures is the development and operation of the Maze application and the handling of our customers data.

Information security is a business enabler and provides competitive advantage that allows us to attract customers in the global markets. 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

The information security policy and sub-policies applies to all Maze information assets. This includes but is not limited to any handling or combination of personal data, such as the collection, registering, organizing, structuring, storing, handling, or changing, reporting, reading, using, transferring by sending or other transfer, spreading, adjusting, bundling, limiting, deleting or destruction, independent of the processing is automated or not. The policies applies to all persons in Maze (such as managers, permanent employees, and part-time consultants) independent of their physical location.

### Information security principles

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

- **Confidentiality** of information shall be assured (e.g. preventing unauthorized access and disclosure of confidential and/or 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 upheld through privacy by design.
- **Legislative and regulatory requirements** will be met (Norwegian Law (such as The Norwegian Privacy Act), GDPR (EU), HIPPA (US)). We will keep our ISO/IEC 27001 certificate up to date.
- **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 investigated and concluded.
- **Sub-policies policies, procedures and guidelines** exist to support this policy.
- **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.**

#### **Assurance, monitoring and reviewing**

The Information Security Team will regularly measure and review the effectiveness of our Information Security Management System, and report back to management on significant findings and propose improvements. Maze will conduct internal audit carried out by external advisor as well as external audits of ISO/IEC 27001 certificate (London 2019-12-02, Certificate No: 10000208447-MSC-UKAS-NOR).

#### **Approved**

Policy approved by Senior Management on 28th of September, 2020.

Signed: Frode Berg, CEO