Information Security Policy

1. Background and purpose:
Managing information is the basis of Evira's operations. It's essential that information is handled correctly for internal confidence as well as for external customers and partners. The purpose of this policy is to demonstrate our commitment to managing information securely.

Information security can be summarised in the following four areas of requirements:

- Availability: that information is accessible when needed by authorised users
- Accuracy: that information is protected from incorrect changes or removal
- Confidentiality: that information only is accessible to authorised users
- Traceability: that access and changes to confidential information is traceable

With the establishment of this policy, the company commits to adhere to applicable requirements regarding information security and responsibilities.

2. Scope:
This policy applies to all information handled by the company, regardless of format, including but not limited to, electronic, printed, and verbal information. The policy applies to all employees, consultants, suppliers and any other parties who handle information.

3. Guidelines and principles:
Evira commits:

- to continuously work on knowledge development about how to establish and ensure information security with the operation,
- to seek help from external experts when needed,
- to treat information as sensitive unless otherwise stated,
- to continuously evaluate and assess threats and risks,
- to work preventively against threats and risks to avoid undesired effects,
- to incorporate information security as a natural and integral part of the company's routines, and
- to regularly revise and update management systems, security measures, and crisis management plans.

4. Responsibility:
The responsibility for maintaining the company's work with information security should follow the company's normal structures. Employees have an individual responsibility to highlight potential shortcomings or risks that are discovered.

Any deviations or exceptions made from this policy or other information security routines should be reported to the nearest manager and then reported to the

management team. Serious violations are reported to the appropriate protection body or authority.

5. Monitoring and revision:
This policy and other information security routines should be reviewed and updated annually, or if significant changes occur within the company or in the world. The review aims to ensure the policy's relevance and accuracy, as well as to ensure there is ongoing awareness of the policy and other routines within the organisation.

6. Validity of the Information Security Policy:
The policy was revised by the company's management team and owners on 2023-08-31 and is valid until 2026-02-28.