INFORMATION SECURITY POLICY

DOCUMENT CLASSIFICATION	Public
DOCUMENT TYPE	Policy
VERSION	1.5
DATE	15 August 2025
DOCUMENT AUTHOR	Christoffer Sundby, CEO
DOCUMENT OWNER	Christoffer Sundby, CEO

1. Purpose

We protect the information entrusted to us to safeguard our employees, partners, customers, reputation and finances. We aim to:

- Comply with legal, regulatory, and contractual requirements.
- Ensure the right people have the right access to the right information at the right time.
- Protect personal data in accordance with GDPR.
- Act as responsible stewards of data.

2. Scope

This policy applies to all employees and third parties who access Spenn systems or information.

3. Principles

Our information security approach is based on risk management, compliance with laws and regulations, and business needs. We follow ISO/IEC 27001 and related standards.

4. Our Commitment

- Maintain confidentiality, integrity and availability of information.
- Align security efforts with Spenn's business objectives and stakeholder requirements.
- Achieve and maintain ISO/IEC 27001 certification and other relevant accreditations.

5. Security Objectives

- Identify, assess, and manage security risks on an ongoing basis.
- Continuously improve processes and controls in response to experience, incidents and changes in the threat landscape.
- Ensure all employees understand and follow our security procedures

6. Roles and Responsibilities

- Chief Technology Officer (CTO): Leads security efforts and approves exceptions to this policy.
- Information Security Forum: Oversees the risk treatment plan, evaluates controls, and conducts reviews.
- All employees and third parties: Must comply with this policy and complete required training.

7. Training and Awareness

We provide regular training and awareness activities and make this policy readily accessible to employees and relevant third parties.

8. Compliance and Review

Compliance is monitored through internal and external audits. Breaches of this policy may result in disciplinary action. The policy is reviewed at least annually and updated when necessary.

9. Definitions

- Confidentiality: Only authorized individuals can access information.
- Integrity: Information is accurate, complete, and protected from unauthorized modification.
- Availability: Information is accessible to authorized users when needed.