ISMS / STJÓRNKERFI UPPLÝSINGAÖRYGGIS

Information Security Policy

Published 8/9/2025

Objective

Fuglar have implemented an Information Security Management System (ISMS). The objective of the ISMS is to ensure the business continuity of Fuglar and to minimize the risk of damage by preventing security incidents and reducing their potential impact.

Scope of the Information Security Management System (ISMS)

The scope of the ISMS applies to the following facets of Fuglar operations as well as the management of information and business activities supporting them:

- Software development, including coding, testing, version control and deployment
- Daily operations and customer service, including data handling, communication systems, and user support

The ISMS encompasses the physical and digital infrastructure, personnel, and supporting technology directly involved in these activities.

Policy

The policy's goal is to protect Fuglar's informational assets against all internal, external, deliberate, or accidental threats. The security policy ensures that:

- **Confidentiality** of information will be assured.
- **Integrity** of information will be maintained.
- **Availability** of information for business processes will be maintained.
- **Legislative and regulatory** requirements will be met.
- **Business continuity plans** will be developed, maintained, and tested.

- **Information security training** will be available for all employees.
- **All actual or suspected information security breaches** will be reported to the Chief Technology Officer and will be thoroughly investigated.
- Commitment to **continual improvement** of the information security management system.

Procedures exist to support the policy, including virus control measures, passwords, and continuity plans. Business requirements for the availability of information and systems will be met. The Chief Technology Officer is responsible for maintaining the policy and providing support and advice during its implementation. All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective departments.

This policy will be reviewed and updated yearly and approved by the board. Compliance with the Information Security Policy is mandatory.

This policy is communicated to all employees and contractors via the ISMS portal and during onboarding activities.

This policy is made available to employees, contractors, and relevant external parties upon request.