FOSSID

FossID Information Security Policy

1. Purpose

The purpose of this Information Security Policy is to define FossID's commitment to protecting its information assets, intellectual property, and the information assets of its customers and partners. This policy outlines the framework for establishing, implementing, maintaining, and continually improving our Information Security Management System (ISMS).

2. Scope

This policy encompasses all information assets, processes, and systems that are owned, managed, or used by FossID. It applies to all employees, contractors, consultants, temporary staff, and other workers at FossID, including all personnel affiliated with third parties.

3. Information Security Framework

FossID ensures information security through the following activities:

- **Information Classification**: Information is classified based on its sensitivity and criticality to ensure appropriate protection levels are applied.
- **Access Control:** Access to information systems and data is managed through defined procedures that ensure that only authorized personnel have access, based on their roles and responsibilities.
- **Risk Management Process:** A risk management process is in place to identify, assess, and mitigate information security risks.
- **Defined Responsibilities, Authorities, and Roles:** Roles and responsibilities are clearly defined within the organization. This includes specifying the duties of staff at all levels to ensure accountability and effective security management.
- **Incident Management Process:** A robust incident management process is established to detect, report, and respond to information security incidents promptly.
- **Business Continuity Management:** Business continuity plans and procedures are developed and maintained to ensure the availability of critical business functions during disruptions.
- **Information Security Objectives:** Clear information security objectives are established and reviewed regularly.

All staff members are responsible for maintaining awareness of this policy and applying its principles in their daily duties. Non-compliance with information security requirements can lead to disciplinary actions, labor law measures, and civil or criminal proceedings.

4. Information Security Objectives

The framework for setting information security objectives is defined in FossID's Information Security Management System (ISMS) and is based on the following principles:

- Protecting of FossID's information assets and intellectual property
- Protecting of customers' and partners' information assets against misuse, data leakage and destruction
- Maintaining the confidentiality, integrity, and availability of data according to established targets
- Strengthening systems and processes by considering actual the context and all identified risks

5. Management Commitment

FossID's management is committed to ensuring compliance with applicable requirements related to information security and continually improving the ISMS. This commitment is demonstrated through regular reviews, resource allocation, and strategic decision-making aimed at enhancing information security.

6. Communicating the Information Security Policy

The management team is responsible for communicating the Information Security Policy to all individuals working for or on behalf of the organization. The policy is made available to the public by publishing it on FossID's website and distributing it to interested parties upon request through appropriate channels.

DocuSigned by:
Stuart Dross
C65B8A6F659D4D2...

Stuart Dross, CEO