SECURITY POLICY

Introduction

The Information Security Policy defines the fundamental objectives and principles for managing information security at **Terraverse, s.r.o.**

Objectives, Scope, and Principles

The primary objective of information security management is to ensure the protection of Terraverse, s.r.o.'s key information assets, which are essential tools for implementing the company's strategy.

Information assets include all information required for the company's operations and all resources necessary for acquiring, processing, storing, using, and protecting such information. These assets comprise, in particular, data, information, software, hardware, end-user devices (computers, laptops, printers, etc.), infrastructure (Infrastructure as a Service-IAAS, networks, network devices, etc.), personnel (both internal and external staff handling information assets), and suppliers (software developers, testers, etc.). Information assets also include information processed in non-electronic form, such as printed documents and records.

The principle of ensuring information security involves identifying critical information assets, assessing all aspects that may pose a risk to them, and implementing adequate measures to ensure their required availability, confidentiality, integrity, and authenticity.

Target Groups

The company's framework for managing information security encompasses all stakeholders, including internal and external employees, suppliers, and customers. Anyone who comes into contact with the company's information assets must be familiar with this policy and, as necessary, be informed of the specific requirements, rules, and procedures for handling them as defined in the company's internal governance documentation.

TERRAVERSE, s.r.o.
ID 19610076 VAT ID CZ19610076
IDDS: dtqz9fw

Na Příkopě 583/15, Staré Město
110 00 Prague, Czech Republic

sales@terraverse.info
www.terraverse.info

TERRAVERSE

Principles of Information Security Management

All key aspects of information security are documented in the company's internal governance documentation. The company's management regularly reviews, updates, and approves these documents, forming a unified set of guidelines.

Responsibility for information security management at the highest level lies with the security manager, who is accountable for ensuring compliance with security policies and procedures.

Core Principles Governed by the Information Security Management System are as follows:

1. The company adopts and enforces all necessary measures to ensure information security, following best practice guidelines and, in particular, in accordance with the requirements of ISO/IEC 27001:2022 and ČSN ISO/IEC 27001:2023 Information Technology—Security Techniques— Information Security Management Systems.
2. The company's top management has committed to providing adequate resources for the implementation and operation of required information security measures.
3. The company's information assets are identified and assessed through risk analysis, taking into account potential impacts on the company in the event of breaches in availability, reliability, authenticity, or confidentiality.
4. Information is classified and labeled according to its level of confidentiality.
5. The use of information assets is always managed in accordance with their classification, including access control.
6. Access to informational assets is granted strictly based on the purpose for which they are used. When this purpose no longer exists, access must be revoked.
7. Physical security measures provide a solid foundation for protecting information assets.
8. End users of information assets are trained on prescribed procedures and rules related to their use.
9. Suppliers and customers are informed of the information security procedures necessary to ensure the security of information assets involved in supplier-customer relationships with Terraverse s.r.o., including the protection of customer information used by Terraverse s.r.o. in delivering products and services. Key information security aspects within supplier-customer relationships are contractually regulated.
10. Any information security breach, or even suspected breach, must be reported immediately by all stakeholders to the Security Manager, who will ensure it is reviewed and documented.

In Prague, on August 26, 2025

Daniel Szantai

CEO

TERRAVERSE, s.r.o.
ID 19610076 VAT ID CZ19610076
IDDS: dtqz9fw

Na Příkopě 583/15, Staré Město
110 00 Prague, Czech Republic

sales@terraverse.info
www.terraverse.info