INFORMATION SECURITY POLICY

PURPOSE

The purpose of information security in Techstep is to ensure the confidentiality, integrity, and availability of information belonging to the company, as well as any information we process or store on behalf of our customers, partners, suppliers, or any other third party. Information security is a core part of reaching Techstep's vision and goals. Success in our business depends on building and maintaining trust and confidence with employees, shareholders, customers, suppliers, partners, and other stakeholders.

SCOPE

This policy applies to all systems, people, and processes that constitute the organization's information systems, including board members, directors, employees, suppliers, and other third parties who have access to Techstep systems. Techstep's executive management team has the responsibility for integrating the principles into day-to-day operations.

OUR APPROACH

A regular cycle will be used for setting objectives for information security. These objectives will be based on a clear understanding of business requirements, informed by the management review process, during which the views of relevant interested parties may be obtained.

Information security objectives will be documented for an agreed time period, together with details of how they will be achieved. These will be evaluated and monitored as part of management reviews to ensure that they remain valid.

Techstep's information security management is built on the ISO/IEC 27001 framework. In accordance with ISO/IEC 27001, the reference controls detailed in Annex A of the standard will be adopted where appropriate by Techstep. These will be reviewed on a regular basis considering the outcomes from risk assessments and in line with information security risk treatment plans. For details of which Annex A controls have been implemented and which have been excluded, please see the Statement of Applicability.

Additional frameworks may be used in cases where these objectives and controls are not sufficient to reduce risks to an acceptable level. The threat landscape shall be continuously evaluated, incorporating threat intelligence sources and external cybersecurity reports to stay ahead of emerging risks.

ROLES AND RESPONSIBILITIES

The ownership and responsibility for Techstep's information security, including risk management and privacy, lies with the company's CEO. The operational responsibility has been delegated to the Chief Information Security Officer (CISO), who is responsible for maintaining, communicating, and ensuring that information security and privacy objectives are met.

Other roles and responsibilities are further described in the Techstep Management System.

OUR COMMITMENTS

Techstep is committed to complying with all relevant laws and legislation, as well as contracts, industry standards, and service-level agreements.

Information Security Objectives

The overall goals for information security at Techstep are:

- Safeguard assets that are managed by Techstep.
- Ensure our ability to maintain critical business operations and services.
- Protect the confidentiality, integrity, and availability of information that Techstep administers against illegal acts, accidents, and mishaps.
- Ensure that information security measures support Techstep in maintaining high trust with customers and stakeholders.
- Ensure compliance with applicable laws, regulations, and policies.
- Ensure that privacy and data classification are protected and properly managed.
- Continually improve the effectiveness of Techstep's management system and information security controls, incorporating ideas for improvements from any source.
- Achieve ISO/IEC 27001 certification and maintain it on an ongoing basis.

General Principles

- Risks are identified through risk and vulnerability analyses.
- The threat landscape shall be continuously evaluated, integrating external threat intelligence sources.
- The information security measures must always be proportionate to the acceptable level of risk.
- When incidents occur, emergency measures shall be activated to limit damage and allow for a rapid return to normal operations.
- Information security should be an integral part of all project planning and management.
- A good security culture is built upon correct attitudes among employees.
- The executive management team is responsible for ensuring that all employees receive mandatory security awareness training at least annually.
- Access to confidential information and assets must be protected, ensuring compliance with statutory and contractual confidentiality requirements.
- All information security incidents must be reported internally and, where required by law, to the appropriate authorities. This will be followed by improvements and lessons learned.
- A data classification policy will be implemented to ensure proper handling of public, internal, and confidential data.

Techstep defines policies across a wide variety of information security-related areas that accompany this overarching Information Security Policy. Each of these policies is communicated to the appropriate audience both within and external to the organization.

Third-Party Risk Management

Techstep is committed to ensuring that suppliers and third parties adhere to strict security requirements. This includes conducting vendor security assessments, audits, and contractual obligations to maintain high standards of information security.

UPDATES

This policy shall be reviewed and updated annually or when deemed necessary due to changes in the threat landscape, regulatory environment, or business operations.

Revision History

Version	Change Date	Author	Description of Changes	Approved By	Approval Date
1.0	2021-05-18	Head of IT	Initial release	CEO	2021-05-18
1.1	2022-01-14	Head of IT	Added revision control, clarified objectives	CEO	2022-01-14
2.0	2022-08-29	CISO	Document format changed	CEO	2022-08-29
3.0	2023-11-06	CISO	ISO/IEC27001:2022 alignment	CEO	2023-11-06
3.1	2023-12-13	CISO	Changed document layout and overall content	CEO	2024-01-16
3.2	2025-01-16	CISO	Clarified objectives	CEO	2025-01-28