INFORMATION SECURITY POLICY

PURPOSE

The purpose of information security in Techstep is to safeguard information assets belonging to the company, and equally, any information we process or store on behalf of our customers, partners, or suppliers. 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 employees and representatives of Techstep ASA and its subsidiaries. Techstep's executive management team has the responsibility for integrating the principles into day-to-day operations.

OUR APPROACH

Our information security objectives, procedures and activities are defined in our Techstep Management System, which shall ensure the confidentiality, integrity and availability of our own information as well as our customers' and partners' information.

All security initiatives shall be based on risk assessments and integrated into an enterprise security architecture that provides and maintains measurable, cost-effective, and appropriate security. This will ensure that appropriate technical and organisational information security controls are established.

Techstep's information security management is built on the ISO/IEC 27000 framework and described in the Techstep Management System. Additional frameworks may be used in cases where these objectives and controls are not sufficient to reduce risks to an acceptable level.

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 the security and privacy objectives are met.

Other roles and responsibilities are described in the document *Governing Roles and Responsibilities*.

OUR COMMITMENTS

Techstep is committed to complying with all relevant laws and legislations, 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 solve priority tasks and services
- ensure the integrity and confidentiality of information that Techstep administers against illegal acts, accidents and mishaps
- ensure that safety will make Techstep maintaining a high confidence of its customers and all other relationships
- ensuring compliance with applicable laws, regulations and policies
- ensure that privacy is protected

General principles

- Risks are identified through risk and vulnerability analyses
- The threat landscape shall be continuously evaluated, and new threats shall be risk assessed
- The security measures must always be proportionate to the acceptable level of risk
- When incidents occur, emergency measures shall be activated to limit the damage and making it possible to quickly return to normal operation
- Security should be an integral part of all project planning and management
- Good security culture is built upon correct attitudes among employees
- The executive management team is responsible for ensuring that all employees should have the necessary training to fulfil their security responsibilities
- Access to confidential information and assets must be protected so that the statutory and contractual confidentiality requirements are met
- All security incidents must be reported internally and to the authorities whenever required by law, followed by improvement and learning

UPDATES

The Information Security Policy shall be reviewed and updated annually or when considered necessary i.e., due to changes in the threat landscape.

Version number	Approved by	Approval date	Document owner	Change history
1.0	Jens Haviken, CEO	18.05.2021	Head of IT	Document created
1.1	Børge Astrup, CEO	14.10.2021	Head of IT	Change of format and approved by new CEO

1.2	Børge Astrup, CEO	29.08.2022	CISO	Complete review and update of the entire document to align with ISO/IEC 27001. Updated roles and responsibilities.