Security Policy

Company:	Nordnet Bank AB, Nordnet AB (publ)
Approved by:	Board of Directors
Date of approval:	2025-01-20 (replaces 2023-11-23)
Document owner:	Head of Security
Revised:	Annually or more often if required
Confidentiality class:	Open

1 Introduction

1.1 Background

This Security Policy has been established for Nordnet Bank AB and Nordnet AB (publ) ("Nordnet").

1.2 Purpose and objective

The purpose of this policy is to establish guidance and general principles for security at Nordnet, as well as to establish the Board's direction with regards to security objectives. If any other guiding security documents are in conflict with this policy, the Security Policy shall have precedence.

The overall objective with Nordnet's security is to enable business strategy, through realization of the following strategic security objectives:

- Customers' perception of their online security when interacting with Nordnet is of the highest security standard (Engaged customer).
- Innovation and significant revenue streams are identified and protected with trust by design and adequate resources (Profitable growth).
- Regulatory compliance and risk management practices are fully implemented, and requirements met on all Nordnet's operating markets (Strong governance).
- Embracing simplicity for the dispersion of security, in order to contribute to a good understanding, encourage ownership and promote inclusion (Engaged employees).

In order to achieve the strategical objectives above, Nordnet shall:

- Enable the right conditions for business strategies to be realized by being forward leaning and continuously improving security management (Passion).
- Maintain and strengthen the security level with easy-to-use methods and straight to the point measures to protect Nordnet and customers (Simplicity).
- Openly communicate and strive to include all employees to iteratively improve security (Transparency).

1.3 Regulatory basis

This policy has been established in accordance with following regulations:

- Digital Operational Resilience Act (EU) 2022/2554 (DORA)
- The General Data Protection Regulation (EU) 2016/679 (GDPR)
- Lag (2004:297) om bank- och finansieringsrörelse (the Swedish Banking and Financing Act)
- Finansinspektionen's Regulations and General Guidelines (FFFS 2014:4) regarding the management of operational risks
- EBA Guidelines on ICT and security risk management EBA/GL/2019/04

2 Definitions

Security – Security in the Nordnet context concerns the safeguarding of Nordnet's company assets. Company assets include the people, facilities, equipment, information, IT systems and other assets necessary for conducting its business.

Information security – Information security means the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide:

a) *Confidentiality*, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
b) *Integrity*, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; and
c) *Availability*, which means ensuring timely and reliable access to and use of information.

Cyber security – Cybersecurity is defined as the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, to strengthen the confidentiality, integrity and availability of these systems.

3 Guiding principles

The following are Nordnet's fundamental guiding security principles:

1) The Board of Directors shall decide on the strategic security objectives, the security risk appetite and ensure that the organization has the necessary means to achieve the security objectives.

2) The CEO shall approve annual security initiatives and participates actively in the Security Committee where status of ongoing security activities and quarterly reviews are reported, in order to identify where supportive measures are needed.

3) A Head of Security shall be appointed at all times to ensure that Nordnet protects its staff, has a secure platform, and maintains customer trust.

4) The Risk Owners shall be responsible for managing their security risks with support from Nordnet's security organization.

5) Nordnet shall adopt and implement a tailored security management system, built on proven standards, that enables a systematic approach to security.

6) Head of Security shall conduct a yearly review of Nordnet's security management system and present the result to the Security Committee and to the Board of Directors.

7) Security shall be integrated throughout the organization via underlying CEO approved instructions with clear allocation of responsibilities as well as underlying security guidelines.

8) Nordnet shall determine the value of information assets in relation to assessed risks in order to implement proportional measures.

9) A risk assessment, analysis of incident reports and security related compliance gaps shall be the basis of risk management decisions. The risk management process shall be based on the same principles as operational risk management within Nordnet and the risk-based approach means that Nordnet assess risks in order to reduce or eliminate uncertainty.

10) Security shall be considered in all parts of the organization and phases of projects, such as, but not limited to:
    a) a strong security and risk awareness culture where all personnel are responsible for following prescribed security measures,
    b) systematic evaluations and controls of security measures and risks,
    c) procedures for the regular testing, assessment and evaluation of the effectiveness of the security measures are in place,
    d) evaluation of security aspects in the New Product Approval Process (NPAP),
    e) ensure regulatory compliance throughout the supply chain.

4 Communication and trainings

The Head of Security shall provide a training program to ensure awareness regarding security among employees at all levels and long-term inhouse consultants. The training program may vary from year to year but shall always include a security introduction training for all new employees and continuous security awareness training for all employees.