Security Policy
for the SEB Group

derived from the Rules of Procedure for the Board of Directors

adopted by the Board of Directors of
Skandinaviska Enskilda Banken AB (publ)
on 22 October 2025

Group Security & Cyber Defence

Security Policy

1. Introduction

Security is a vital part of Skandinaviska Enskilda Banken AB (SEB) and the SEB Group's business. Maintaining a high level of security is important to SEB and expected by customers, shareholders and regulators. Security inherent in products and services, and the reliability of them, are prerequisites for retaining and attracting customers.

Security is important for several reasons:

- Security keeps our employees and customers safe
- Security protects our assets, data and systems
- Security enables trust and keeps SEB compliant to regulatory requirements

Financial services are of great importance to society and SEB is expected to contribute to the operational resilience, performance and stability of the financial system, wherever SEB is present, by assuring confidentiality, integrity and availability in its business processes.

2. Purpose

The purpose of this Policy is to define overall principles and objectives for security within the SEB Group. This will contribute to improve SEB's security posture over time.

3. Scope

This Policy applies to the SEB Group and shall be implemented in all parts of the Group taking local rules into account where relevant.
Security in SEB covers information security (including cyber, physical, personnel and IT Security).

4. Security objectives

The objective of security work in SEB is to:

- protect the customers and the assets, including people, information, infrastructure, finances, and reputation, against potential threats;
- associate the SEB brand with robust security; and
- support SEB's business goals by enabling trusted, regulatory compliant and resilient financial solutions globally.

5. Overall security principles

The following overall security principles lay the foundation for security in SEB. Supporting instructions and guidelines shall be based on the principles in this Policy.

5.1 Security is a business enabler

Security shall be seen as a business enabler as it attracts and retains customers and builds trust in the financial market by ensuring compliance, privacy, quality of data and resilience of our business.

5.2 *Security by design and default*
Security shall be implemented by design and by default. This means that everything we create shall be created with security in mind from the very first onset.

5.3 *Security in line with best practice*
Security shall be in line with best practice, international standards and in accordance with local laws and regulations. If local law requirements are lower than SEB Group requirements the Group level requirements take precedence.

5.4 *A management system shall be established and maintained*
A management system for managing security shall be implemented and used to minimise security risks and to ensure a structured and methodical way of implementing, maintaining and continually improving security within SEB. There shall be sufficient resources available for establishing and maintaining the management system ensuring effective and regulatory compliant information security management.

5.5 *Identify SEB assets and understand the level of protection needed*
The level of protection needed for SEB assets, including people, information, Information and Communication Technology (ICT), infrastructure, finances, and reputation, shall always be identified, understood and implemented.

5.6 *Use a risk-based approach*
Security risks shall be identified, measured, assessed, monitored, managed, mitigated and reported. When managing security risks, security measures shall be prioritized and allocated using a risk-based approach. This means that risks shall be identified, analysed and understood so that the most effective measures are chosen to mitigate risk. This is contrary to the "one size fits all" approach where security is applied indiscriminately.

5.7 *Apply a holistic and global view on security*
A holistic and global view shall be applied to security work in the SEB Group as security in its nature is not an isolated circumstance.

5.8 *A sound company culture enables security*
Security awareness, mindset, and behaviour (culture) shall be a natural part of SEB's company culture to ensure a sustainable security culture improving the overall security over time.

6. Security Governance Model

6.1 The Board of Directors (the "Board") of SEB is responsible for the management of the affairs of SEB and the SEB Group. The Board shall ensure that SEB and the SEB Group are organised in such a way that it has an appropriate and transparent governance structure with a clear division of functions and responsibilities that ensures an efficient and sound steering of SEB and the SEB Group. The Board fulfils

these responsibilities among other things through the adoption of this Security Policy for the SEB Group, which outlines the overall principles and objectives for security within the SEB Group.

6.2 The President and Chief Executive Officer (“President") is responsible for the day-to-day management of the activities of SEB in accordance with the directives set by the Board, and the execution of the security management within the SEB Group. The President fulfils these responsibilities among other things through the adoption of the Security Governance Instruction for the SEB Group, which describes the governance model and management of the security work in the SEB Group.

6.3 The Chief Security Officer (“CSO”) is appointed by and reports to the Chief Operating Officer and Deputy President (“COO and Deputy President”), after consultation with the President and the Chief Risk Officer (“CRO”). The CSO is responsible for establishing and overseeing the implementation, adoption and effectiveness of the SEB Information Security Management System including security strategy, controls and internal rules for security. The CSO is also Head of Group Security & Cyber Defence.

6.4 The activities of the security work are further governed by the Security Governance Instruction for the SEB Group.