Group Policy

Group Information Security Policy

Organization	Group IT
Date	February 21, 2024
Document owner	Jörgen Hellberg, CIO (Chief Information Officer)
Document manager	Erkan Kahraman, CISO
Information category	Internal

Table of contents

1 Introduction

PostNord relies on its information as a critical asset; and its unavailability or incorrectness could disrupt business operations and affect its brand. Ensuring information's **confidentiality, integrity and availability** is therefore vital to ensuring delivery of a high-quality service.

2 Purpose

This governance document, at the highest level, sets out PostNord's approach to managing information security and defines **the security strategy, principles, and goals** for the PostNord group of companies.

This policy is supported by topic-specific instructions as needed, to further mandate the implementation of information security controls.

3 PostNord's Principle of Protection

Cybersecurity is a crucial aspect of any organization, and it encompasses three main components: *confidentiality*, *integrity*, and *availability*.

At PostNord, our guiding principle is to prioritize **availability** first, followed by integrity, and then confidentiality. This is because our primary responsibility to society is to ensure the continuous delivery of post. By prioritizing availability, we ensure that our services remain accessible and reliable, while also maintaining the integrity and confidentiality of the information we handle.

4 Strategic Priorities

PostNord's goal is to ensure that information assets are properly secured in relation to applicable laws and regulations, business requirements and the risk position taken for the current environment.

PostNord's information security policies are built on the following guiding principles: to **protect** the business, **enable** the business, and **earn trust**. PostNord information security strategy and tenets are defined to realize the security vision and assist in decision making;

Protect the business.

- Implement a risk-based approach. We implement functional security controls driven by a value-chain risk assessment of the business.
- Keep a holistic security view. We know that technology alone is not enough to protect the organization and we include the people and process elements in the center of our security strategy.
- Make security everyone's responsibility. Maintaining an effective and efficient security posture for PostNord requires a proactive stance on security issues from everyone. Increased awareness and participation are key for our success.

Enable the business.

- Support the digital transformation. Embed security into the development and acquisition cycle of products, software and IT-services.
- Make security seamless. Implement user friendly-security controls and improve communication. Security shall be seen as a business enabler rather than a blocker.
- Manage scale with automation. Build guardrails and automated security controls that are preventive and can scale.

Earn trust.

- Build a security culture. We understand the importance of building a security culture by being empathetical and approachable.
- Be transparent. We shall be open and honest about our security weaknesses and risks to relevant stakeholders.
- Gain recognition. Implement industry-standard information security governance model and being eligible for independent verification.

5 Roles and Responsibilities

PostNord has a strong security culture promoting individual integrity and security awareness and values incident prevention and management, both with respect to services and the personal data processed within them. At PostNord, liability for information and IT security is an extension of operational responsibility, both for management and employees. This means that all employees have a security responsibility in parity with their operational responsibility.

- PostNord's *Group Leadership Team* is ultimately responsible for information security.
- *Managers* are responsible for information security within their areas of responsibility. This includes
    - following up their employees' mandatory training and
    - managing their employees' access (on- and off-boarding) to applications.
- *Employees* are individually responsible for the information security needs of their own work.
- *All Users* are individually responsible for:
    - reporting incidents and errors discovered in the IT environment, or suspect behaviour that may affect PostNord’s information assets or the IT environment
    - completing training in security topics, such as avoiding social engineering attacks and how to approach social media
    - reading and understanding the Acceptable Use Instruction, which outlines the acceptable use of computer equipment and associated services at PostNord.

6 Governance Framework

This policy is the foundation of PostNord's information security management system and the supporting governance framework which includes:

- Information Security Instruction
- Acceptable Use Instruction

At a lower level, this policy and the above named instructions are supported by topic-specific guidelines and the control framework managed by the PostNord CISO Office.

7 Document Control

7.1 Reviews and updates

This instruction document is required to be reviewed and if necessary, updated annually by the CISO (Chief Information Security Officer) based on a regular risk assessment.

7.2 Revision History

Version	Date	Author	Change Comment
1.0	2020-10-20	BE	Initial version.
2.0	2022-11-21	JH/EK	Revised version.
2.1	2024-02-21	EK	Annual review and update of security principle.