Information Security Policy

DSB

Telegade 2, DK-2630 Taastrup, CVR no. 25050053

Department responsible: IT Security

Approved by: The Board of Directors **Date**: 14 November 2024

1. Introduction

The Information Security Policy supports DSB's overall purpose: 'A sustainable way forward with room for all of us'.

DSB's social responsibility is to promote mobility that does not have a negative impact on the climate. As a provider of public transport, we have a responsibility to provide a secure journey towards a sustainable operation of a digital, electric fleet, customer-focused solutions and an efficient operation of DSB. Continuous achievement of DSB's objectives requires a significant general digitalisation at DSB. At the same time, the current threat scenario requires a constant focus on cyber and information security.

Adequate levels of cyber and information security help to ensure a stable service for our customers and confidence in a sustainable, public mode of transport. At DSB, we put the customer first when we promote mobility, demonstrate socially responsible behaviour and practise information security in everything we do.

We must ensure that information is reliable and accessible and that it can be restored. We must protect sensitive data, including personal data about customers and employees as well as confidential information about DSB. Data must only be accessible to authorised persons who have a work-related need to access them, and data must be protected against cyber attacks.

The policy is updated once annually and in case of significant changes.

2. Purpose

The purpose of this Information Security Policy is to:

'develop and ensure an adequate level of information security based on weighing up risks and costs and never compromising passenger safety.'

The policy applies to all employees of the DSB Group as well as to external consultants who have access to DSB's systems and information. The policy covers all IT systems used, whether internal, external, administrative or linked to our train operations. The policy covers both information in the physical world (e.g. paper and speech) and information processed digitally.

3. Our ambition and targets

As a supplier of infrastructure critical to society, DSB continuously works to strengthen cyber and information security. We do this by, among other things, complying with applicable legislation in Denmark and the EU and by collaborating with relevant authorities and sector forums on information security. We maintain certification in information security and develop and train our employees, management and culture to ensure that we practise information security in everything we do.

Our objectives for information security are to:

- Maintain a certified information security management system
- Increase employee awareness of information security
- Detect, investigate and prevent threats to information security at DSB
- Detect, register and reduce information security risks
- Manage information security through increased use of technology

These objectives have been approved by the Executive Team and translated into underlying KPIs, which are regularly reported to the Executive Team.

4. This is how we achieve our goals

The Executive Team is ultimately responsible for information security at DSB and has the overall responsibility for ensuring that our information security management system is efficient and continuously developed.

IT security must ensure the framework for the practical implementation of cyber and information security.

DSB managers and employees are responsible for working with information security and for complying with the Information Security Policy and underlying guidelines.

To develop and ensure an adequate level of information security, we work on the basis of the following principles:

- We continuously maintain and improve our information security management system to strengthen cyber and information security. We work according to recognised standards and frameworks.

- We comply with relevant information security requirements, including laws, regulations and contractual obligations.

- We make demands on our suppliers' and subcontractors' information security. We follow up to ensure that services and information security meet our requirements. We can outsource our duties, but not our responsibilities.

- We continuously ensure that management and employees have sufficient understanding of their responsibilities and roles in terms of practising information security and complying with applicable legislation relating to information security.

- We work on the basis of a risk-based approach to information security, where current and expected risks and threats are balanced against business requirements and management expectations.

- We monitor the threat scenario and continuously adapt our actions to ensure that information is reliable, accessible and recoverable. We protect sensitive and confidential information so that it is only accessible to authorised persons.

- We integrate and systematise information security into existing activities, processes and architecture.

4.1. Impacts, risks and opportunities

IT Security works in a structured manner to prevent, detect and mitigate cyber and information security risks and opportunities. The Executive Team will determine an acceptable level of risk. Risks above that level are reported to the Executive Team on an ongoing basis, along with impacts in the form of threats and incidents as well as potential improvements.

DSB's main risks are that the safety of our passengers is affected and that we have to stop train operations. We prioritise measures to prevent and mitigate these risks and take appropriate contingency measures.

5. Organisation, responsibility and approval

The Board of Directors of DSB has overall responsibility for approving the policy. The Board of Directors decides whether DSB should have cyber insurance.

The policy is translated into underlying information security guidelines that define roles and responsibilities for every individual area. The guidelines are approved by the Deputy Director of IT. IT Security must update the Information Security Policy and underlying guidelines and ensure that employees acquaint themselves with these. IT Security assesses whether exemptions from requirements in underlying guidelines may be approved.

Definition of information security

Information security means to preserve the confidentiality, integrity and availability of information by protecting information and information systems from cyber threats, unauthorised access, use, disclosure, disruption, modification or destruction of data.

6. Interaction with other policies and guidelines

- Corporate Social Responsibility Policy
- Compliance Policy
- Data Protection Policy
- Data Governance and Data Ethics Policy
- Code of Conduct for information security – employees of DSB
- Code of Conduct on information security – external consultants etc.
- Information Security Manual