Security – Group policy

Contents

1 Purpose 2

2 Scope 2

3 Roles and responsibilities 2

4 Overall security objectives 3

4.1 DNB must have an appropriate and managed level of security 3

4.2 Security work must be well integrated into DNB's operations 3

4.3 DNB must give priority to security work 4

4.4 DNB aims to promote transparency and a good security culture 4

4.5 The security level in DNB must be evaluated 4

1 Purpose

DNB is responsible for protecting assets at DNB belonging to our customers, employees, owners, operations, partners or society in general. Security at DNB is a matter of ensuring our ability to avoid damage to or loss of assets as a result of undesirable, intentional actions, as well as technological, environmental or human errors or accidents.

In addition, good security management and control is an important driver for strengthening our innovative capacity and customer confidence in the bank. A good level of security is important for DNB's reputation and corporate responsibility.

This policy establishes roles and responsibilities within security work and how DNB is to manage security and set overall goals for security work in the Group. The document does not cover work on ensuring a safe working environment/HSE. See the People Guide for information about the working environment/HSE.

2 Scope

This document applies to all permanent and temporary employees in the Group.

In principle, it also applies to all companies in the DNB Group, including the Group's international operations.

The governing document does not apply to:

1. Companies in which DNB has no controlling interest as defined by the Norwegian Private Limited Liability Companies Act, or companies which DNB owns jointly with other financial institutions. In such companies, DNB should use its influence as owner in the governing bodies to work towards ensuring that such companies have governing principles in place relating to corporate responsibility and ethics that are in line with DNB's own governing principles.

2. Companies which DNB has taken over or acquired for temporary ownership. Such companies must implement and comply with principles for ethics and corporate responsibility that are in line with DNB's own governance principles.

In the event of any conflict, legislation and other binding external rules will take precedence over this document. The person responsible for implementation must notify the document owner of any such conflict.

3 Roles and responsibilities

The Group Chief Executive Officer (CEO) is responsible for security in DNB's day-to-day operations and must review and evaluate performance and the extent to which security objectives have been achieved with all or part of the Group Management team at least once a year. The review is intended to ensure that the CEO knows the security status in DNB and makes the necessary decisions. The CEO must inform the Board of Directors of the results of the review.

The Group Executive Vice President for Technology & Services (T&S) is the document owner and responsible for establishing the Group's function for comprehensive security management, and for ensuring that good governance information is provided to the Group Management team and the Board.

The Chief Security Officer(CSO/CISO[1]) has a **Group-wide responsibility for security, and heads Group Security. The CSO is to lead the security work in the Group and implement centralised measures and activities that are to be used throughout the Group for setting security objectives for the Group and maintaining an appropriate level of security. The CSO must evaluate the security level and report this to the CEO and the Board.

The Group Executive Vice Presidents (Group EVPs) own risks associated with their own area of responsibility and are responsible for the implementation of security work in their own business areas and staff and support units. The Group EVPs must ensure that the CSO is involved in all processes and decisions that be of significance to the Group-wide responsibility for security. The Group EVPs must ensure that the CSO is notified about security risks and any deviations from compliance with security routines and procedures, as a basis for the Group Management team's evaluation and review of security.

Group Risk Management and Group Compliance are the Group's second line of defence and are responsible for conducting an independent review of security in DNB.

Group Audit reviews and audits security as the third line of defence.

All employees must familiarise themselves with the security rules that apply and actively contribute to a good level of security in DNB.

Any deviations from this policy must be handled by the responsible unit and reported in accordance with the deviation reporting process.

4 Overall security objectives

4.1 DNB must have an appropriate and managed level of security

DNB's security objectives are set on the basis of regulatory requirements and expectations issued by authorities in the countries in which we operate and set out in agreements we have entered into, as well as the Group's targets and risk appetite. The details of the security objectives are based on internationally accepted security practices.

The security level must fulfil the security objectives set, enable the management of risk and support the Group's business needs and expectations.

The aim of DNB's security work is to prevent security incidents, but also to detect, manage and prevent the recurrence of security incidents.

DNB must manage security in third-party relationships, and the service receiver[2] is responsible for ensuring an appropriate security level when all or parts of the operations are carried out by external suppliers and third parties.

4.2 Security work must be well integrated into DNB's operations.

Key factors for achieving the correct level of security are well-integrated organisation of security routines and procedures, appropriate security activities, and technical measures that are carried out and maintained as part of operations in general.

The risk methods and tools used in the operations should contribute to identifying, assessing and managing security risks as part of the Group's overall risk management.

[1] Chief Security Officer (CSO) or Chief Information Security Officer (CISO). CSO is used in this document.
[2] IT contract owner or IT supplier manager

4.3 DNB must give priority to security work

Establishing and maintaining an appropriate security level is crucial for DNB's operations, for the Group's performance of its social mission, and for partners and customers.

DNB must have sufficient expertise and capacity to achieve the appropriate security level and to carry out security work at all levels. DNB must organise specialist functions to ensure that the Group has the necessary security competence for supporting operational units in the performance of security work. Sufficient resources must be allocated for day-to-day operations and necessary investments to ensure an appropriate security level.

4.4 DNB aims to promote transparency and a good security culture

DNB plays an important role in society and must, as far as possible, be open about its security work both within the Group and externally. The CSO may share information and experience with relevant stakeholders and specialist communities with a view to raising awareness and strengthening expertise on security matters in society in general, and in the financial industry in particular.

DNB must actively promote positive attitudes, necessary competence and good conduct relating to security work. Activities that enable employees to practise routines and procedures must be carried out periodically, and at least annually. This will develop attitudes and competence among employees that will promote a high level of security, so that an appropriate security culture is incorporated as a natural part of operations. It must be easy and safe to ask questions and report on ambiguities, errors, deficiencies and breaches of security in DNB.

4.5 The security level in DNB must be evaluated

Follow-up and control of the security level is carried out in accordance with the **three lines of defence.**[3]

DNB must make sure that the organisation, external suppliers and third parties achieve the correct level of security and have a process for evaluating security work. The process must be integrated into the Group's management processes and internal control. Efforts must be made to ensure that the effect of security work can be measured in a consistent manner.

Security incidents must be reviewed and evaluated by the functions involved so that lessons learned from the incidents can be used to improve and strengthen DNB's security work.