Confidentiality and integrity

Digital Reporting Portal (DLR)

This document discusses the operation of the Digital Reporting Portal (Digitaal Loket Rapportages – DLR) and the measures De Nederlandsche Bank (DNB) has taken to ensure the security and reliability of the DLR reporting environment.

The Financial Supervision Act (Wet op het financieel toezicht) and other legislation require that institutions subject to our supervision submit regular reports in digital format. They must do so by means of the DLR reporting system that we make available. The exchange of data between you and us through the DLR takes place over the internet. The data you report to us are confidential, whereas the internet is a public network. It will be clear that this combination carries certain risks. We have therefore taken measures in several areas to safeguard the confidentiality and integrity of the reported data:

Encryption during connection.

Encryption prevents third parties from accessing the information that you and we exchange.

Robust authentication.

Authentication enables both you and us to establish unequivocally the identity of the party we exchange data with. The DLR system uses eHerkenning (eRecognition), assurance level 3 (2 factor authentication).

A secure infrastructure.

The DLR system is a client-server system. Your computer system and internet browser are the client environment, while the DLR application and the computer system it runs on together are the server environment. We have taken measures on the server side to safeguard the confidentiality and integrity of the reporting system. It is your responsibility to take adequate security measures in the client environment.

We have limited influence on the client environment.

Except for authentication data, the DLR therefore never stores data in the client environment, but always in the server environment, even the reports you have not yet finalised or submitted. This set-up enables us to take adequate measures to ensure the security of stored data. However, our staff are unable to view any report until it has been submitted. We only verify on a regular basis whether we can get appropriate access to the DLR server. We also conduct security assessments each year, which include penetration tests. Where needed, we use the outcome of these periodic assessments to further improve our system. We have a responsible disclosure policy under which users may report vulnerabilities.

Security procedures.

We have several different procedures in place to further enhance the security of the DLR system. The number of DNB system administrators authorised to access the system is restricted, and system use is logged. Incoming system abuse is monitored, and we will take measures if we observe such abuse. We will shut down the system if needed. DLR will terminate the connection with a reporting entity that has not used the system for a while.

Risk awareness.

Integrity is one of DNB's core values and as such we give it our ongoing attention. Our staff and management are aware of their responsible position in society, and they act accordingly. We are well aware that what was secure yesterday need no longer be secure tomorrow. We therefore test and evaluate all the above measures on a regular basis.