euroclear

Post-trade made easy

Data Security Rules and Contingency Planning for Errors and Other Exception Conditions

Decision by the CEO

To: Depository Participants
Issuer Agents
Settlement Members

Reference to Euroclear Finland Rules:	2.1.21
Entry into force:	7 May 2018
Supersedes:	The CEO’s Decision on Data Security Regulations as well as Preparations for Malfunction and Other Exceptional Situations in force as of 2 February 2015

List of Contents

1 Scope of Application

This Decision shall apply to organisations applying for the status of a Depository Participant or Settlement Member and to organisations that have been granted said status. This Decision shall apply to Infinity and the systems connected thereto.

2 Purpose and Aims

This Decision describes the principles that must be followed in order to maintain data security in data systems operated by Euroclear Finland. The purpose of the Decision is to provide a high standard of data security and ensure uninterrupted operations for Euroclear Finland’s book-entry register, settlement system, any other systems and Participants’ systems.

3 Contents of the Decision

3.1 General Data Security Principles

Each Participant connected to Euroclear Finland’s systems is required to employ a security policy and data security principles derived therefrom. The Participant shall create a written document of the general data security principles that have been approved by the Participant's management.

Internal instructions and supervision shall be used to make users aware of the security policy, the data security principles and the instructions drawn up on the basis thereof, and to ensure that users follow said instructions and principles and know their responsibilities relating thereto.

Each Participant shall appoint an owner for the data systems that are connected to Euroclear Finland’s data systems. This Data System Owner shall have the overall responsibility for the use of the systems. The Participant shall notify Euroclear Finland of its Data System Owner in writing.

Each Depository Participant's data system owner shall ensure that any users tasked with updating data in the Book-Entry Register either directly or through a subsystem of another Participant understand their responsibilities as persons maintaining data in the Book-Entry Register. In case of an error situation, the Data System Owner or a person appointed thereby shall, without delay, contact Settlement and Register Operations of Euroclear Finland, who shall evaluate the required corrective measures and provide all parties concerned with instructions for addressing the issue. Notification of errors shall also be regulated by the Decision by Euroclear Finland's CEO on the obligation to create a plan for the resolution of errors and discrepancies.

Each Depository Participant's Data System Owner shall ensure that the users of the Depository Participant's data system comply with their obligation to maintain secrecy. This secrecy obligation shall be observed especially in error situations where, as a result of an error by another Depository Participant, confidential or otherwise incorrect customer information is accidentally transmitted from the Book-Entry Register to the affected Depository Participant’s data system.

3.2 Identity and Access Management Documentation

In systems connected to Euroclear Finland’s data systems, the practical aspects of access rights maintenance shall be handled in a safe and reliable manner. Access rights shall always be personal and associated with a single identity. Each identity shall be covered by a reliable identification procedure and it shall be possible to block or suspend each identity's access rights when necessary. Each user shall be responsible for the user credentials entrusted to him or her. Each Participant shall ensure that all users understand that the user credentials they hold are a safety factor for the entire system, and should be used in a reliable and secure manner. Each Participant shall also ensure that the access rights granted to users are in line with the roles and responsibilities of the users.

Each time a transaction is completed or information is registered using a system connected to Euroclear Finland's systems, the username of the person performing the task shall be registered in the relevant system's transaction log. If the source of the transaction is a computer program residing in a Participant's data system, the program's individual identifier shall be registered in the transaction log instead of a username. It shall be possible to identify the source of each transaction transmitted to Euroclear Finland's data systems based on usernames and program identifiers registered in the transaction log.

Euroclear Finland shall maintain each Participant's access rights in accordance with the instructions provided by the Participant's business unit that uses the relevant application connected to Euroclear Finland's data systems. Maintenance activities shall be performed only at the request of the Data System Owner or a person authorised thereby, and the Participant shall be responsible for both issuing maintenance requests and performing maintenance concerning its own systems.

Any changes related to to access rights due to the access rights being restricted or the employment relationships being terminated shall be processed without delay. If a Participant decides to restrict a user's access rights or terminate the user's employment relationship, the user's access rights shall be updated without delay.

Each Depository Participant's Data System Owner shall maintain up-to-date information on the access rights (and the scope thereof) of the persons tasked with updating data in the Book-Entry Register.

3.3 Structural Protections for Data Systems

The production and testing environments of the systems connected to Euroclear Finland's data systems shall operate as discrete systems. Each Participant shall ensure that under no circumstances shall it be possible to transmit test materials from its testing environment to Euroclear Finland's production systems.

The systems' operating principles and technical solutions shall be realised in a way that ensures that potential hardware failures or software faults in the Participant's own systems (those connected to Euroclear Finland's data systems) do not jeopardise the performance of Euroclear Finland's daily schedule across the various systems. If a Participant system connected to Euroclear Finland's systems or part thereof forms a significant part of the Book-Entry System or settlement operations (based on the volume of transactions or a service it provides), the system shall be duplicated. For example, Depository Participant systems wherein accounts are kept on behalf of customers shall always be considered significant systems as referred to above. In the event of a serious malfunction, this backup system shall be available for use within 4 hours.

If a Participant system connected to Euroclear Finland's systems consists of several interconnected subsystems, each of which has its own data communications connections to outside the Participant's system, the Participant shall take special care to ensure the security and integrity of both external and cross-system data communications.

If a Participant intends to transmit, from its own data system to Euroclear Finland's data systems, customer-generated or software-generated transactions or other transactions that have not been processed by one of the Participant's users, the security of any such activities shall be verified prior to their introduction. The integrity and origin of any such transmitted transactions shall be verified. Data systems shall maintain a log file of transactions transmitted to Euroclear Finland's systems. This log shall indicate each transaction's identification data as well as the source of the transaction, its target system and the time of its registration.

3.4 System Backups

At regular intervals, system backups shall be made of all Participant data systems connected to Euroclear Finland’s data systems.

Depository Participant systems are required to have a separate system backup plan that indicates the system's backup schedule, the backup media and software used, backup storage location and retention period, the procedure for restoring the system from backups as well as the persons responsible for the backups.

Recovery backups shall be created at sufficiently frequent intervals, as this will allow Depository Participant data systems to be recovered regardless of the type of interruption and the time of its occurrence. If the Depository Participant holds customer accounts, transaction logs shall be used to ensure that each account's balance and transaction history can be reconstructed.

Whenever changes are made in the programs residing in a Depository Participant system, the security and integrity of the source code shall be checked.

3.5 Data System Change Management

Any significant changes in the software and the workflow of a Depository Participant system shall be tested in the Book-Entry Register’s testing t environment prior to transferring the changes into production. All changes in the application and utility programs in a Depository Participant system shall be handled with due care so as not to interrupt the normal daily operations of the Book-Entry System.

Before transferring any such changes into production, sufficient backups shall be created of the Depository Participant system, allowing the system to be reverted to a state preceding the changes.

3.6 Physical Safeguards and Facility Access Control

Physical safeguards and facility access control shall be used to ensure no unauthorised persons will, without constant supervision, have access to premises housing hardware, systems or workstations that are connected to Euroclear Finland’s data systems. Particular attention shall be paid to the access control of data centres, operations centres and other similarly critical facilities.

Forms containing input data transmitted to the Book-Entry Register, reports generated by a Depository Participant system and other corresponding materials relating to use of data systems shall be classified and filed in an appropriate fashion, ensuring that they will not compromise the data security of the system and those connected thereto.

3.7 Depository Participants Acting Solely on their Own Behalf

The CEO of Euroclear Finland may grant a Depository Participant acting solely on its own behalf permission to act in derogation of the obligations set forth herein where this is possible without jeopardising the reliability of the entire Book-Entry System.

euroclear

Post-trade made easy