Policy on Cybersecurity

Document purpose and scope

The purpose of the Policy is to protect the Group's data and IT infrastructure against cyberattacks and unauthorized exploitation of systems, networks and technologies. The Policy sets out that every user needs to be aware of their role in preventing and reducing cyber threats – not only technical users, but all users of the Bank's IT solutions. The Policy is reviewed on an annual basis. It has many operating procedures linked to it.

Which ESG-related issues does the Policy address?

The Policy sets out the measures that the Group applies to protect itself against cyberthreats. The Group continuously improves its cybersecurity safeguards and applies state-of-the-art technological solutions adequate to the level and type of emerging risk. These safeguards include encryption, data anonymization, firewalls, blocking spam emails, digital identity management, multi-factor authentication and others. The Policy's requirements related to IT infrastructure include:

- configuration of IT system and service security and the related controls, as well as patch management,
- protection of the network to prevent and stop cyber-attacks and mitigate their impact.

When it comes to information security, the Policy provides guidelines for the processing, storage and transmission of data to ensure that the information is appropriately protected from modification, loss, disclosure or unauthorized access. Additional requirements apply to cloud-based data processing. The Group defined the minimum security level for various classes of data. Regarding confidentiality, data is classified as confidential, internal or public. When setting the level of data protection, business and regulatory environment is taken into consideration, including personal data protection, bank secrecy principle and other confidentiality factors. When it comes to IT assets, access rights are granted depending on roles and responsibilities. The Policy states that access right entitlements should be reviewed periodically. It also addresses the segregation of responsibilities for key controls. The document defines the requirements for user identity management and access to data. Such measures are intended to ensure the confidentiality, integrity and accessibility of data for authorised users.

The document provides guidelines related to the monitoring, detection and response to security incidents. It introduces requirements related to malicious software intended to detect, prevent and respond to cyberattacks. It also sets out rules for the registration, classification, assessment, communication and management of incidents. The document addresses cyber intelligence solutions intended to prevent and mitigate impact on the organization. Under the Policy, relevant units are responsible for reporting incidents to decision-making bodies. Separate procedures apply to reporting special situations and incidents to regulators and the National Cybersecurity System (KSC).

The Policy also govern third party cyber security risk management. It provides criteria for the certification of services provided by third parties based on their cybersecurity risk level and cyber-risk monitoring and control measures applied during the duration of their contract.

Separate principles apply to regular testing designed to identify, manage and eliminate vulnerabilities in order to prevent cybersecurity attacks and incidents. The Policy also addresses Business Continuity Plans (BCP) and Disaster Recovery Plans (DRP).

It sets out the roles and responsibilities in the cybersecurity management process, including management reporting. The Policy also defines the frequency of audits carried out by subject-matter experts. Such frequency results from regulatory requirements (including the National Cybersecurity System Act) and the applicable standards such as ISO/IEC 27001 or PCI DSS.

The highest management level responsible for the Policy

The Policy is developed and updated by the Chief Information Security Officer (CISO), who reports directly to the MB Vice-president in charge of the Digital Transformation Division. Cybersecurity matters are also a regular item on the agenda of the proper committee for operational risk management (whose chairman is the MB Vice-president in charge of the Risk Management Division and vice-chairman is the MB Member in charge of the Legal and Compliance Division).

Application across the Bank's subsidiaries

The Policy applies across the Group.