5 Cybersecurity Rules Policy

Document purpose and scope

The Policy aims to promote responsible use of the internet and IT resources by all employees of the Bank. Data protection is a shared responsibility by everyone employed. All employees have to follow the cybersecurity rules.

Which ESG-related issues does the Policy address?

The Policy's cybersecurity rules address:

1) protection of information and IT equipment,
2) employees' conduct when using the internet, including social media,
3) response to phishing attacks,
4) use and protection of passwords,
5) reporting suspicious situations to cybersecurity teams.

The Policy requires that employees should be educated and trained. It says that training based on the 5 cybersecurity rules is mandatory for all employees. Based on their role in the Group, employees may be required to take additional cyber security training. The Policy also states how regular phishing exercises should be conducted. They practically train and educate employees on how to identify phishing techniques used by cybercriminals.

The highest management level responsible for the Policy

The Policy is supervised by:

- the Chief Information Security Officer (CISO), who reports directly to the MB Vice-president in charge of the Head of the Digital Transformation Division,
- the Management Board.

Application across the Bank's subsidiaries

The Policy applies across the Group.