Information Security Policy

Information security is critically significant for businesses, not only to protect assets and data but also to build trust with all related parties. Türkiye İş Bankası A.Ş. ("the Bank") considers information security a strategic priority. The objective is to ensure the confidentiality, integrity and availability of information assets across all products and services, thereby preserving the trust of customers, employees, business partners and stakeholders.

To achieve this goal, the Bank has established and maintains an Information Security Management System (ISMS) aligned with the internationally recognized ISO/IEC 27001 standard. This framework provides a systematic approach to identifying and analyzing threats, assessing and treating risks, implementing appropriate controls and ensuring the continuous improvement of information security practices.

The Bank adopts a holistic approach to information security that goes beyond technological measures and encompasses people, processes, physical environments and third-party service providers. Preventing unauthorized access to information (confidentiality), ensuring accuracy and completeness (integrity), and maintaining accessibility to authorized users when required (availability) form the foundation of this approach.

The Bank ensures compliance with applicable legal, regulatory, and contractual requirements. Information security is the shared responsibility of all employees, process owners and relevant stakeholders involved in the Bank's operations. To strengthen this responsibility, policies, procedures and governance structures are supported by regular training and awareness programs, embedding information security into the Bank's corporate culture.

An effective incident management process is implemented to prevent, detect and respond to information security events. Lessons learned from such events are used to enhance system resilience and drive continuous improvement. Business continuity and disaster recovery plans are maintained to minimize the impact of potential disruptions. In addition, third parties and suppliers are obliged to comply with the Bank's information security requirements enforced through contractual obligations and assessments.

The Bank is committed to effectively managing information security risks and ensuring compliance with legal and regulatory obligations, in alignment with the ISO/IEC 27001 standard. The Information Security Policy is reviewed annually, updated if necessary and made available to the public in line with the principle of transparency.