ENPARA BANK INC.

INFORMATION SECURITY AND CYBERSECURITY POLICY

The purpose of this policy is to establish a clear and comprehensive framework for protecting Enpara Bank's assets, customer data, and information systems against cyber threats. This policy covers Enpara Bank's information assets, information system processes and infrastructure, all employees, third-party suppliers, consultants, and any other stakeholders who have access to the bank's systems, data, or technology resources.

At Enpara Bank, information security is defined as the protection of information assets against threats, with the aim of ensuring business continuity and minimizing financial and operational losses. Information security seeks to guarantee the confidentiality, integrity, and availability of all information that is stored, processed, or transmitted.

At Enpara Bank, information security and cybersecurity are managed through a risk-based approach, with processes planned, implemented, and reviewed in accordance with international information security standards. This risk management approach encompasses the identification, assessment, and treatment of information security and cybersecurity risks, as well as the implementation of necessary preventive measures. The Bank manages these risks using an integrated risk management methodology that aligns with regulatory requirements, ISO 27001 standards, the Bank's information systems strategy, and its broader corporate risk management framework—all while maintaining a level of risk tolerance acceptable to the business.

Ultimate responsibility for ensuring information security within the bank rests with the board of directors. All employees and suppliers are required to comply with the legal regulations of our country, relevant laws and regulations, banking laws, BDDK regulations, and this policy. To this end, everyone who uses, manages, and accesses the bank's information systems;

✓ Protect the confidentiality, integrity, and availability of information assets,

✓ Understand and implement information security and cybersecurity policies, standards, procedures, and guidelines,

✓ Use IT resources in accordance with laws, policies, and business objectives,

✓ Ensure the confidentiality and privacy of customer information

✓ Adopt and implement the clean desk and screen policy,

✓ Share information only with authorized individuals,

✓ Use strong, hard-to-guess passwords and ensure their confidentiality

✓ Ensure that information is properly backed up and business continuity is maintained,

✓ Classify information and ensure that necessary controls are implemented,

✓ Report information security incidents and potential vulnerabilities.

A comprehensive information security awareness training program is developed and implemented to raise the level of information security and cybersecurity awareness among all employees, external service providers, and customers.

Initiatives that support the objectives and goals outlined in our information security policy are monitored and reported on throughout the year. The continuous improvement of the information security management system is ensured, and efforts toward continuous improvement are reviewed by management.