

Pacific Private Bank Information Security Policy

1. This Pacific Private Bank Limited (hereinafter - the Company) Information Security Policy (hereinafter - the Policy) defines the scope of information security of Pacific Private Bank Limited and the information security objectives of the Company.
2. The scope of the Company's information security management system includes:
 - 2.1. Provision of electronic transaction services to business and private customers;
 - 2.2. Issuance of loans backed by collateral;
 - 2.3. Provision of term deposits;
 - 2.4. Provision of management services for corporate clients.
3. The Company undertakes to ensure the confidentiality, integrity and availability of the services provided and all information managed by the Company; to manage the risk properly and have the confidence of stakeholders; to maintain, manage and continuously improve the information security management system in accordance with the requirements of the standard ISO / IEC 27001 (ISO / IEC 27001: 2013) (hereinafter - the Standard).
4. The Information Security objectives are:
 - 4.1. Continuously improve the effectiveness of the information security management system in implementing Information Security Policy and its objectives;
 - 4.2. Allocate the resources necessary for the proper functioning of the information security management system;
 - 4.3. Ensure effective risk management and the use of appropriate risk management measures to manage the risk to an acceptable level through the annual risk assessment and the implementation of the risk management plan;
 - 4.4. Meet the needs of stakeholders, implement contractual obligations and applicable information security requirements;
 - 4.5. Ensure the competence and awareness raising of employees in the field of information security;
 - 4.6. Ensure the basic security principles of the provided services and all information managed by the Company;
 - 4.7. In the event of a breach of security of the information system, assess the damage caused, limit its consequences and take the necessary measures to eliminate it, ensure measures for business continuity;
 - 4.8. Regularly update the objectives of the information security management system;
 - 4.9. Regularly update the technical means used to ensure information security;
 - 4.10. Carry out regular audits of the Company's information security management system and eliminate discrepancies found during the audit.
5. Final Provisions
 - 5.1. This Policy is approved by the decision of the Board of the Company.
 - 5.2. The Board appoints Chief Technology Officer to ensure that the information security management system complies with the requirements of the Standard, to inform the Board about the effectiveness of the information security management system and to acquaint the Company's employees with the Information Security Policy.
 - 5.3. The Policy shall be made available to stakeholders in a form that is accessible and comprehensible to them.
 - 5.4. The Policy is reviewed periodically, at least once a year, and revised as necessary.