Land Bank of Taiwan Cybersecurity Policy

Article 1. Land Bank of Taiwan Co., Ltd. (hereinafter referred to as the Company) established the Policy to enhance cybersecurity management, ensure data, system, equipment, and network security, and protect customer rights and interests.

Article 2. The Policy is implemented in accordance with the "Cyber Security Management Act" and related subsidiary legislation.

Article 3. Cybersecurity in this Policy refers to the protection of the information and communication system or data from unauthorized access, usage, control, leakage, alteration, destruction, or other forms of infringement to ensure information assets are adequately protected.

Article 4. The goal of cybersecurity is to ensure the confidentiality, integrity, and availability of the Company's information and communication assets and to protect the Company's operations from the impact of information security incidents.

Article 5. The Cybersecurity Policy shall include at least the following items and the Company shall also establish related management regulations:

I. Purview and responsibilities of cybersecurity;

II. Personnel management and cybersecurity training and education;

III. Information and communication systems security management;

IV. Network security management;

V. System access control management;

VI. System development and maintenance security management;

VII. Information asset security management;

VIII. Physical and environmental security management;

IX. Sustainable business operations planning and management;

X. Other cybersecurity management matters.

Article 6. To effectively promote cybersecurity tasks, the Company shall establish the “Cybersecurity Initiative Committee” to take charge the Company’s cybersecurity policies and goals, cybersecurity maintenance plans and implementation status, and discussions regarding other important cybersecurity matters. It shall also organize regular meetings of the Cybersecurity Initiative Committee to ensure cybersecurity.

Article 7. The Company’s units shall ensure the accuracy of the information and communication processing procedures, the security of related information and communication systems and equipment, and prevent the theft, alteration, interference, sabotage, intrusion, sales, leaks, or inappropriate use of such data, systems, equipment, and networks or other actions detrimental to the interests of the Company.

Article 8. Cybersecurity requirements must be considered in advance for the Company’s outsourced establishment and operation of the information and communication system, as well as the provision of information and communication services. The Company shall clarify the supplier’s cybersecurity liabilities and confidentiality provisions and include them in the contract. The Company must require suppliers to abide by the contractual obligations and implement audits.

Article 9. The Company shall use legal software, execute system security updates, and regularly update related virus codes and virus scan engines to prevent intentional inappropriate or illegal use and deter the intrusion and damage of hackers and viruses.

Article 10. The Company shall establish and implement cybersecurity maintenance

plans and implement regular assessments of the implementation status.

Article 11. The Company shall establish related mechanisms for cybersecurity incident reporting, response, and exercises to ensure the continuous operations of the Company’s businesses.

Article 12. Every employee must be responsible for cybersecurity. All employee of the Company shall have the responsibility and obligation to protect the information assets they access or use. When they become aware of any violation of cybersecurity protocols, they must implement prevention measures and immediately report such violations. Employees may not leak business secrets they learned or use such information in an inappropriate manner during and after their employment.

Article 13. The Policy shall be sent in writing or by other means to all employees, other public and private authorities (institutions) that connect with the Company for operations, and information and communication service providers to facilitate compliance. Violators of the Company’s cybersecurity regulations shall be held accountable based on the severity of their violations.

Article 14. This policy is subject to evaluation at least once a year to reflect the latest development in government regulations, information technologies and the Company's business practices, and thereby ensure the effectiveness of cybersecurity practices.

Article 15. Matters not stipulated in this Policy will be handled in accordance with relevant laws or regulations of the competent authorities or other relevant rules of the Company.

Article 16. The Policy shall be approved by the Audit Committee and submitted to the Board of Directors for approval before implementation; the same

applies to subsequent amendments.