Information Technology Security Policy

BCPG Public Company Limited (hereinafter referred to as the "Company") recognizes information technology as a key factor in supporting its business operations and enhancing its competitiveness in line with leading organizations. The Company is committed to maintaining modern, standardized, and efficient information technology systems, with appropriate information technology security management aligned with the Company's information technology security requirements.

The Company is also committed to promoting and developing employees' knowledge and capabilities in information technology to enable them to perform their duties effectively and to ensure that the use of information technology complies with applicable laws. In addition, the Company supports continuous learning and self-development of employees through information technology systems. Accordingly, the Company has established standards for the use of information systems and networks as guidelines for appropriate practices.

Section 1: Information Security Policies

The Company aims to establish direction and provide support for personal data protection and information security in the use of information systems, in accordance with business requirements, applicable laws, regulations, and relevant procedures.

The information security policies shall be documented, reviewed, endorsed, and approved by management and communicated to users of the Company's assets to ensure their awareness of and compliance with such policies. The Company shall review these policies at specified intervals and revise them as appropriate to ensure alignment with the Information Technology Security Policy of Bangchak Corporation Public Company Limited.

Section 2: Organization of Information Security

The Company aims to manage information security relating to its information and information processing facilities that are accessed, processed, or used for communications with external parties.

The Company shall establish an Information Security Management Committee to coordinate responsibilities, assess risks, and review information security activities. The Company shall also coordinate with external service providers and external users of information and establish clear requirements governing access to the Company's information and information processing facilities.

Section 3: Human Resource Security

The Company aims to ensure information security before employment, during employment, and upon termination or change of employment or position of employees and external parties.

The Company also aims to enhance knowledge and awareness of information security threats and related issues, as well as practices relating to personal data protection, in order to reduce risks arising from theft, fraud, misuse of equipment, and errors in the performance of duties.

Section 4: Asset Management

The Company aims to protect its assets against potential damage and to ensure an appropriate level of protection for information.

The Company shall maintain an inventory of assets, identify asset custodians and asset owners, and establish appropriate rules for the acceptable use of assets. Assets shall be classified according to their confidentiality levels and appropriately labeled to facilitate their management in accordance with the assigned classifications.

Section 5: Access Control

The Company aims to establish and manage access rights to its information systems, network systems, operating systems, and applications in order to prevent unauthorized disclosure or theft of information and information processing facilities.

Section 6: Physical and Environmental Security

The Company aims to control and prevent unauthorized physical access and to protect its assets against loss, theft, damage, disruption, or interference.

The Company also aims to prevent unauthorized disclosure of information and to ensure that its business operations are protected against disruption or interruption.

Section 7: Operations Security

The Company aims to manage information security in its operations and to establish appropriate operational management processes to protect information systems against malware, viruses, and other malicious threats.

Section 8: Communications Security

The Company aims to securely manage communications, network systems, and the transfer of information to external parties in order to prevent unauthorized disclosure or modification of the Company's information.

The Company shall also establish information security requirements, service levels, and management requirements for network services, including such requirements in agreements or contracts relating to network services provided by external service providers.

Section 9: System Acquisition, Development and Maintenance

The Company aims to ensure that information security is considered a fundamental and essential component in the acquisition and development of information systems.

Appropriate measures shall be implemented to prevent errors, loss, unauthorized modification, and misuse of information; maintain the confidentiality of information; authenticate the identity of information senders; and preserve the integrity and completeness of information through appropriate cryptographic controls.

The Company shall also maintain the security of software, information, and files associated with its systems and services and reduce risks arising from attacks that exploit known or publicly disclosed technical vulnerabilities.

Section 10: Supplier Relationships

The Company aims to appropriately manage its relationships with external service providers, including establishing information security requirements and conditions applicable to such service providers and conducting appropriate evaluations of their performance.

Section 11: Information Security Incident Management

The Company aims to ensure that information security incidents and weaknesses affecting its information systems are appropriately addressed within a suitable timeframe.

The Company shall establish consistent and effective approaches and procedures for managing information security incidents involving the Company's information.

Section 12: Information Security Aspects of Business Continuity Management

The Company aims to prevent disruptions or interruptions to business activities and to protect critical business processes from the effects of failures or unavailability of information systems and related services.

The Company shall ensure that information systems can be recovered and restored within an appropriate timeframe in order to support business continuity.

Section 13: Compliance

The Company aims to prevent violations of applicable laws, regulations, procedures, contractual obligations, and other information security requirements.

The Company shall also ensure that audits and assessments of information systems are conducted effectively while minimizing interference with or disruption to business processes.

Section 14: Information Security for Use of Cloud Services

The Company aims to ensure the secure use of cloud services within the organization, with a focus on protecting the Company's information systems and information while enabling employees to perform their duties efficiently through the appropriate use of various technologies.

The Company shall establish principles and requirements for the secure use of cloud services in order to reduce risks and enhance business capabilities. This policy establishes requirements for the selection and management of cloud computing services to ensure that information is appropriately protected according to its importance to the business and its classification based on the Company's confidentiality requirements.

Section 15: Cryptography

The Company aims to establish guidelines for the use of cryptography and the management of cryptographic keys to ensure that cryptographic controls are implemented appropriately and effectively.

The use of cryptography and cryptographic key management shall be consistent with business requirements, information security requirements, and applicable laws, regulations, rules, agreements, and contractual obligations relating to cryptography.

- Signed -

Ms. Sattaya Mahattanaphanij

Senior Executive Vice President

Corporate Excellence