Information Technology and Cyber Security Policy

Bangchak Corporation Plc., "the company", has a policy to ensure that it's information technology system is an important factor that supports the company's ***Sustainable Development for the Environment and Society Policy*** in order to meet our stakeholders' expectations. The company emphases the importance of having internationally recognized, modern, effective, and safe guidelines, work process, and standards in place for its operations.

The company has developed Cyber Security Policy to ensure that Bangchak Corporation Plc and its subsidiaries have safe and reliable IT system and processes as well as ensure the protection of information by considering cyber security risks, maintaining confidentiality, data protection, accuracy, completeness, and readiness for appropriate operations including in accordance with regulations, regulations, laws, information security laws.

Information Technology and Cyber Security Policy

1) ***Verification and Risk Management***

Project owner and the functional department assigned to oversee the company's information system shall provide information technology risk management that covers the risk identification, risk assessment, and control risk to be within the acceptable level, including assigning responsible person for information technology risk management to ensure appropriate information technology risk management.

2) ***Information Technology and Resource Management***

Project owner shall align the management of information system with the company's strategy, including ensuring appropriate level of human resources to manage IT systems and develop risk management plans in cases where there's a lack of human resource.

3) ***Protection of IT Assets***

3.1) Access Control

Project owner and the functional department assigned to manage the company's IT systems shall develop and use security standards that limit access and usage of the company's IT systems, categorized by information types, importance, or level of confidentiality. Access control should include time usage limitation and channel limitation. Proper defense of cyber attacks and malware shall also be instated.

3.2) Physical and Environmental Security

Project owner and the functional department assigned to manage the company's IT system shall develop measures to protect, control usage, and maintain physical property related to IT technology and equipment that are the core infrastructure of the company's main IT systems. System protection measures shall also include access controls and data confidentiality.

3.3) Information Management and Data Protection

(1) Classification of Information Assets

Project owner and the functional department assigned to oversee the company's IT system shall specify guideline for the classification of information assets and prioritize information confidentiality level in accordance with relevant laws and regulations as well as the company's requirements and manage information confidentiality level in accordance with the company's operational guidelines.

(2) Emergency Plan and Backup System

Project owner and the functional department assigned to manage the company's IT system shall develop a backup system to ensure system redundancy and develop business continuity plans including cases where operation cannot be conducted electronically as well as plans to bring systems back in operation. The emergency plans shall be updated to ensure that they are always ready for new situations and emergencies. The plans shall also assign responsible persons for maintaining the main system, the backup system, and for developing and maintaining emergency plans as well as to test the main and backup systems readiness and emergency plans.

(3) Cryptographic Control

Project owner and the functional department assigned to oversee the company's IT system shall specify measures for cryptographic control as well as guidelines for cryptography in alignment with risk level of each type of information as set by the company. In addition, relevant project owner and the functional department shall conduct follow up activities to ensure that policies and procedures being comply to.

Users Control

(1) Users Control

Project owner and the functional department assigned to oversee the company's IT system shall have policy to control users and access as follow:

1. ***Protecting Information and IT Assets During Periods of Non-Activities***

Project owner and the functional department assigned to oversee the company's IT system shall ensure that all access to the company's IT systems including computers require username and password to log in and log out. Each user shall immediately log out of the systems and devices when it is no longer being used or when user is away from the device.

2. ***Access from Mobile Devices and External Networks***

Project owner and the functional department assigned to oversee the company's IT system shall develop measures to protect the security of mobile devices. Security measures should be appropriate to the risk levels based on threat of attacks on the system or forced connections. The measures shall also includer guidelines for using equipment outside of the company's network.

3. Control of Software Installations

Project owner and the functional department assigned to oversee the company's IT system shall develop operational work plan and procedures to control the installation of software on operable systems in order to prevent unauthorized software installation. The relevant departments shall specify a list of software standard that are authorized for installation on the company's computers. The approved software list shall be officially documented, updated, and communicated to all users within the company.

(2) Control of IT Outsourcing

Project owner and the functional department assigned to oversee the company's IT system shall develop requirements and framework for external IT service providers to ensure effectiveness and security. The requirements and framework shall extend to sub-contractors of IT service providers.

3.4) Management of Computer Network and Data Transmission

(3) Security of Information Communicated over Computer Network

Project owner and the functional department assigned to oversee the company's IT system shall control and ensure that the company's network is secured including specifying security level requirements, level of services, and network management services in the contract or service agreement both externally and internally. Separation of networks based on access needs, level of impact to the IT security system and importance on information reside within the network shall also be considered

(4) Control of Data Transmission

Project owner and the functional department assigned to oversee the company's IT system shall control flow of information exchange between departments, between companies within Bangchak Group, and with external entities by:

1. Information Technology Department shall ensure that requirements for operational information exchange is well defined based on communication channel, type of information, and sensitivity level. Memorandum of Agreement should be developed between parties that are exchanging information including internally, within Bangchak Group's companies, and external entities.
2. Information Technology Department shall specify measures for controlling electronic messages such as e-mail, electronic data interchange, and instant messaging. Electronic messages that are deemed important shall be appropriately protected from unauthorized access and interferences.
3. Department Heads shall ensure that personnel both internal and external sign non-disclosure agreement.

3.5) Protection of Information Technology Systems

(5) Malware Protection

Project owner and the functional department assigned to oversee the company's IT system shall develop measures to detect, prevent, and restore systems to protect assets from malware including user awareness raising.

(6) Management of Technical Vulnerabilities

Project owner and the functional department assigned to oversee the company's IT system shall ensure that technology vulnerabilities are appropriately addressed by:

1. Conduct penetration test with department that have connections to untrusted networks using independent personnel from Information Technology Department in accordance with Risk and Business Impact Analysis as follow:
   1.1. Testing must be conducted at least once every 3 years or after every major change for systems designated as high importance.
   1.2. Testing must be conducted once every 5 years for other importance systems
2. For all important systems, vulnerability assessment must be conducted at least once a year or after any major change. Findings must be reported to relevant departments for corrective actions.
3. For all important system, testing of measures that may impact system security and cyber security drill must be conducted at least once a year.

3.6) System Acquisition, Development and Maintenance

Project owner and the functional department assigned to oversee the company's IT system shall define requirements the procurement, development, and maintenance of IT system in order to reduce errors in the product/service requirements, system design, development, and testing of new or modified IT systems, this includes ensuring that the procured systems are in accordance with contracts.

4) *Information Technology Security Standards*

Information Technology Department shall develop standards for protecting IT system security in accordance with the Information Technology and Cyber Security Policy and communicate it contents to all relevant parties to ensure that all parties understand and operate in accordance with the policy. In addition, responsible person must be assigned to ensure the effectiveness of the company's 14 measures as follow:

1 Information Security Standard
2 Organization of Information Security
3 Human Resource Security
4 Asset Management
5 Access Control
6 Cryptographic Control
7 Physical and Environmental Security
8 Information System Operations Security
9 Network Communications Security
10 System Acquisition, Development and Maintenance
11 IT Outsourcing
12 Information Security Incident Management
13 Information Security Aspects of Business Continuity Management
14 Compliance

5) *Review of Policy*

The Information Technology and Cyber Security Policy shall be reviewed annually at the minimum or when there are any major changes. IT department and relevant departments shall ensure that their measures, standards, and guidelines are updated in accordance with any policy changes.

6) *Communication of Policy*

All departments are responsible for communicating and supporting the provisions within this policy.

7) *Reporting*

The company's Board of Director must be informed of the compliance to the Information System and Cyber Security at least once a year or when there are any events that may affect the implementation and compliance of the policy. This includes damages to computer systems or information technology system resulting from defect, neglect, or violation of standards and regulations set by the company. In such events the Chief Executive Officer is responsible for the risk, damage, and resulting dangers.

8) *Enforcement Provisions*

This Policy shall be applied to all Bangchak Group's employees (temporary and permanent) and external parties including suppliers and service providers. The Policy is effective immediately.