Information Technology and Cyber Security Policy

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

The company has developed Information Technology and 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) Information System Development Control

To ensure that the development of digital and information technology systems within the organization aligns with the Company's strategies, while maintaining security and effective control, all systems under development are required to undergo a review process by the IT Solution Architect Committee, as designated by the Company, prior to the initiation of development. This is to ensure that:

1.1) The development, modification, and changes to digital and information technology systems comply with the policies set forth by the IT Committee

1.2) There is a comprehensive view of the overall digital and information technology systems within the organization (Enterprise Architecture)

1.3) Risks associated with various systems can be clearly identified

1.4) Data connectivity and flow across the entire organization (Data Flow Visibility) are clearly understood to support effective information security management and governance

1.5) All systems are recorded in an organized manner within the Company's System Inventory.

Furthermore, prior to any system going live (Go-Live), a formal Change Management process must be implemented, with due consideration to potential risks and impacts. Approval by the Committee is granted upon meeting one of the following conditions:

Criteria Category	Committee Approval Required (✓)	Committee Approval Not Required (✗)
1. Type of Information Involve	The system processes or stores personal data (subject to the Personal Data Protection Act (PDPA)), business information, or other sensitive information.	The system does not process or store personal data or the Company's confidential information.
2. Integration with Critical Systems	The system is integrated with or connected to other critical systems, such as ERP, HR, Finance, Email Gateway, or Internet-facing systems.	The system is not integrated with any other system or operates as a standalone system.
3. System Scale	The system is of medium to large scale, comprises multiple modules, and has integrations with other systems.	The system is small in scale and is intended solely for use within a department, business unit, or other limited organizational unit.
4. User Scope	The system is intended for use by employees across the organization and/or external customers/users.	The system is intended solely for use by operational personnel within a single department.
5. Impact of System Failure	A system failure may adversely affect business operations or the Company's compliance with applicable laws, regulations, or recognized standards.	System failure has no significant impact on the organization and is used only to support individual or departmental tasks.

2) Security Measures with a Focus on Sustainability

The Company has established an Information Security and Cyber Security Policy that ensures the security and resilience of its digital and information technology systems in alignment with the Company's sustainability framework and overall Bangchak Sustainability policy.

3) Governance and Ethical Use of AI within the Organization

The Company shall establish clear guidelines for the use of Artificial Intelligence (AI) technologies within the organization to ensure they are utilized effectively, transparently, and ethically, with due consideration to data security. These guidelines aim to support employees in their work and enhance the quality of the Company's services.

3.1) AI Scope

3.1.1) This Policy applies to the use of both third-party AI services (e.g., ChatGPT, Microsoft Copilot, and Google Gemini) and AI systems developed internally by the Company.

3.1.2) This Policy applies to all personnel at all levels who are directly or indirectly involved in the use of AI.

3.2) Appropriate AI Use Guidelines

3.2.1) Only AI services approved by the Company may be used.

3.2.2) AI may be used for data analysis, automation of repetitive tasks, and preliminary decision support to improve operational efficiency.

3.2.3) AI shall not be used to make significant decisions affecting individuals without appropriate human review and approval.

3.2.4) Information classified as Top Secret shall not be entered into any AI system.

3.2.5) Information classified as Confidential, sensitive information, or personal data shall be handled as follows:

3.2.5.1) Such information shall not be entered into any AI system unless appropriate safeguards have been implemented and authorization has been obtained from the data owner.

3.2.5.2) Such information may only be entered into AI systems provided or approved by the Company.

3.2.6) Sources shall be properly cited whenever AI-generated content is used in official documents or publications.

3.2.7) AI shall not be used in a manner that infringes upon the rights of others, intellectual property rights, or applicable laws and regulations.

3.3) AI Accountability

3.3.1) AI users are accountable for their use of AI and shall verify the accuracy and appropriateness of AI-generated outputs before use.

3.3.2) The Information Technology and Cybersecurity Committee (IT Committee) is responsible for overseeing AI governance within the Company.

3.3.3) The department that adopts AI for use is responsible for assessing and managing AI-related risks.

3.3.4) The Company reserves the right to monitor the use of AI to ensure compliance with the Policy.

3.4) Information Security and Privacy

3.4.1) AI shall be used in accordance with this Policy to prevent unauthorized disclosure or leakage of information.

3.4.2) AI systems shall undergo appropriate security and risk assessments before being deployed in critical processes.

3.4.3) The collection, processing, and storage of personal data by AI systems shall comply with the Personal Data Protection Act (PDPA).

3.5) AI Training and Awareness

3.5.1) The Company shall provide training to employees on the secure and ethical use of AI.

3.5.2) The Company shall promote awareness of both the capabilities and limitations of AI to encourage responsible and effective use.

3.6) Reporting of AI Issues and Inquiries

3.6.1) Employees who encounter issues or require guidance regarding the use of AI may contact IT-service@bangchak.co.th.

3.7) AI User Guidelines

Do	Don't
1. Understand the capabilities, limitations, and terms of service of each AI service, as AI systems may have limitations, such as the recency of the data used for processing.	1. Do not assume that AI is always accurate or use it without appropriate judgment.
2. Verify the accuracy of AI-generated outputs carefully to prevents system errors when using AI to assist with programming.	2. Do not rely on AI-generated results and use them immediately without verification.
3. Ensure that the Company's information is protected from unauthorized disclosure. ● Define and review access permissions for shared information in Microsoft 365 at least once a year, such as SharePoint on Teams Channels, or documents in Microsoft 365. ● Remove sensitive information before submitting it to AI. (Top Secret and Confidential information shall not be entered into any AI system, and shall comply with the Company's Information Technology and Cyber Security Policy.) ● Use the Company's Copilot for organizational work.	3. Do not use Company information or important information without appropriate caution. ● Do not submit important information into AI systems, such as personal names, IP addresses, or passwords. ● Do not use a personal Copilot accounts for organizational work.

Do	Don't
4. Always consider potential impacts before using AI. Use AI in accordance with the applicable terms of service and for constructive purposes.	4. Do not use AI without considering the potential impacts that may result.
5. Report issues or request additional information at **IT-service@bangchak.co.th.**	5. Do not ignore abnormalities identified during AI usage. For example, discovering important information belonging to another department within the Company.

4) End User Computing (EUC)

The Company shall establish guidelines for the use, control, and governance of End User Computing (EUC) tools to ensure that data processing conducted by end users is secure, accurate, and fully compliant with the Company's Information Technology and Cyber Security policy.

Definition: End User Computing (EUC) refers to data processing or the development of small-scale applications by end users for specific business purposes, including calculations, reporting, data analysis, and business process automation.

4.1) EUC Usage Policy

4.1.1) Users are required to obtain approval from their supervisor or authorized approver before using EUC tools to process critical work or important organizational information.

4.1.2) Data processed through EUC must have appropriate access controls in place.

4.1.3) Users shall maintain appropriate version control for EUC tools, particularly those supporting business reporting or decision-making.

4.1.4) EUC shall not be used as the primary system for storing or processing high-risk information, such as Personally Identifiable Information (PII) or financial information, unless appropriate security controls have been implemented in accordance with the Company's IT policies.

4.1.5) EUC solutions that have a significant impact on business operations shall be backed up regularly and periodically reviewed by the responsible departments.

4.1.6) Macros or scripts that directly access Company systems in real time shall undergo risk assessment and obtain approval from the IT Solution Architect Committee before implementation.

4.2) Security Management

4.2.1) Devices used for EUC shall be protected by Company-approved security controls, including antivirus software, endpoint protection, and Data Loss Prevention (DLP).

4.2.2) EUC solutions developed by users should be stored in secure locations with appropriate backup and access controls.

4.2.3) The use of EUC to process or store legally regulated information (e.g., PDPA) shall be approved and recorded in the Company's Record of Process asset (ROPA).

4.3) Monitoring and Governance

4.3.1) The Company reserves the right, through designated functions, to monitor and review the use of EUC where reasonably necessary to manage risks.

4.3.2) Each business unit shall register and maintain an inventory of EUC under its responsibility for monitoring and risk assessment purposes.

4.3.3) EUC solutions identified as high risk shall be subject to appropriate risk mitigation measures or migrated to enterprise.

5) 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.

6) 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.

7) Protection of IT Assets

7.1) 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.

7.2) 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.

7.3) Information Management and Data Protection

7.3.1) 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.

7.3.2) 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.

7.3.3) 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.

7.4) Users Control

7.4.1) 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:

7.4.1.1) 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.

7.4.1.2) 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.

7.4.1.3) 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. Therelevant 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.

7.4.2) Control of IT Outsourcing

The project owner department, or the department assigned to oversee the Company's information systems, is responsible for maintaining information security as follows:

7.4.2.1) During Procurement

External service providers must be assessed for their information security capabilities to ensure compliance with the Company's standards and policies. A risk assessment of potential threats from the external service provider must be conducted, and appropriate preventive measures must be defined before granting access to the Company's information systems or data.

7.4.2.2) During Operations

Ongoing monitoring and evaluation must be carried out to ensure continuous compliance with the Company's information security policies.

7.4.2.3) In the event that an external service provider replaces existing personnel with new personnel

The Company must be notified to deactivate the system user account of the previous personnel and request the creation of a new user account for the replacement personnel.

7.4.2.4) Upon Contract Termination or Cancellation

User accounts granted to external service providers must be deactivated, or the system administrator must be notified to do so, in order to prevent system access—such as through VPN. In addition, the Company must follow up to ensure that the external service provider securely deletes all Company data from their environment or any information systems used, using irreversible methods, to ensure that no operational data previously accessed can be leaked or recovered.

7.5) Management of Computer Network and Data Transmission

7.5.1) 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 contractor 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

7.5.2) 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:

7.5.2.1) 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.

7.5.2.2) 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.

7.5.2.3 Department Heads shall ensure that personnel both internal and external sign non-disclosure agreement.

7.6) Protection of Information Technology Systems

7.6.1) 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.

7.6.2) 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:

7.6.2.1) 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:

7.6.2.1.1) Testing must be conducted at least once every 3 years or after every major change for systems designated as high importance.

7.6.2.1.2) Testing must be conducted once every 5 years for other importance systems

7.6.2.2) 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.

7.6.2.3) For all important system, testing of measures that may impact system security and cyber security drill must be conducted at least once a year.

7.7) 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 systemin 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.

8) 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

9) 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.

10) Communication of Policy

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

11) Reporting

To ensure that IT security system management is continuously reviewed and improved, the Company requires that compliance with the Information Technology and Cyber Security Policy, including any relevant regulations and requirements, be reported to the Board of Directors 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.

12) 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.

-signed-

Mr. Chaiwat Kovavisarach

Group Chief Executive Officer and President,

Executive Director, Director with Authorized Signature

(26 June 2025)

Reviewed and approval by Information Technology and Cybersecurity Committee on 28 Apr 2025.