- Translation -

Information Technology Security Policy

Bangchak Sriracha Public Company Limited ("Company") regards its information technology (IT) system as crucial to the support to **the sustainable policy of business development** to accommodate its move to meet the expectations and demands of stakeholders. Notably this move comes in the form of guidelines, tools, and operating standards that are sophisticated, efficient, and safe on a par with international standards.

The Company desires that its IT actions, as well as those taken by its affiliates, command security and credibility. Also, its data and information assets should come under proper stewardship with due regard for risks arising from potential threats to information security and cybersecurity, measures designed for confidentiality, accuracy, integrity, and readiness for implementation. Also, these must align with rules, regulations, and laws concerning information security. To this end, the Company has therefore defined the following IT security policy.

IT Security Policy

Below are the details of the IT Security Policy.

1) Risk audit and assessment

Project owner units or units assigned to handle the Company's information systems must institute IT risk management embracing risk identification, assessment, and control in line with the corporate risk appetite. Also, they must appoint suitable responsible parties to manage IT risks for proper risk management.

2) IT resource management

Project owner units must institute IT resource management in line with the Company strategic plans by embracing sufficient human resource administration and IT system for IT implementation. They must also put in place key risk management in cases where resource allocation falls short of IT operation.

3) Information asset security

3.1) Access and information system control

Project owner units or units assigned to handle the Company information systems must define IT system security standards for the control of IT system access and applicable. Such systems must prove compatible with data types, priorities, or confidentiality classes as well as data access authorities, time, and channels. Also, they must provide mechanisms preventing penetration through invaders' networks and from undesirable software that could harm the Company data.

3.2) Establishment of physical and environmental security

Project owner units or units assigned to handle the Company information systems must define preventive and control measures as well as measures for physical maintenance of information and hardware asset, the infrastructure supporting the Company information systems to keep them in ready condition. They must also prevent unauthorized access to information assets or unauthorized information disclosure.

3.3) Management of information and safeguarding of confidential information

(1) Classification of information assets

Project owner units or units assigned to handle the Company information systems must define guidance for grouping information assets and assigning information confidentiality classes. Such classes must align with laws and requirements related to the Company and they must manage data confidentiality classes accordingly.

(2) Development of backup systems and emergency management plans

Project owner units or units assigned to handle the Company information systems must develop suitable backup information systems and keep them ready for use. To this end, they must select key information systems and map out emergency management plans for emergency cases where electronics operation is interrupted. To elaborate, they must adjust such emergency plans for suitable finetuning in line with respective application. They must define personnel's roles and responsibilities for those in charge of information and backup information systems as well as backup plans for emergencies where electronics operation is interrupted. Finally, they must ensure that information systems, backup systems, and emergency plans are regularly tested.

(3) Control of data encryption

Project owner units or units assigned to handle the Company information systems must define encryption measures together with an approach for encryption standard selection in line with risks to data of each confidentiality classes. They must also regularly monitor compliance with such policies and procedures.

3.4) Control of operating personnel

(1) Control over users

Project owner units or units assigned to handle the Company information systems must institute control over the application of information assets and information systems as follows.

1. Define measures to protect hardware information assets while idle.

Project owner units or units assigned to handle the Company information systems must require that users of computers or IT systems enter passwords and logout immediately

once they no longer in use. They must ensure that computer display screens and critical hardware are locked when they are not in use or become idle as defined.

2. **Define application of mobile devices and work from networks outside the Company.**

Project owner units or units assigned to handle the Company information systems must define proper measures for controlling the security of mobile communication devices fitting risks associated with connecting external devices with the Company's computer networks. They must also set out control measures for those devices exported for application outside the Company.

3. **Define control over software installation on systems**

Project owner units or units assigned to handle the Company information systems must develop work procedures and measures controlling software installation on production systems to limit software installation by users, prevent unauthorized software installation, and define in writing authorized software standards, as well as constantly updating them. Also, they must inform users within the Company for their compliance.

(2) Control over IT outsourcing

Project owner units or units assigned to handle the Company information systems must develop requirements and work scopes of IT outsources for efficiency and security. Such items must embrace IT subcontractors.

3.5) Management of computer network systems and information transfer

(1) Security of information communication through computer network systems.

Project owner units or units assigned to handle the Company information systems must control and ensure that management of computer network system control is secure as well as ensuring definition of qualifications concerning security, service levels, and management needs for network service in agreements or contracts for internal or external network services. Finally, they must ensure partition of computer network systems suiting the need to access network systems, impacts of information security, and criticality of data on such networks.

(2) Information transmission control

Project owner units or units assigned to handle the Company information systems must institute control over data exchanged among units and affiliates of Bangchak Group as well as among the Company and external agencies. The criteria are as follows.

1. Digital and Information Technology (DI) must ensure proper work requirements for information and data exchange for the types of communication and confidentiality classes. It must also ensure written agreements are in place

concerning information and data exchange among units and affiliates of Bangchak Group as well as among the Company and external agencies.

2. DI must define measures for controlling electronic messaging, including E-mails, electronic data interchange (EDI), and instant messaging. Critical electronics messages must be properly protected from attempts to access or modify and from disruption from unauthorized parties.
3. Department managers must ensure that those personnel and agencies serving the Company sign written non-disclosure agreements (NDAs) over the Company data.

3.6) Prevention of threats to information systems

(1) Prevention of threats posed by malignant software

Project owner units or units assigned to handle the Company information systems must define measures for detection, prevention, and system restoration to prevent these assets from malignant software and must also raise proper awareness among users.

(2) Management of technical vulnerabilities

Project owner units or units assigned to handle the Company information systems must ensure that the Company information systems are proven against potential technical vulnerabilities under the following criteria:

1. Staging of penetration tests of critical work systems against untrusted networks, to be undertaken by third parties. Such tests must comply with risk and business impact analysis as follows:
   1.1 For work systems assessed to be highly critical, tests are required every three years and with each significant change to the systems.
   1.2 For other critical work systems, tests are required every five years.
2. Staging of vulnerability assessment for each critical work system at least annually and with each significant change to the systems. The outcomes are to be reported to applicable agencies for acknowledgment as well as formulation of corrective and preventive measures.
3. Staging of procedure and process tests for managing incidents that could impact the security of information systems at least annually. As a minimum, these tests must include cybersecurity drills.

3.7) Procurement, development, and supervision of information systems

Project owner units or units assigned to handle the Company information systems must institute proper requirements for procuring, developing, and supervision of information systems to minimize errors in setting out needs, design, development, and tests of newly developed or

newly modified information systems. They must also ensure that developed or procured work systems comply with agreements.

4) Standards for IT system security

DI must institute security standards for units that align with the announced IT system security policy and roll them out among all involved so that all may access, understand, and comply with these standards. It must also clearly assign responsible parties under such standards, which fall into the following aspects:

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. Operations security
9. 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) Policy revision

It is required that the IT Security Policy be revised at least annually or with each significant change. DI and related units must modify procedures and methods in line with each modified policy.

6) Publicity

All units are responsible for publicizing this policy as well as supporting and responding to this policy.

7) Reporting

All units are required to report their compliance with the IT Security Policy, rules, and requirements to the Board or Director of the company at least annually or with each incident potentially and significantly affecting such compliance, including computer systems or data facing damage or causing threats to the Company or any person(s) due to the omission, negligence, or violation of the IT Security Policy, rules, and requirements of the Company. The CEO is responsible for the risk, damage, or threats.

8) Enforcement

The IT Security Policy is enforced on Bangchak Sriracha Public Company Limited's employees, temporary contractors, and regular-hired contractors as well as external parties and agencies serving the Company. The effective date is the date after this announcement.

Mr. Bundit Hansapaiboon

Chief Executive Officer