# Information and Cyber Security Policy

**PURPOSE**

1. Protect information and related assets from a range of threats.
2. Maintain the confidentiality, integrity, and availability of the organization, customer and business partner information and resources.
3. Minimize business risks and maximize business opportunities related to information.

**SCOPE**

1. This policy applies to all information and systems that the organization owns or operates, and to all individuals who have access to these systems and data, including employees, contractors, consultants, volunteers, and third-party vendors.
2. This policy covers all IT systems, software, databases, applications, and network resources, whether on premises, cloud-based services, IoT, or managed, that the company uses to conduct business.

**POLICY STATEMENT**

**1. Identify**

1.1. Asset Management

1.1.1 Hardware Inventory

The organization will maintain a current inventory of all hardware, including type, manufacturer, model, serial number, firmware version, location or workforce members-assignment, in-service date, and retirement/disposal date. Inventories should be reviewed to ensure that all firmware versions are current and supported by the manufacturer with security updates. Manual or automated reports are acceptable. Acceptable file versions include a screen capture, .csv file, export from excel file, word document, spreadsheet, etc.

1.1.2 Software Inventory

The organization will maintain a current inventory of all software (including operating systems) including type, publisher, version, location or workforce members-assignment, in-service date, and retirement/disposal date. Inventories should be reviewed to ensure that all software versions are current and supported by the publisher with security updates. Manual or automated reports are acceptable. Acceptable file versions include a screen capture, .csv file, export from excel file, word document, spreadsheet, etc. Network Diagram & Communications Flow

1.1.3 Documentation

The organization will maintain a current and comprehensive network diagram that includes allowed ports, protocols, and services.

The organization will maintain documentation of the organization and clients' configurations, implementations, repairs, services, and related information for a time period of no less than seven years or as defined in federal, state, or industry regulations.

1.1.4 Network Diagram & Communications Flow

The organization will maintain current network diagrams.

- One diagram will include the physical network assets including their location, IP address, allowed ports, protocols and services.
- Another will be a logical diagram including the functions supported by each network device.
- Diagram organizational communications flows, including cloud services.
- Inventory cloud services and other external systems.
- Manual or automated diagrams are acceptable.
- Diagrams must be reviewed or updated quarterly.

1.1.5 Resource Classification

The organization must ensure that the organization's resources including hardware, devices, data, IoT, personnel, and software are prioritized for security based on their classification, criticality, and business value. This will help to ensure that the most important resources are protected from unauthorized access, use, disclosure, disruption, modification, or destruction.

Resources will be classified based on the following criteria:

• Sensitivity: The level of confidentiality of the resource.
• Criticality: The importance of the resource to the organization's operations.
• Business value: The financial or strategic value of the resource to the organization.

Resources will be prioritized based on their classification and business value. Resources that are classified as high-sensitivity, high-criticality, and high-business value will be given the highest priority. Resources that are classified as low-sensitivity, low-criticality, and low-business value will be given the lowest priority.

The organization will implement appropriate security controls to protect its prioritized resources from cyber security threats. These security controls will be commensurate with the risk posed by the threat and the value of the resource. security controls.

1.1.6 Security Responsibility

Employees are responsible for following all cyber security policies and procedures, and for reporting any suspicious activity to the security team.

Contractors, consultants, and volunteers are responsible for following all cyber security policies and procedures that are applicable to their work.

Suppliers are responsible for implementing appropriate security controls to protect the organization's data and systems.

Partners are responsible for implementing appropriate security controls to protect the organization's data and systems, and for complying with the organization's security policies and procedures.

The organization will appoint a Security Officer to lead and manage its cyber security program. The Security Officer will be responsible for the following:

• Developing and implementing policies, procedures, and controls to protect the organization's systems, data, and networks from cyber security threats.
• Overseeing the organization's cyber security posture and identifying and assessing risks.
• Developing and implementing mitigation strategies to reduce cyber security risks.
• Providing leadership and guidance to the organization's cyber security team.
• Communicating with senior management and the board of directors on cyber security risks and threats.
• Working with third-party vendors to ensure that their cyber security practices are aligned with the organization's requirements.
• Responding to cyber security incidents and restoring systems and data to their original state.
• Educating and training the workforce on cyber security best practices.

The organization will set up a security team which is responsible for ensuring the security of the organization's information and systems. This includes the following responsibilities:

• Developing and implementing security processes and procedures that define how the organization will protect its information and systems.
• Monitoring the organization's security posture to identify and assess security risks.
• Implementing security controls to mitigate identified security risks.
• Responding to security incidents to contain the damage and minimize the impact.
• Communicating security risks and incidents to management and other stakeholders.

1.2 Business Environment

The organization's role in the supply chain is identified and communicated. This includes the organization's position with clients, vendors, and partners.

The organization's place in critical infrastructure and its industry sector must be identified, documented, and communicated.

Priorities for the organization's mission, objectives, and activities must be established, documented, and communicated.

1.3 Governance

1.3.1 Security Policy

This security policy must be reviewed by the organization's management each year and updated as necessary. The policy and any changes must be communicated to all workforce members.

Exception to the policy shall be documented to ensure transparency, accountability and consistency in decision making process.

1.3.2 Client Security

Only workforce members authorized by the organization's management may access client systems, and only for authorized purposes.

Authorized workforce members must only use access control systems approved by the organization to access client sites and data. Access is limited admin rights to a maximum of 7 days ensures that privileged access is granted only for legitimate, time-sensitive operational needs and is revoked promptly to maintain a strong security posture.

Information and Cyber Security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.

The organization workforce members are required to maintain confidentiality of client information as if it was the organization information.

Specifically,

- Workforce members will only access client sites and data using approved mechanisms.
- No protected information may be removed from the client site by physical or electronic means without specific authorization by the organization's management.
- No information overheard or seen at customer sites may be shared for purposes other than those authorized by the organization.
- Workforce members will be trained in all regulations appropriate to their work with clients.
- Workforce members will be subject to all civil and criminal penalties for non-compliance with regulations required of clients.

Any client information protected by federal, state, or industry regulations must be managed in accordance with those regulations.

1.3.3 Roles and Responsibilities

Information and Cyber Security roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) must be established and documented.

1.3.4 Compliance

The organization will comply with all applicable laws and regulations, including:

- Relevant Digital Laws
- Industry Regulations
- Contracts
- Insurance Policy Requirements

Legal and regulatory requirements regarding cyber security, including privacy and civil liberties obligations, must be understood and managed. Governance and risk management processes will address cyber security risks.

Copyright Protection and Software License:

To minimize the risk of legal exposure, this policy is to outline the requirements around installation software on Banpu computing devices.

- You must read understand any software copyright restrictions. If you think that Banpu will not be able to comply with any part of the terms, do not download or use the material.
- Ensure that you comply with any expressed requirements or limitations to the use of such software.
- Software requests must be approved by the requester's manager and then be made to the IT department or Service Desk in writing.
- Software must be selected from an approved software list unless no selection on the list meets the requester's need.

1.4 Risk Assessment

The Security Officer must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of organization data. All organizational resources, including devices, removable media, and cloud platforms must be included.

The organization must subscribe or receive cyber threat intelligence from information sharing forums, sources, or managed security service providers.

A comprehensive analysis of security threats must be conducted at least every three years. It must be reviewed annually and updated as needed.

The risk analysis must comprehensively describe the organization’s information system, including identifying and documenting the following components:

- The computer hardware and software that make up the organization's information system.
- The categories and qualifications of workforce members who use the system.
- The functions and activities that are supported by the information system.
- The data and information that are collected, processed, and stored by the information system.
- The physical environment that houses information system components.
- On-site and off-site storage of information.
- The organizations to which information is transmitted.
- The data and information that are transmitted to other organizations.
- The internal and external connections between the organization's information system and the information systems of other organizations.
- The risk analysis must identify threats to the security of the organization's company data, including natural, human, and environmental threats. The risk analysis must identify the nature of each threat or vulnerability and how each may damage information security.

The risk analysis must indicate the preventive measures that the organization has implemented (or is planning to implement) to limit the damage that might be caused by each threat or vulnerability.

The risk analysis must evaluate the likelihood and the impact that each security threat or vulnerability might occur.

The risk analysis must describe the nature and extent of the damage each threat might cause to the integrity, availability, and confidentiality of the organization's information resources.

The risk analysis must identify high-priority threats that are the focus of risk-management efforts.

The risk analysis must recommend controls or actions to lessen the risk associated with high-priority threats. The risk analysis must be reviewed and approved by the Security Officer.

The results of the risk analysis must be shared with other members of the organization management team.

1.5 Business Continuity Plan

The organization will develop a comprehensive written plan to continue business during, or resume business immediately after, a disruption or disaster. This plan must go beyond the tasks required to recover the organization's IT infrastructure, and include a:

- Risk Analysis identifying potential risks and mitigation strategies.
- Business Impact Analysis to identify the organization's functions and the effect of critical functions.
- Communications Plan to contact workforce members, customers, and vendors.
- An alternate site plan if the organization's company facilities are not available.
- Ability to redirect incoming phone calls; e-mail; access to the organization's on-line resources.
- Ability to continue critical services to customers.
- Ability to continue critical technology functions.
- Recovery strategies based on the Risk Assessment and Business Continuity Plan

1.6 Risk Management

The organization has the corporate risk management process, risk response, and risk tolerance that includes cyber security. All risk management refers to those parts of the organization.

Some entities in our group of companies those are defined as businesses in critical infrastructure must develop risk management according to sector specific risk.

1.7 Supply Chain Risk Management

The organization will develop a process for managing cyber supply chain risks associated with acquisition, delivery, integration, operations and maintenance, and disposal of the information systems and services program to implement and sustain the capability to:

- Assess and provide appropriate risk response to cyber risks that arise from the acquisition and use of covered articles.
- Prioritize assessments of cyber risks throughout the supply chain and risk response actions based on critical assessments of the mission, system, component, service, or asset.
- Develop an overall cyber security supply chain risk strategy and high-level implementation plan, policies, and processes.
- Integrate supply chain risk management practices throughout the acquisition and asset management life cycle.
- Include critical suppliers in contingency planning, incident response, and disaster recovery planning and testing.

Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts to meet the objectives of an organization's cyber security program and cyber supply chain risk management plan. Third- party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.

**2. Protect**

2.1 Identity Management, Authentication and Access Control

2.1.1 Account Management The organization shall:

- Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.
- Assign account managers for information system accounts.
- Establish conditions for group and role membership.

• Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
• Require approvals by system owners for requests to create information system accounts.
• Create, enable, modify, disable, and remove information system accounts in accordance with approved procedures.
• Monitor the use of information system accounts.
• Notify account managers when accounts are no longer required, when users are terminated or transferred, and when individual information system usage or need-to-know changes.
• Authorize access to the information system based on a valid access authorization or intended system usage.
• Review accounts for compliance with account management requirements annually.
• Establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
• Employ automated mechanisms to support the management of information system accounts.
• Ensure that the information system automatically disables temporary and emergency accounts after usage.
• Ensure that the information system automatically disables inactive accounts after 30 days.
• Ensure that the information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies appropriate IT personnel.

2.1.2 Physical Access Control

The organization shall:
• Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides.
• Issue authorization credentials for facility access.
• Review the access list detailing authorized facility access by individuals annually; and
• Remove individuals from the facility access list when access is no longer required.
• All unauthorized persons or external parties must be authorized to enter restricted areas by the appropriate personnel. Authorization shall be based on a documented need to access the restricted area and a review of the external party's security clearance.
• All unauthorized persons or external parties must be escorted by authorized personnel while in restricted areas. Escorts shall be responsible for ensuring that external parties comply with all security requirements.

2.1.3 Remote Access

The organization shall:
• Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed.
• Authorize remote access to the information system prior to allowing such connections.
• Ensure that the information system monitors and controls remote access methods.
• Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
• Ensure that the information system routes all remote accesses through limited managed network access control points to reduce the risk for external attacks.
• Authorize the execution of privileged commands and access to security-relevant information via remote access only for IT support.
• Document the rationale for such access in the security plan for the information system.
For IT user support purposes, remote access to the endpoint must be allowed or approved from the approver or owner of that asset. On each remote connection request, the end user or authorized person must authorize or allow the connection to be established.

2.1.4 Least Privilege and Separation of Duties The organization shall:

- Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
- Authorize explicitly access to hardware and software controlling access to systems and filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists.
- Separate duties of individuals as necessary, to prevent malevolent activity without collusion.
- Document the separation of duties of individuals.
- Define information system access authorizations to support separation of duties.

2.1.5 Privileged Accounts

The organization shall ensure that the information system:

- Limit privileged and administrative access to authorized users who require escalated access for their job responsibilities and where possible those users will have two accounts: one for administrative functions and a standard account for day-to-day activities.
- Privileged accounts must be reviewed at least quarterly to verify the Continued business need
- Ensure that the information system audits the execution of privileged functions.
- Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

2.1.6 Network Access Control

The organization must establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

The organization must establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

2.1.7 Account Identity Verification

The organization must establish robust identity proofing procedures. This may include multiple steps such as user registration, verification of physical identity (e.g., via documents), and creation of digital credentials (like usernames or access tokens).

The organization must uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

The organization shall uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

The verified identities need to be bound to credentials with authenticators (like passwords or software generated OTP) using a secure, tamper-resistant process. During each interaction to the system, users' authenticators should be asserted to confirm they are indeed the person tied to those credentials.

This policy will not be applied to service or system accounts.

2.1.8 Access Enforcement

The organization must ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

The organization must ensure that the information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on applicable policy.

2.1.9 User Authentication

All systems housing the organization's data (including laptops, desktops, tablets, and other devices) are required to be protected with a password or other form of authentication. Except for the instances noted in this policy, users with access to the organization's systems and data are not allowed to share passwords with anyone.

The organization has established following password configuration requirements for all systems and applications (where applicable):

• Minimum password length: 12 characters
• Password complexity: contains a mixture of numbers, special characters and both uppercase and lowercase letters.
• Prohibited reuse for five (4) iterations.
• Change, if compromised
• Invalid login attempts set to five.
• Automatic logout due to inactivity = 30 minutes

The organization will enhance the security of systems and protect sensitive data by implementing multi-factor authentication (MFA) with these conditions:

• All new systems must use MFA for user authentication. This means that users must provide two or more factors to log in to the system.
• Legacy systems are exempt from the MFA requirement. However, there must be an annual review of whether the MFA can be implemented for legacy systems and plan to adopt as soon as practicable.
• The organization will declare the valid factors of authentication and combination of those factors.

The organization will also establish the main identity management system which prefers to being used among organization's systems.

2.2 System Use Notification

The organization shall ensure that the information system:

• Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:
• Users are accessing an organization's information system.
• Information system usage may be monitored, recorded, and subject to audit
• Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.
• Use of the information system indicates consent to monitoring and recording.
• There are no rights to privacy.
• Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system.
• For publicly accessible systems, the organization shall ensure that the information system:
• Displays system use information, before granting further access.
• Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities.
• Includes a description of the authorized uses of the system.

2.3 Awareness and Training

The organization's personnel are required to participate in security training in the following instances:

• All new hires are required to complete security awareness training before receiving login credentials.

• Formal security awareness refresher training is conducted on an annual basis. All employees are required to participate in and complete this training.

On an annual basis, the organization will conduct email phishing exercises for its users. The purpose of these tests is to help educate users on common phishing scenarios. It will assess their level of awareness and comprehension of phishing, understanding and compliance with policy around safe handling of emails containing links and/or attachments, and their ability to recognize a questionable or fraudulent message.

The organization should have addition awareness training for these groups of personnels according to their roles and responsibilities:

• Privileged users
• Third-party stakeholders (e.g., suppliers, customers, partners)
• Senior executives
• Physical and cyber security personnels

2.4 Data Security

2.4.1 Data Classification

Data residing on corporate systems must be continually evaluated and classified into the following categories:

• Employees Personal Use: Includes individual user's personal data, emails, documents, etc. This policy excludes an employee's personal information, so no further guidelines apply.
• Marketing or Informational Material: Includes already-released marketing material, commonly known information, data freely available to the public, etc. There are no requirements for public information.
• Operational: Includes data for basic organizational operations, communications with vendors, employees, etc. (non-confidential). Most data will fall into this category.
• Confidential: Any information deemed confidential. The following list provides guidelines on what type of information is typically considered confidential. Confidential data may include:
• Employee or customer Social Security numbers or personally identifiable information (PII)
• Financial data (for public company listed in stock market, refer to data those are not officially publish to the public)
• Personnel files
• Medical and healthcare information
• Company, federal, or business information
• Network diagrams and security configurations
• Communications regarding legal matters
• Account credentials such as user account login information, including usernames, passwords, and emails
• Bank account information and routing numbers
• Payroll information
• Credit card information
• Trade secrets and intellectual property (IP)
• Any confidential data held for a third party (be sure to adhere to any confidential data agreement covering such information)

2.4.2 Data Storage

Stored Data includes any data located on organization-owned or organization-provided systems, devices, media, etc. The following guidelines apply to the storage of the different types of organizational data.

• Operational data should be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). Some type of system- or disk-level redundancy is encouraged.
• Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard or code secured.

2.4.3 Data Transmission

The following guidelines apply to the transmission of the different types of organizational data.
• Confidential data must not be transmitted outside the organization's network without the use of strong encryption.
Data while transmitted includes any data sent across the organization network or any data sent to or from an organization-owned or organization-provided system. Types of transmitted data that shall be encrypted include:
• VPN tunnels
• Remote access sessions
• Web applications
• Email and email attachments
• Remote desktop access
• Communications with applications/databases

2.4.4 Data Destruction

You must follow your records retention policy before destroying data.
• Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:
• Paper/documents: Cross-cut shredding is required.
• Storage media (CD's, DVD's): Physical destruction is required.
• Hard drives/systems/mobile storage media: At a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the organization must use the most secure commercially available methods for data wiping. Alternatively, the organization has the option of physically destroying the storage media.

2.4.5 Storage Capacity Management

The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

2.4.6 Data Protection

a) Data Protection

To prevent data leakage, the organization must provide sufficient access control for all operational and confidential data. The organization will use proper encryption for confidential data where the access control is considered insufficient.
• IT Admin will not take any action on the information without the permission of the information owner.
• IT Admin will make sure that there are proper safeguards in place to recover from any disaster.
• IT Admin should maintain proper documentation of all activities involving the information owner.
• IT Admin will inform the information owner of any risk or shortcomings as they are identified.

b) Data Protection using cloud platform

To provide the proper control of the scalable computing resources technology.
• Acquiring/Deploying on Cloud Computing should be authorized by Head of Digital Team or representatives.

• Any software computing issues, and all related laws should be assured, recorded, and monitored.
• Administrative privileges, identifies, billing information, and relevant security credentials to cloud services should be stored as separately backup and reviewed on a timely basis.
• Ensure how disaster recovery and continuity of service are addressed.
• Ensure your service development model (private access, public access) are protected align with the business requirement.
• Enable data encryption feature to secure data in Transit, and data at Rest.
• Manage access by using Role-Based Access Control (RBAC)
• Enable Access Log for regularly audit access.
• Prepare cloud provider exit plan with these key considerations:
• How will data be migrated out of the cloud provider? Will there be an additional cost?
• How will unwanted data be securely erased? What kind of proof and audit trail?
• What are the obligations of each party regarding an exit plan?

2.4.7 Software and Information Integrity

All employees are responsible for maintaining the integrity of data in their possession or under their control. This includes ensuring that data is accurate, complete, and consistent; that it is protected from unauthorized access, use, disclosure, modification, or destruction; and that it is disposed of properly when no longer needed.

The organization data owners are responsible for defining the data requirements for their business area and for ensuring that the data is collected, stored, processed, and used in a manner that meets those requirements.

Data owners are also responsible for developing and implementing data security and integrity procedures.

The organization will provide the technical infrastructure and support necessary to ensure the integrity of data. This includes implementing security measures to protect data from unauthorized access, use, disclosure, modification, or destruction; and developing and implementing data backup and recovery procedures.

The organization will employ integrity verification tools to detect unauthorized changes to source code, software and firmware used in the organization.

Installation or use of unauthorized or pirated software is strictly prohibited and the authorized software must be regularly updated with the latest security patches.

The company shall monitor Internet usage from all devices connected to the corporate network, and the usage records must be preserved for a period of time required by law and privacy consideration.

2.4.8 Non-Production Data

The organization will ensure that production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.

2.4.9 Hardware Integrity

The organization must implement at least one mechanism to check the integrity of each piece of hardware it uses. This mechanism must be able to generate a unique signature for each piece of hardware and compare the current signature to the stored signature to detect unauthorized changes. The organization must also implement a process to regularly check the integrity signatures of all hardware components.

2.4.10 Data Masking

The organization has to ensure the purpose of utilizing or disclosing information should be determined based on the necessity of accessing or using that particular set of data, such as compliance with laws, adherence to relevant contracts, or conformity with standards that the organization is required to follow. Data should be obscured to reveal only what is strictly necessary.

2.4.11 Web Filtering

a) Acceptable Use of Internet

• Internet access is provided for business use only. Limited personal use is allowed, provided it does not interfere with work duties or violate security policies.

b) Web Filtering Implementation

• Web filtering technology must be deployed on all networks to monitor and restrict access to harmful or non-compliant web content.

• Internet traffic must be routed through secure, managed gateways with logging and inspection capabilities.

c) Blocked Web Categories

The following categories must be blocked by default:

• Malware and Phishing Sites
• Pornographic or Adult Content
• Gambling and Betting
• Illegal or Copyright-Infringing Content
• Hate Speech or Extremist Sites
• Weapons or Violence Promotion
• Anonymous Proxies or VPNs
• Unauthorized Cloud Storage or File-Sharing Services
• Cryptomining or Hacking Tools

d) Monitoring and Logging

• All user web access will be logged and monitored.

• Logs will be retained for a minimum of 3 months (or longer as required by regulation) and reviewed
periodically.

• Anomalies or potential violations will trigger alerts to the security operations team.

e) Exceptions and Whitelisting

• Temporary or permanent access to restricted sites must be requested through IT.
• All exceptions must be documented and regularly reviewed.

f) User Responsibilities

• Users must not attempt to bypass web filtering mechanisms.

• Any suspected access to malicious websites or phishing attempts must be reported immediately to the IT Helpdesk or Security team.

2.5 Information Protection Processes and Procedures

2.5.1 Baseline Configuration The organization must:

• Develop, write down, and keep under configuration control a current baseline configuration for all information systems.

• Review and update the baseline configuration annually, and when required by audits or as part of installing or upgrading information system components.

• Keep one previous version of the baseline configuration for each information system to support rollback.

2.5.2 System Development Life Cycle The organization shall:

• Acquire, develop, and manage the system that incorporates information security and privacy considerations;

• Define and document information security and privacy roles and responsibilities throughout the system development life cycle;

• Identify individuals having information security and privacy roles and responsibilities; and

• Integrate the organizational information security and privacy risk management process into system development life cycle activities.

2.5.3 Configuration Change Control The organization must:

• Identify the types of changes to information systems that are subject to configuration control.

• Review proposed configuration-controlled changes and approve or disapprove them, taking into account security impact analyses.

• Document configuration change decisions.

• Implement approved configuration-controlled changes.

• Keep records of configuration-controlled changes for at least one year.

• Audit and review activities related to configuration-controlled changes.

• Coordinate and oversee configuration change control activities through a designated configuration change control entity (e.g., committee, board) that meets at and [conditions].

2.5.4 Data Backup

The organization must regularly back up its information, software, and system images, in accordance with its own requirements. It must also regularly test its backup and restore procedures. Separation of duties must be used for these functions.

2.5.5 Physical Operating Environment

The organization must develop, write down, and share a physical and environmental protection policy that covers its purpose, scope, roles and responsibilities, management commitment, coordination among different parts of the organization, and compliance with all relevant laws, executive orders, directives, regulations, policies, standards, and guidelines. The policy must also include procedures to help implement the physical and environmental protection policy and its associated controls.

2.5.6 Data Destruction

The organization will establish approved methods for destroying electronic media (hard drives, CDs, USB drives), paper documents (shredding, burning), and equipment that contains confidential data.

2.5.7 Protection Improvements

The organization will establish a protection improvement process that involves updating security policies and procedures, deploying new security controls, or improving existing controls.

2.5.8 Sharing Effectiveness of Protection

The organization must enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for auditing, regulatory requirements, cyber security incident management and lesson learned.

2.5.9 Response Plans and Recovery Plans

The organization shall develop response plans for incident response and business continuity that could be tailored to its specific needs and address the following:

• Identification and classification: How to identify and classify incidents and disruptions.

• Notification and escalation: How to notify and escalate incidents and disruptions.

• Mitigation and containment: How to mitigate and contain incidents and disruptions.

• Recovery: How to recover from incidents and disruptions.

• Communication and coordination: How to communicate and coordinate during incidents and disruptions.

Response plans shall be reviewed and updated regularly and tested regularly to ensure their effectiveness.

2.5.10 Personnel Security

The organization must develop a personnel security program that includes the following:

• Background checks for new employees and contractors.
• Security clearances for employees with access to sensitive information or systems.
• Access control procedures for employees and contractors.
• Security awareness training for employees and contractors.
• Disciplinary procedures for employees who violate security policies and procedures.

The personnel security program must be reviewed and updated regularly.

2.5.11 Vulnerability Management Program

The organization shall develop a vulnerability management program that includes processes for identifying and assessing, prioritizing, remediating, and monitoring vulnerabilities.

The vulnerability management program shall be reviewed and updated regularly.

2.6 Maintenance

The organization must perform regularly scheduled maintenance of all assets to help identify potential issues before they become significant problems, ensuring the smooth operation of the entire system.

To protect assets from unauthorized access, use, disclosure, disruption, modification, or destruction, organizations must ensure that maintenance and repairs of industrial control and information system components are performed securely. This requires establishing an approval process for all maintenance and repair requests.

For remote maintenance, the organization must develop policies and procedures that cover these criteria including (but not limited to) allowed activities, personnel qualification, security controls, monitoring, and audit trails.

All maintenance and repair work must be documented in a timely and accurate manner. Documentation must include date/time, type performed, personnel, tools/equipment, and any observations.

2.7 Protective Technology

2.7.1 Audit/Logs

The organization must develop audit/log record management policies and procedures that address the types that will be created and maintained, the security controls, the reviewing procedures, and the archiving procedures.

The audit/log record management policies and procedures shall be reviewed and updated regularly.

2.7.2 Removable Media

The organization must ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

The organization will implement removable media management procedures in accordance with the organization's data classification.

2.7.3 Principle of Least Functionality (POLF)

To reduce the attack surface of systems by disabling unnecessary functionality, organizations must develop principle of least functionality (POLF) policies and procedures that cover the following:

• Identifying and documenting unnecessary functionality on systems
• Disabling or removing unnecessary functionality from systems
• Monitoring systems for new functionality and assessing its necessity

2.7.4 Communications and Control Network Protection

The organization shall implement the following security controls on all communications and control networks:

• Networks shall be segmented to isolate different types of traffic and reduce the risk of unauthorized access and compromise.

• All users and devices shall be authenticated and authorized before accessing communications and control networks.

• All sensitive data transmitted over communications and control networks shall be encrypted to protect it from unauthorized access.

• Intrusion detection and prevention systems (IDS/IPS) shall be deployed to monitor communications and control networks for suspicious activity.

• Communications and control networks shall be scanned regularly for vulnerabilities to identify and remediate them before they can be exploited by attackers.

The organization shall develop and implement a process for incident response to detect and respond to security incidents on communications and control networks.

The organization shall provide training to all employees on the organization's communications and control network protection policies and procedures.

2.7.5 System Resiliency

To ensure that systems are resilient to failures and disruptions, the organization must:

• Develop resilience requirements for all systems.

• Implement mechanisms to achieve those requirements.

• Test resilience mechanisms regularly.

• Review and update resilience requirements and mechanisms regularly.

**3. Detect**

3.1 Anomalies and Events

The organization will establish baselines for all critical systems and processes. Baselines are sets of normal operating parameters that are used to identify anomalies.

The organization will establish processes to detect and analyze anomalies using automated and manual methods. Automated methods may include monitoring system logs and metrics for deviations from baselines. Manual methods may include investigating systems and processes for unusual activity. The detection and analysis processes must include these activities:

• Anomalies will be correlated to identify related events. This may involve analyzing multiple systems and processes to see if they are exhibiting similar anomalous behavior.

• The impact of anomalies will be assessed to determine the level of response required. The impact of an anomaly may include financial loss, disruption to operations, or damage to data.

• Thresholds will be set for anomalies to determine when further investigation or action is necessary. Thresholds may be based on historical data, expert judgment, or risk assessment.

3.2 Security Continuous Monitoring

3.2.1 Network

The organization will continuously monitor its network traffic for anomalous and suspicious activity. This includes using intrusion detection and prevention systems (IDS/IPS) to detect and block malicious traffic, and security information and event management (SIEM) systems to correlate events and identify potential threats.

3.2.2 Physical Environment

The organization will continuously monitor its physical security systems, such as access control and video surveillance, for unauthorized activity. This includes:

• Monitoring access control logs to identify unauthorized entries and exits.

• Monitoring video surveillance footage to identify suspicious activity, such as people loitering or tampering with equipment.

• Conducting regular physical security audits to identify and address vulnerabilities, such as unsecured doors and windows, or weak perimeter security.

3.2.3 Personnel Activity

The organization will monitor employee accounts for suspicious activity, such as unusual logins or access to sensitive data.

3.2.4 Malicious Code

The organization will continuously monitor its systems for malicious code using antivirus and antimalware software, keeping software up to date with the latest security patches, and implementing security controls to prevent malicious code from being introduced into its systems.

3.2.5 Unauthorized Mobile Code

The organization will implement policies and procedures to monitor and prevent unauthorized mobile code from being installed on its devices and educate employees on the risks of unauthorized mobile code.

3.2.6 External Service Provider Activity

The organization will monitor the activity of its external service providers for the following potential cyber security events such as abnormal network traffic, unauthorized access attempts, data breaches, malware infections, and denial-of-service attacks.

3.2.7 Unauthorized Access

The organization will monitor for unauthorized personnel, connections, devices, and software by using a variety of methods, including:

• Network monitoring: The organization will monitor network traffic for unusual activities, such as unauthorized connections or excessive traffic from a single source.

• Device monitoring: The organization will monitor devices that connect to its networks and systems for unauthorized activity, such as unauthorized software installations or unusual file activity.

• Software monitoring: The organization will monitor software on its networks and systems for unauthorized activity, such as malicious code or unauthorized access to sensitive data.

• User activity monitoring: The organization will monitor user activity on its networks and systems for unauthorized activity, such as unusual login attempts or excessive access to sensitive data.

3.2.8 Vulnerability Scan

The organization will monitor and scan for vulnerabilities in the system and hosted applications at least quarterly and/or randomly in accordance with organization-defined process and when new vulnerabilities potentially affecting the system are identified and reported.

3.3 Detection Processes

3.3.1 Roles and Responsibilities

The security team is responsible for developing, implementing, and maintaining the organization's detection processes. The security team is also responsible for investigating and responding to security incidents.

IT staff is responsible for configuring and maintaining the organization's security systems and tools. IT staff is also responsible for assisting the security team with investigations and responses.

All employees are responsible for reporting suspicious activity to the security team. Employees should also be aware of the organization's detection processes and how to report security incidents.

3.3.2 Activities

The organization's detection processes will include the following activities:

• Monitoring: The organization will monitor its networks, systems, and applications for suspicious activity. This may involve monitoring network traffic, system logs, and application logs.

• Alerting: The organization will use security systems and tools to generate alerts when suspicious activity is detected.

• Investigation: The security team will investigate alerts to determine whether a security incident has occurred.

• Response: The security team will take appropriate action to mitigate the impact of a security incident.

3.3.3 Process Testing

The security team will test its detection processes using a variety of methods, including penetration testing, vulnerability scanning, threat simulation and test case scenarios.

The security team will test the detection processes on a regular basis, at least quarterly. The security team may also need to test the detection processes more frequently if there are significant changes to the organization's security posture or to the detection mechanisms themselves.

3.3.4 Communication Plan

The organization will establish communication plan for event detection information will include the following:

• Identifying the personnel who need to be notified of event detection information based on their roles and responsibilities.

• Determining the communication channels that will be used to notify personnel of event detection information.

• Developing communication templates for different types of event detection information such as suspicious activity, security incidents, and vulnerabilities.

• Training personnel on how to communicate event detection information.

When the security team detects an event, the security team will communicate the information to the appropriate personnel using the communication channels that have been established. The communication will include type of event, severity, and recommended course of action.

3.3.5 Improvement

The organization will continuously improve its detection processes by conducting security incident reviews, tool evaluation, and procedure testing.

**4. Response**

4.1 Response Planning

The organization will develop an incident response plan that:

• Provides a roadmap for implementing and maturing the organization's incident response capability.

• Defines the structure, organization, and role of the incident response capability within the organization.

• Meets the organization's unique requirements, such as its mission, size, structure, and functions.

• Specifies reportable incidents and metrics for measuring the incident response capability's effectiveness.

• Defines the resources and management support needed to maintain and improve the incident response capability.

• Describes how incident information will be shared.

• Is reviewed and approved by authorized personnel on a regular basis.

• Explicitly assigns responsibility for incident response to specific entities, personnel, or roles.

The organization will establish Cyber Security Incident Response Team (IRT) which will work on clearly defined roles and responsibilities as a virtual team. The IRT will include the Security Officer, head of the security team, head of the information technology department and functional roles such as finance, legal, communication, and operations. The organization will establish criteria to activate the IRT according to the response plan.

4.2 Communications

The organization will develop a communication plan that will define the following:

• Who will be notified of the incident?
• When will stakeholders be notified?
• What information will be shared with stakeholders?

The organization will also define the communication channels that will be used to communicate with stakeholders. This may include email, phone, and social media.

When a cyber security incident is detected, the security team will initiate the response communications process.

The security team will communicate with internal stakeholders throughout the incident response process, including management. The IRT will be responsible for making statements to external stakeholders, such as customers and law enforcement agencies.

The security team will communicate with internal stakeholders to keep them informed of the incident and to obtain their input on the response. The security team will communicate with internal stakeholders on a regular basis and will provide them with updates on the status of the incident, the steps that are being taken to respond, and the impact of the incident on the organization.

The incident response team (IRT) will communicate with external stakeholders through designated individuals to keep them informed of the incident and mitigate its impact on the organization's reputation. Designated individuals will communicate with external stakeholders in a timely and transparent manner, providing accurate information about the incident.

4.3 Analysis

The organization will conduct timely and thorough analysis of cyber security incidents to ensure effective response and support recovery activities.

When a notification is received from a detection system, the security team will investigate the notification to determine whether it represents a security incident.

In case the result of investigation indicates a potential cyber security incident, the security team will analyze the incident to ensure effective response and support recovery activities. This analysis will include collecting and analyzing data from a variety of sources, determining the type of incident, the systems and data affected, the scope of the incident, the method used to exploit the vulnerability, and the impact of the incident on the organization.

When a cyber security incident occurs, the security team will assess the need for forensic analysis. If forensic analysis is required, the security team will follow the organization's forensic analysis procedures.

The security team will also develop a hypothesis about how the incident occurred and who was responsible, and test and refine this hypothesis as needed. The results of the analysis will be used to develop a response plan and to support recovery activities.

4.4 Mitigation

When a cyber security incident occurs, the security team will initiate the mitigation process. The security team will follow the organization's mitigation procedures to prevent the expansion of the incident, mitigate its effects, and resolve the incident. The mitigation procedures will include the following steps:

1. Identify affected systems: The security team will identify the systems that are affected by the incident.

2. Contain the incident: The security team will take steps to prevent the incident from spreading to other systems.
3. Eradicate the threat: The security team will remove the threat from the affected systems.
4. Recover the affected systems: The security team will restore the affected systems to their normal state.
5. Investigate the incident: The security team will investigate the incident to determine the root cause and to identify any lessons learned.

The security team will document its findings from the mitigation effort. The security team will also provide a report of its findings to management and to other stakeholders as needed.

When a new vulnerability is found, the security team will assess its severity and impact, taking into account the organization's risk appetite and tolerance. Based on this assessment, the team will recommend whether to mitigate the vulnerability or accept it as a risk. If mitigation is recommended, the team will develop a plan and submit it to management for approval.

4.5 Improvements

After each cyber security incident, the security team will conduct a post-incident review to identify lessons learned. The post-incident review will include the root cause of the incident, gaps in the organization's detection/response capabilities, and areas where the organization can improve its response processes.

The security team will document the lessons learned from the post-incident review and share them with the organization's incident response team (IRT). The IRT will review the lessons learned and develop recommendations for improving the organization's response strategies and activities.

The IRT will present their recommendations to management for approval. Management will then implement the recommendations and monitor the effectiveness of the improvements.

**5. Recover**

5.1 Recovery Planning

The security team will develop recovery processes and procedures for all critical systems and assets. The recovery processes and procedures will include the following steps:

1. Identify the systems and assets that are critical to the organization's operations
2. Assess the risks to the systems and assets.
3. Develop recovery plans for each system and asset.
4. Test the recovery plans on a regular basis.
5. Maintain the recovery plans up to date.

The recovery plans will include the following information:

• The steps that need to be taken to restore the system or asset to its normal state.
• The resources that will be needed to restore the system or asset.
• The personnel who will be responsible for restoring the system or asset.

The security team will also develop and implement a process for incorporating lessons learned into the recovery processes and procedures. The lessons learned will be identified from post-mortems of cyber security incidents and from other sources.

5.2 Communications

The IRT will work with the public relations department to develop and implement a public relations plan for each cyber security incident. The public relations plan will include the following:

• A statement to be released to the media
• A messaging strategy for communicating with customers and other stakeholders
• A plan for responding to media inquiries

The IRT will also work with the public relations department to monitor social media and other online channels for mentions of the incident.

The IRT will work with the public relations department to develop and implement a reputation repair plan. The reputation repair plan will include the organization's key stakeholders, the impact of the incident on the organization's reputation, a messaging strategy to address the concerns of stakeholders and implementing actions to demonstrate the organization's commitment to security.
The security team will communicate recovery activities to internal stakeholders as well as executive and management teams on a regular basis. The communication will include the following:

- The status of the recovery effort
- Any known impacts of the incident
- The steps the organization taking to mitigate the impact of the incident
- The timeline for recovery

The security team will also provide updates to executive and management teams on the progress of the recovery effort and any potential risks or challenges.

(Mr. Chanin Vongkusolkit)
Chairman of the Board of Directors
Banpu Public Company Limited

(Mr. Sinon Vongkusolkit)
Chief Executive Officer
Banpu Public Company Limited