Policy

Information and Cyber Security

Revision	00
Effective Date	*2021-04-30*
Process Owner	Health, Safety, Environment and Community Engagement

Document Revision Control				
Revision	Author	Effective Date	Change Description	Ref. Doc no.
00	mingkwan_k	2021-04-30	This policy has been approved in BOD Meeting on 30 April 2021.	BPP-AM-PO-002

Approval Record		
Approver	Job title	Date
Somruedee Chaimongkol	Chief Executive Officer	2021-05-12
Kirana Limpaphayom	Chief Executive Officer - BANPU Power	2021-05-12
Praphan Likitwacharapakorn	Chief Operating Officer - Power Business	2021-05-12
Issara Niropas	Vice President - Asset Management	2021-05-10

Introduction:

Digital Transformation is the company's strategic direction, and digital technology is the foundation for the business transformation process. Adopting new technology also introduces new risks to balance security with digital transformation.

Objective:

This policy is designed for the organization-wide benefit of active digital technology related usage and its operation and ensure compliance with the relevant legislation and agreements with third parties.

Scope:

This policy applies to all employees in Banpu Power and subsidiary companies including third parties who access Banpu Power's Digital resources.

Enforcement

Head of Information Technology will document cases of violation in order to maintain company integrity. Any employees in violation of these policies is subject to disciplinary action, including but not necessarily limited to termination.

Definitions:

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability (CIA)

Confidentiality

which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity

which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Availability

which means ensuring timely and reliable access to and use of information.

Cybersecurity

Cybersecurity means protecting the things which are vulnerable through information and communication technologies (ICT); it includes information, both physical and digital, and non-information such as vehicles, electronic appliances, etc.

Data Privacy

Data privacy is the right of a person to control how personal information is collected and used.

Policy Statement / Principles:

1. Clean Desk Policy: - The Basic step of Security and Privacy controls

To establish the minimum requirements for maintaining a “clean desk” – where sensitive/confidential information is secure in locked areas and out of site. It is a part of standard basic privacy controls.

1) Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day.

2) Any sensitive/confidential information must be removed from the desk and locked in a drawer when the desk is unoccupied, and at the end of the day.

3) File cabinets containing sensitive/confidential information must be kept closed and locked when not in use or when not attended.

4) Printouts containing sensitive/confidential information should be immediately removed from the printer.

5) Whiteboards containing Restricted and/or Sensitive information should be erased.

2. Computing Devices

2.1 Company Owned Devices

The following security controls must be activated on all personal accountabilities:

1) The device should comply with company standard specification and configuration.

2) The software must be provided and installed by the IT Department.

3) The user should NOT attempt to change or disable any security settings applied to the device.

2.2 Personally Owned Devices — BYOD

Banpu Power will permit the use of personally owned devices, subject to the following requirements:

1) Users must allow the installation of Mobile Device Management (MDM) software.

2) The use of jailbroken or rooted devices is not permitted and constitutes a material breach of policy.

3) Users must accept that Banpu Power’s security policy will be enforced on the device.

4) Users are responsible for backing up all personal information.

5) Banpu Power will never access sensitive personal information from user devices. The MDM software does NOT collect the following information from personal devices:

- Keystroke activity
- Internet usage outside of the company-provided secure browser software.
- Access to photos
- The ability for IT to read user emails sent or received from personal accounts.

Banpu Power’s is committed to protecting user privacy while enforcing only those policies required to protect the organization's data, intellectual property, and computer and network systems.
Banpu Power has implemented management software that provides for separation of business and personal data. Every effort will be made to focus management only on organizational apps and data.

2.3 Internet of Things Devices (IoT)

The Internet of things (IoT) is the network of physical devices, vehicles, home appliances, and other

items embedded with these components, which enables these objects to connect and exchange data.

- Electronics ·
- Software
- Sensors
- Actuators
- Connectivity

Banpu Power will permit the Internet of Things (IoT) devices, subject to the following security requirements:

1.Securing Devices

1) Make hardware tamper-resistant

2) Provide for firmware updates/patches

3) Specify procedures to protect data on device disposal

2.Securing networks

1) Use strong authentication

2) Use strong encryption and secure protocols

3) Minimize device bandwidth

4) Divide networks into segments

3. Copyright Protection and Software License:

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

1) You must read and understand any software copyright restrictions. If you think that Banpu Power will not be able to comply with any part of the terms, do not download or use the material.

2) Ensure that you comply with any expressed requirements or limitations to the use of such software.

3) Software requests must be approved by the requester’s manager and then be made to the Information Technology department or Help Desk in writing.

4) Software must be selected from an approved software list unless no selection on the list meets the requester’s need.

4. User Login and Password:

1) Each person is responsible for the login name and password.

2) Two- Factor Authentication must be enabled to secure user accounts.

Password Requirements:	**Password Protection:**
1) Contain a mix of alphabetic and non-alphabetic characters. 2) A strong password must be at least 8 characters long. 3) Not contain the user id a part of the password. 4) Be changed at least every 90 days. 5) Not be reused until after at least three iterations.	1) Must not be shared with anyone. 2) Must not be inserted into email, or other forms of electronic communication. 3) Passwords may be stored only in “password managers” authorized by the organization. 4) Do not use the "Remember Password" feature of applications. 5) Any user suspecting that password may have been compromised must report the incident.

3) All login names and privileges should be reviewed at regular intervals.

4) In the case of an employee leaving the organization, the functional head will be responsible for making sure that all the employee's system IDs are revoked.

5. Remote Access

To define security requirements for connecting to Banpu Power's internal network. These requirements are designed to minimize potential damages, which may result from the unauthorized use of resources.

1) Secure remote access must be strictly controlled with encryption Virtual Private Networks(VPN).

2) Authorized users shall protect their login and password, even from family members.

3) All notebooks that are connected to Banpu Power internal networks via remote access must be installed the most up-to-date anti-virus software. This also includes personal computers.

4) Third-Party contact IT representative to request the remote access, and their notebooks shall meet all security requirements.

6. Third-Party Access

To minimize the risks, associate with Third Party access to Banpu Power’s internal network. These requirements shall be applied:

1) The Head of IT department must authorize a request for Third- Party access.

2) Third- Party will be restricted to the minimum services and functions.

3) Third- Party will only access using the devices to meet all security requirements.

4) All Third Parties granted access must be given a unique login and password.

5) The Third Parties are solely responsible for login, and password remains confidential

7. Information Protection:

7.1. Data Classification

The company classifies data in the following classes:

Level	Classification	Safeguard	Description	Example
0	Public	Everyone can view	Business data that is specifically prepared and approved for public	Brochures, Public news
1	Internal	-Only employees. -Print and forward to other employees is allowed.	Business data that is for internal employees only not intended for public consumption at all.	Work instruction, Product catalog
2	Confidential	-Only the intended recipient. -Cannot be printed or forward.	Sensitive business data that could cause damage to the business if shared with unauthorized people.	Product research, payroll, contracts, security reports, forecast summaries, Personally identifiable information (PII) e.g., credit card, bank account, salary data
3	Restricted	-Only management level	Very sensitive business data that would cause damage to the business if shared with unauthorized people.	Trade secret, passwords, pre-announced financial reports.

7.2. Information Protection

The Company has assigned the information owner to responsible information for each application.

1) The information owner will communicate the importance of the information, level of classification, security controls, and monitoring requirements to the IT Administrator (IT Admin).

2) IT Admin will not take any action on the information without the permission of the information owner.

3) IT Admin will make sure that there are proper safeguards in place to recover from any disaster.

4) IT Admin should maintain proper documentation of all activities involving the information owner.

5) IT Admin will inform the information owner of any risk or shortcomings as soon as they are identified.

The protection for Non-public Information **(Classification Level 1, 2, 3)**

1) Encryption should be considered.

2) When storing it on removable media, you must protect it against theft and unauthorized access.

3) When printing it, you must protect the information against theft and unauthorized viewing.

7.3 Information Protection on Cloud Computing Platform

The objective is to provide the proper control of the scalable computing resources technology.

1) Acquiring/ Deploying on Cloud Computing should be authorized by Head of Information Technology.

2) Any software compliance issues, and all related laws should be assured, recorded, and monitored.

3) The physical location of Banpu Power information or application should be identified.

4) Administrative privileges, identities, billing information, and relevant security credentials to cloud services should be stored as separately backup and reviewed on a timely basis.

5) Ensure how disaster recovery and continuity of service are addressed.

6) Ensure your service deployment model (private access, public access) are protected align with the business requirement.

7) Enable data encryption feature to secure data in Transit, and data at Rest.

8) Manage access by using Role- Based Access Control (RBAC).

9) Enable Access Log for regularly audit access.

10) Prepare cloud provider exit plan with these key considerations:

a) How will data be migrated out of the cloud provider? Will there be an additional cost?

b) How will unwanted data be securely erased? What kind of proof and audit trail?

c) What are the obligations of each party regarding an exit plan?

8. Collaboration Services:

1) These services must support legitimate, mission-related activities of the company and be consistent with prudent operational, security, and privacy considerations.

2) Each employee will be assigned a unique email address to be used on the collaboration platform.

3) 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.

Inappropriate use:

The following uses of company provided Internet access are not permitted:

1) Download or distribute pirated software or fake information.
2) Deliberately propagate any virus, worm, Trojan horse, hoax.
3) Play Internet- based games or participate in online gambling.
4) Personal usage that degrades internet performance.
5) Transmitting messages containing profanity, derogatory, politic, defamatory, sexual, racist, harassing, or offensive material.
6) The promotion or publication of one's political or religious views, the operation for any undertaking for personal gain.
7) Transmitting messages inadvertently those results in Banpu Power becoming liable for contractual issues or being embarrassed by statements or claims, which may not be official Banpu policy.

Appendix A

APP 1 – Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 – Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 – Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 – Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 – Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 – Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 – Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 – Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 – Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

APP 10 – Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 – Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 – Access to personal information

Outlines an APP entity’s obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 – Correction of personal information

Outlines an APP entity’s obligations in relation to correcting the personal information it holds about individuals.

Responsibility:

- Data Protection Officer (DPO): Responsible for ensuring that the Banpu Power and subsidiary companies comply with Data Protection Regulations.
- Information Owner: Responsible for handling variances from accepted practices. If the request for information requires controls that are inconsistent with policy, the owner is then responsible for the necessary changes and subsequent repercussions.
- Head of Information Technology: Allocates sufficient resources and manages Information Technology staff, which takes steps to ensure that all workers in the Information Technology Department are conducting their daily activities in a manner of compliance.
- Information Technology Administrators (IT Admin): Responsible for establishing, maintaining, implementing, administering information systems security on a daily basis to assure the secure information system environment.
- All Employees: Responsible for compliance with policy and all other Banpu Power policies defining security measures.

References:

Reference

1. Information Security Management System (ISMS) ISO/IEC 27001:2013
2. Privacy Information Management System (PIMS) ISO/IEC 27701:2019
3. SANS Institute Security Policy Template
4. Gartner Policy Toolkit

Related Policy

1. IT Corporate Policy
2. Information Disaster Recovery Policy
3. Privacy Policy

The relevant laws from each country

Country	Data Protection Laws
Australia	• Australian Privacy Principles (APP) The summary of Australian Privacy Principles - in Appendix A The current version can be found on this webpage https://www.oaic.gov.au/privacy/the-privacy-act/ **Obligation to comply**: Any Banpu Power employees outside Australia who have access to personal information that has been included on any shared IT platforms have an obligation to comply with the Australian Privacy Principles (APP) in respect of such information.
China	• Cybersecurity Law of the People's Republic of China effective 2017
Indonesia	• Law No.11 of 2008 on Electronic Information and Electronic Transactions • Regulation No.82 of 2017 on Operation of Electronic Systems and Transactions
Japan	• Act on the Protection of Personal Information ("APPI") of 2017
Singapore	• Personal Data Protection Act 2012
Thailand	• Copyright Law B.E.2537 • Computer Crime Act B.E.2550 • Personal Data Protection Act B.E.2562 (2019)
Vietnam	• Cybersecurity Law 2018 (CSL 2018)
European Union	• The General Data Protection Regulation (EU) 2016/679