POLICY

Information and Cyber Security Policy

Document Number:	Revision:	Date:	Page 1 of 12	Authorized by:
TH-IT-IT-PO-01	4.0	Dec/2018		Somruedee Chaimongkol **Chief Executive Officer**
Department: Information Technology				

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.

Policy Objective:

BANPU's Digital Assets are critical to the company's security, and as a result, must be protected from loss, modification or destruction. This policy is deliberately designed for the organization-wide benefit of active digital technology related usage and its operation.
This policy also helps to ensure compliance with the relevant legislation, best practices, and agreements with third parties.

Policy Scope:

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

Policy History:

Version	Date	Description
1.0	Aug/2006	The first version of BANPU IT Security Policy
2.0	Sep/2008	To comply with the Computer Crime Act
3.0	Apr/2014	To mitigate IT risks on cloud computing and mobile workforce
4.0	Dec/2018	- Revised the Data Classification level - Added the Data Protection Officer (DPO) to comply with data protection laws - Added Internet of Things (IoT) definition and Basic Security

Policy Contents:

POLICY				
Information and Cyber Security Policy				
Document Number: TH-IT-IT-PO-01	**Revision:** 4.0	**Date:** Dec/2018	**Page 2 of 12**	**Authorized by:** Somruedee Chaimongkol **Chief Executive Officer**
Department: Information Technology				

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.

- 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:

The ability to protect or defend the use of cyberspace from cyberattacks.
[*Source- http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf*]

Cybersecurity also 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.

Records:

Digital and physical records include information created, received and maintained as evidence of the transaction of BANPU business and for compliance with relevant laws, regulations, policies, and agreements with third parties.

Physical records as all information created and captured on the following list.

- paper
- video
- photographs
- maps
- drawings
- models

Digital records as all information created and captured in the following list.

- e-mails
- messaging systems
- websites
- social media
- stored on computer hard drives
- On portable or removable media
- On servers owned or rented by our organization
- On mobile devices
- On cloud-based services

Source Code:
Source code is the set of instructions and statements written by a programmer using a computer programming language. This code is later translated into machine language by a compiler. The translated code is referred to as object code
[Source-https://www.techopedia.com/definition/547/source-code]

The source code will be stored in the central repository with version control and will be governed by other policies under Application Development Life Cycle.

Internet of Things (IoT):
The Internet of things (IoT) is the network of physical devices, vehicles, home appliance, and other items embedded with these components:

- Electronics
- Software
- Sensors
- Actuators
- Connectivity

which enables these objects to connect and exchange data

Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing internet infrastructure.
[Source- https://en.wikipedia.org/wiki/Internet_of_things*]*

POLICY				
Information and Cyber Security Policy				
Document Number: TH-IT-IT-PO-01	**Revision:** 4.0	**Date:** Dec/2018	**Page 4 of 12**	**Authorized by:** Somruedee Chaimongkol **Chief Executive Officer**
Department: Information Technology				

Roles & Responsibility:

Roles	Responsibilities
Data Protection Officer (DPO)	Responsible for ensuring that the BANPU 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 for the information systems security on a daily basis to assure the secure information system environment.
Information Technology Management Committee	The Committee will be composed of Senior management or their delegates from each BANPU major division and subsidiaries. This committee will annually review the control of BANPU security and potential risks in all IT operation locations.
All Staff	Responsible for compliance with policy and all other BANPU policies defining security measures.

POLICY				
Information and Cyber Security Policy				
Document Number: TH-IT-IT-PO-01	**Revision:** 4.0	**Date:** Dec/2018	**Page 5 of 12**	**Authorized by:** Somruedee Chaimongkol **Chief Executive Officer**
Department: Information Technology				

Reference:

The BANPU Enterprise Architecture

- TH-IT-EA-SPM-05 Data Security Framework and Guideline

The Cybersecurity Frameworks

- NIST Cybersecurity Framework (2014)

The relevant laws from each county

Country	Data Protection Laws
Australia	• Workplace Surveillance Act 2005 (NSW)
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
Vietnam	• Cybersecurity Law 2018 (CSL 2018)
European Union	• The General Data Protection Regulation (EU) 2016/679

Enforcement:

The Policy will be approved by the Chief Executive Officer and supported by the Management. It will be annually reviewed and amended when needed.
Head of Information Technology will document cases of violation in order to maintain company integrity.
Any employee in violation of these policies is subject to disciplinary action, including but not necessarily limited to termination.

Exception:

Any deviation from policies must be evaluated in the context of potential risk and approved by Head of Information Technology before that date to ensure overall performance and assurance in IT services.

Audit & Risk Assessment:

Audit of the security of the company will be performed at regular interval time. Every Information Management Committee review or Internal/External Audit fieldwork. Any reports containing critical issues will be submitted to responsible persons and Head of Information Technology for immediate action base on priorities and committed timeframe.

POLICY				
Information and Cyber Security Policy				
Document Number: TH-IT-IT-PO-01	**Revision:** 4.0	**Date:** Dec/2018	**Page 6 of 12**	**Authorized by:** Somruedee Chaimongkol **Chief Executive Officer**
Department: Information Technology				

Policy Statement:

1.Organization Security:

1.1. Segregation of Duties

Segregation of duties defines operation reviews in the Information Technology Department with other departments which reduce security risk. It's composed of the job description; each job description has backup staff when responsibility staff cannot operate on functions

1) Organization Chart must clearly define for review and operation especially developer who is separated from the system administrator in the production environment.
2) Management must establish and maintain sufficient preventive and detective security measures to ensure that 'BANPU information is free from the significant risk of undetected alteration.
3) Production environment must have backup staff when the main staff is absent.
4) Information owner is to control information and define access control information.
5) All workers must be acknowledged and defined responsibilities for information security.

1.2. Third-party

Third-party is necessary for some tasks so preparing policy and contract to create transparently and clarify operation. Security requirement in outsourcing contracts must be defined in business need.

1) Outside consultants, contractors must be subject to the same information security requirements.
2) Whenever communications with third parties necessitate the release of non-public BANPU.

2.Copyright Protection and Software License:

The Company supports strict adherence to copyrights and software license agreement (define the controls in RCC policy). When obtaining material for use inside BANPU.

1) Do not obtain software from such sources for use within BANPU unless express permission to do so is stated by the material owner.
2) You must read and 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.
3) Ensure that you comply with any expressed requirements or limitations attached to the use of such software (for example: not to be used for commercial purposes; cannot charge others for use or distribution; subject to a copyright.

3.Physical Environment and Security:

3.1. Server Room Access

1) Server room doors must be locking all time or other security devices.
2) Access control entry log has been periodically reviewed by management.

3.2. Company-owned devices

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

1) The company-owned device should comply with company standard specification.
2) Who can access the personal computer he/she must key user ID and password in the first level of security and second level by password of each application.
3) Activate the password protected keyboard/screen lock when you leave.

4) The software that allows other users to access your files must be provided by BANPU. This is to Ensure that it has been checked for security holes and legal and licensing restrictions. Any pirate application installation is prohibited and under BANPU right to mitigate any risk without notification.

4.Secure Access Control:

4.1. User Account

1) Every user should have a uniquely assigned login name and password to access computer systems.
2) Each person is responsible for the login name assigned to him/her.
3) All login names and privileges should be reviewed at regular intervals.
4) A login which is not successful should be logged and the log reviewed at regular intervals.
5) 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 before final settlement.

4.2. Password

Reusable passwords used ln identity verification challenges must adhere to the following:

1) Contain a mix of alphabetic and non-alphabetic characters (numbers, punctuation or special characters) or a mix of at least two types of non-alphabetic characters.
2) Not contain the user id a part of the password.
3) Be changed at least every 90 days.
4) Not be reused until after at least three iterations.
5) Not be transmitted in clear text form over the Internet, public networks, or wireless devices.

5.Internet of Things (IoT) Basic Security

5.1. Securing Devices

1) Make hardware tamper resistant
2) Provide for firmware updates/patches
3) Specify procedures to protect data on device disposal

5.2. Securing networks

1) Use strong authentication
2) Use strong encryption and secure protocols
3) Minimize device bandwidth
4) Divide networks into segments

6.Information Protection:

6.1. Data Classification

It is essential that all company information be protected. The company classifies data in the following classes:

Level	Classification	Definition	Impact of Unauthorized Disclosure
0	Public	• Data that the company intentionally shares with the public	Always authorized and no impact
1	Internal	• Data to which large segments of the company's workforce is provided access to perform their jobs and intended for use internal only	May cause minor embarrassment or operational inconvenience.
2	Confidential	• Data to which only limited segments of the Company's workforce need access to perform their jobs	Likely to cause significant harm to the Company, its employees, customers, stockholders, or business partners.
3	Restricted	• Data to which very limited segments of the Company's workforce need access to perform their jobs	Likely to cause severe harm to the Company, its employees, customers, Stockholders, or business partners.

6.2. Information Protection

All information asset and physical asset are BANPU's properties. The Company has assigned information owner to responsible information for each application.

1) The information owner will communicate the importance of the information, level of classification, controls and monitoring requirements to Information Technology Administrators (IT Admin).
2) The IT Admin may not take any action on the information without the permission of the information owner.
3) It is the responsibility of the IT Admin to ensure that information is backed up and stored at a secure place.
4) The IT Admin will make sure that there are proper safeguards in place to recover from any disaster.
5) The IT Admin will make sure that all adequate controls are in place, as specified by the information owner.
6) The IT Admin should maintain proper documentation of all activities involving the owner's information.
7) The IT Admin will inform the information owner of any risk or shortcomings as soon as they are identified.

6.3. Information Security

6.3.1 Authentication

Each user's identity must be verified (authenticated) when the user attempts to log in to the system or application/middleware.

1) Systems are to use authentication services provided by the system access control mechanism.
2) Applications are to use BANPU's common user ID authentication services the where possible.

6.3.2 Non-public Information (Classification Level 1, 2, 3)

The primary requirement for protecting non-public information is that it must be protected from access or viewings except by authorized people.

1) Encryption of non-public information should be considered when it is sent over the Internet, public networks, or wireless devices.
2) When you store non-public information on removable computer media, you must protect the information against theft and unauthorized access.
3) The media contain non-public information and keep them in a locked area or storage device when they are not in use.
4) Do not enter non-public information on Internet websites that offer none of the charge service or non-information privacy control.
5) When printing non-public information, you must protect the information against theft and unauthorized viewing.

6.4. Information Protection on Cloud Computing or Off-premise BANPU data center

The objective of information protection on cloud computing or off-premise BANPU data center is to provide the proper control of the scalable computing resource technology.

1) Acquiring/Deploying any off-premise computing resource or public cloud services for the production environment, should be authorized by Head of Information Technology.
2) Any software compliance issues and all current laws on cloud computing or off-premise BANPU data center should be assured and recorded before operating the service in BANPU environment.
3) The physical location of BANPU information or application should be identified before to operate any IT services.
4) Administrative privileges, identities, billing information and relevant security credentials to cloud services, should be stored as separately backup and reviewed in the timely basis.
5) Ensure how disaster recovery and continuity of service is 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's environment? Will there be additional cost?
    b) How will unwanted data be securely erased? What kind of proof and audit trail?
    c) What are the obligations on each party regarding an exit plan?

7.Internet and E-mail Security:

7.1. Internet Usage

1) Internet accounts are approved for designated employees by their immediate.
2) Each is responsible for the account issued.
3) Sharing Internet account or User-ID's is prohibited.
4) Organizational use of internet services must be related to the company's business.
5) These services must support legitimate, mission-related activities of the company and be consistent with prudent operational, security, and privacy considerations.
6) The Company has no control over the information or content accessed from the Internet and cannot be held responsible for the content.
7) Any software or files downloaded via the Internet into the company network become the property of the company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.
8) All website access should be run through internet proxy and Inappropriate website access should be classified.

Inappropriate use

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

1) To access, upload, download, or distribute pornographic or sexually explicit material
2) No employee may use company facilities knowingly to download or distribute pirated software or information.
3) No employee may use the company's Internet facilities to deliberately propagate any virus, worm, Trojan horse, streaming, hoax or trap-door program code.
4) Play Internet-based games or participate in online gambling.
5) Personal usage that degrades organization internet performance is limited i.e. peer to peer sharing, streaming contents, VDO call etc.
6) Bypassing internal proxy or access non-corporate proxy for personal use is prohibited.

7.2. Company Collaboration services

The company provided e-mail account, Collaboration services for each employee following the company standard. We are going to install the e-mail monitoring system to analyze the use and misuse of the e-mail system.

The management will need to decide on:

1) Each employee will be assigned a unique e-mail address that is to be used while conducting company business via e-mail.
2) Use company e-mail for the business purpose. Using public e-mail or other communication services to exchange BANPU information should be approved by Head of Information Technology.
3) The company prohibits discrimination based on age, race, gender, sexual orientation or religious or political beliefs. Use of electronic messaging resources or others to discriminate for any or all of these reasons is prohibited.
4) Carefully consider how the recipient might interpret a message before composing or sending it.
5) Any employee who discovers a violation of these policies should immediately notify a manager or the Human Resources Department.

Inappropriate use

The following uses of company provided e-mail, Collaboration services access is not permitted:

1) e-mail or Collaboration services may not be used for transmitting messages containing pornography, profanity, derogatory, politic, defamatory, sexual, racist, harassing, or offensive material.
2) The Company provided Collaboration services may not be used for the promotion or publication of one's political or religious views, the operation of a business or for any undertaking for personal gain.
3) Use of e-mail or Collaboration services for personal purpose.
4) Sending unsolicited e-mail to a large number of people without adequate business reasons.
5) Send e-mail inadvertently those results in BANPU becoming liable for contractual issues or being embarrassed by statements or claims, which may not be official BANPU policy.

8.Security Incident Handling:

8.1. Notifications and Point of Contact

The person responsible for contacting for Information Security and Cybersecurity issue, is Head of Information Technology.

The person responsible for IT Security and Cybersecurity may have considerable technical power to configure the firewall, review audit reports and organization representative for any action regarding computing compliance and government support. The actions of this person should be monitored by using separation of duties (if there are multiple administrators) or through careful screening of the individual.

8.2. Identify an Incident

All problems regarding exposed firewall service, weaknesses in network and system, fraud, high infected computer malware unauthorized access or hacking attempts against BANPU information, should be recorded for helping to solve the problem in the repeated incident.

1) Each incident has to necessary fields to keep a historical record.
   - -Recipient
   - -Date
   - -Cause of incident
   - -Symptom
   - -Resolver
   - -Date of Resolving
2) All trouble reports received should be reviewed for symptoms that might indicate intrusive activity.
3) In case repeated incident, take history resolving incident to use solving problem.
4) Evaluation of the impact of the problem.
   - -Is sensitive information involved?
   - -What is the entry point of the incident?
   - -What is the potential damage of the incident?
   - -What is the estimated time to close out the incident?
   - -What resources could be required to handle the incident?

8.3. Handling an Incident

All identified incident must be immediately reported to Head of Information Technology and managers in all business units impacted. The historical incidental record must be taken to ensure that electronic evidence is collected and secured properly.

1) Notification: - All related persons in this incident by e-mail, telephone etc.
2) Containment: - Take activity for the limited scope of damage.
3) Eradication: - Eliminate the reasons for the incident.
4) Recovery: - Re-establish service and systems.
5) Follow Up: - Take action after the incident.

An Incident is where the impact is confined and likely to result only in internal disciplinary action. No overall impact to organization, employees, stockholders, and/or business partners. Examples are negligent disregard bf company policies and procedures, repeated mistakes, and temporary denial or disruption to services.

These kinds of incidents will be investigated and resolved by the manager responsible for the area where the incident was discovered.

8.4. The aftermath of an Incident

These actions can be summarized as follows:

1) An incident record should be taken of the systems' assets.
2) The lessons learned as a result of the incident should be included in the revised security plan.
3) A new risk analysis should be review and developed.
4) An investigation and prosecution of the individuals who caused the incident should commence.
5) An annual summary report of all incidents should be provided and reported to Head of IT.