Plan B Media Public Company Limited
1700, Plan B Tower, New Petchburi Road, Makkasan, Ratchathewi, Bangkok 10400
Tel.+662 530 8053-6 | Fax.+662 530 8057 | E-mail : info@planbmedia.co.th | Tax ID. 0107556000507
www.planbmedia.co.th

Information and Cyber Security Policy

Plan B Media Public Company Limited and the group company (hereinafter referred to as "Company") places importance on the development of digital technology and use of information in conducting business. The Company realizes the importance of information security, including prevention of cyber threats so this policy has been established to create operational guidelines for data security and the use of information technology in Company.

Scope

This policy covers the protection and maintenance of information and cybersecurity of PLANB, whether on-premise or cloud-based systems procured by the Company. It applies to:

1) All employees and departments within the Company
2) External parties authorized to access Company-related computer systems and information

Governance of Enterprise IT

The governance of enterprise IT is intended to ensure that the Company can achieve its strategic goals by utilizing information technology as a tool to support business operations and effectively manage potential risks arising from its implementation. Effective information technology management requires alignment between IT governance processes, resources, and data efficiency to support the organization's policies, strategies, and objectives, as well as appropriate risk management. It must also include reporting and monitoring mechanisms to ensure that the technologies adopted by the Company effectively support strategic execution, help achieve business goals, enhance competitive advantage, and contribute to long-term corporate value.

Guideline

1. Protection of information

- **Access Control**
  - Implement appropriate and adequate measures to ensure that information security aligns with business operations and the significance of each data type Including both internal and external factors that may affect the Company's information security, with a strong emphasis on maintaining the confidentiality, availability, integrity, and accuracy of information in compliance with applicable laws, regulations, and relevant third-party requirements.
  - All directors, executives, and employees must strictly adhere to the Company's information and cybersecurity policies, avoiding any unauthorized use of confidential information, including unauthorized access to other users' data and files, as defined in the Company's rules regarding the use of IT devices and systems.

- Defining roles, responsibilities and duties appropriately for operation about information systems and information security, including setting authorization and control for accessing important information. Moreover, the equipment or space used to store important data both is protected appropriately through physical storage and information systems to prevent any access to sensitive information without permission.
- Data owners are responsible for reviewing user access rights at least once a year to ensure that assigned permissions remain appropriate and aligned with current roles and responsibilities.
- System administrators are responsible for controlling access to data at each confidentiality level, both through direct access and via information systems. They are required to maintain a list of user accounts and passwords to verify and authenticate users' identities for access to each corresponding level of information.
- Password policy is set to be in line with business operations and current situation as well as communicated to all employees that they must keep their password and any other codes specified by the company to access the computer system or company information or personal information confidentially. Password must be kept so that others do not know, and do not share with other people to comply with the password policy strictly.
- Using of personal equipment to connect with the company information system must comply with rules and regulations set by person in charge of information security.
- During the employment period, employees shall not do anything and/or refrain from any actions that cause damage to the company as a result of false information and/or reports or records or communications whether by any means. If there is intentionally violation of policies or measures related to information security that cause damage to the company, the person who violate the rules will be punished according to the regulations of the company, and prosecuted if the operation is against the law.
- The Information Technology Department must define network connection pathways for internet access, which must be routed through security systems such as Firewall or Proxy
- Remote access to the Company's information systems must be conducted exclusively through a Virtual Private Network (VPN) to ensure that data transmitted over public networks is encrypted. VPN usage must be authenticated and logged to enable traceability and post-incident review

- **Physical and Environmental Security**
  - Defining roles, responsibilities and duties appropriately for operation about information systems and information security, including setting authorization and control for accessing important information. Moreover, the equipment or space used to store important data both is protected appropriately through physical storage and information systems to prevent any access to sensitive information without permission.

- Employees shall use the assets of the company with care, responsibility for the equipment. Any received equipment from the company should be always in good condition by contacting repair department when damage occurs. The company's assets must not be lost or destroyed, even if equipment are not their responsibility directly. Do not bring any property to use for other purposes except for company's benefit. Any equipment that has important information or able to access the information system of the company must be prevented from being used by people who are not authorized, such as setting a password or screen saver of the computer when not in use. If the device is lost or stolen, notify the management information system division as soon as possible to consider the appropriate actions for information security.
- There is a centralized maintenance of information technology equipment for maintaining equipment in good condition and continuous usage.
- Data owners are responsible for reviewing user access rights at least once a year to ensure that assigned permissions remain appropriate and aligned with current roles and responsibilities.

2. Information Management and Confidentiality Protection

- **Information Classification**

The Company classifies information and assigns levels of importance or confidentiality based on internal guidelines for organizational confidentiality. These guidelines serve as a prudent and appropriate framework for managing and securing electronic documents. The following processes and procedures have been established for handling critical documents:

1) Information Classification:
   - Administrative Information: Includes data related to policies, strategies, performance commitments, human resources, budget, finance, and accounting.
   - Operational Information: Refers to data used by each department based on its specific functional responsibilities.
2) Information Prioritization:
   - Highly Critical Information
   - Moderately Critical Information
   - Low Critical Information
3) Information Confidentiality Levels:
   - Top Secret: Disclosure in whole or in part may cause the most severe damage.
   - Secret: Disclosure in whole or in part may cause serious damage.
   - Confidential/Internal Use: Disclosure in whole or in part may cause harm.
   - Public: Information that may be disclosed or distributed freely.

4) Access Level Classification:

- Executive Level: Access is granted according to roles, responsibilities, and placement on the authorized personnel list within the respective unit.
- General User Level: Access is limited to authorized or published information designated for general users.
- System Administrator or Legally Authorized Personnel Level: Access is granted based on assigned privileges within the scope of legal and official duties.

- **Data Backup**
  - Critical data is securely stored, including the determination of business continuity plans and incident response procedures in place with regular test of disaster recovery planning. The data recovery plan in the event of a disruption must be tested regularly to ensure its effectiveness and applicability in actual emergency situations.
  - System administrators or designated personnel are responsible for performing data backups and verifying the integrity of the backed-up data in accordance with the defined schedule and in compliance with the Company's data backup and recovery policy.
  - In the event of an issue that results in incomplete data backup, a root cause analysis shall be conducted, followed by appropriate corrective actions. A summary report shall be prepared and submitted to the Information Technology Manager for review and further action.

- **Cryptographic Controls**

To ensure appropriate and effective data encryption, and to safeguard the confidentiality, integrity, and authenticity of sensitive or classified information from unauthorized disclosure, tampering, or access by unrelated external parties, the Company has established the following data encryption control measures:

Data Management

- Defining roles, responsibilities and duties appropriately for operation about information systems and information security, including setting authorization and control for accessing important information. Moreover, the equipment or space used to store important data both is protected appropriately through physical storage and information systems to prevent any access to sensitive information without permission.
- Password policy is set to be in line with business operations and current situation as well as communicated to all employees that they must keep their password and any other codes specified by the company to access the computer system or company information or personal information confidentially. Password must be kept so that others do not know, and do not share with other people to comply with the password policy strictly.

- In cases where critical data is transmitted over public networks, the Company shall employ internationally recognized encryption technologies, such as Transport Layer Security (TLS)/Secure Socket Layer (SSL) and Virtual Private Network (VPN) connections, to ensure secure communication and data protection.
- The Company has established security measures for situations in which computers or work-related devices are taken offsite, such as for repairs or service by external providers at installation locations. In such cases, all devices must undergo a data deletion or masking process prior to removal, in order to mitigate the risk of data leakage.

User Privilege

- The Company implements strict access control measures for information and data processing equipment, taking into account the nature of usage and the security requirements of its information systems. Guidelines and criteria for access authorization are clearly defined to ensure appropriate permission levels based on roles and responsibilities. Employees at all levels are required to understand and strictly adhere to these policies while recognizing the importance of system security. For example, software installations may only be performed by authorized personnel with administrator-level privileges, and access to the server control room is restricted to authorized staff, with entry and exit logs maintained at all times.
- Access rights to data and information systems, such as internal application systems, internet usage, and shared storage, shall be granted only to the extent necessary for employees to perform their duties. For instance, employees may access files within their own department, while access to other departments' data is limited to designated shared areas only. All access permissions must be formally approved in writing by authorized personnel and reviewed regularly to ensure continued appropriateness and compliance.
- In cases where it is necessary to grant access to the Company’s information systems or network to external individuals on an urgent or temporary basis, clear procedures and guidelines must be followed. Such access must be formally approved by authorized personnel, with the reasons and duration of access clearly documented. Access rights must be promptly revoked upon the expiration of the approved period.

User Account and Password Management Controls

- The Company has established measures to protect user password data by employing file encryption systems for password storage. This is intended to prevent unauthorized individuals from accessing or modifying such information. For example, all passwords are encrypted prior to being stored in the system database to ensure the confidentiality and integrity of user credentials.
- Regular reviews are conducted on user accounts in critical systems, with particular attention given to accounts that no longer have valid access rights—such as those belonging to former employees

or system-generated accounts. The Company will immediately revoke access upon identifying any inappropriate or unauthorized accounts, through measures such as disabling the account, deleting it, or resetting the password, as deemed appropriate.

- The Company enforces strict user authentication and authorization controls prior to granting access to information systems. This includes the use of two-factor authentication (2FA) and the requirement that each user be assigned a unique personal account to ensure secure system access. To further enhance security, the Company has established comprehensive password management guidelines to prevent unauthorized access, as outlined below:
    1) Passwords must be at least 9 characters in length and should contain a combination of letters and numbers
    2) Passwords must include special characters (e.g., : ; < > $ @ #)
    3) Passwords must be changed at least once every 3 months
    4) Previously used passwords cannot be reused for the last 4 password cycles
    5) If a user enters an incorrect password more than 5 times, the system will suspend access to mitigate security risks
    6) Users who receive an initial or reset password must change their password immediately upon first login

- **Privacy and Protection of Personally Identifiable Information**
    - The Company regularly conducts training programs to raise employee awareness on information security and cybersecurity. These programs include communication and educational initiatives related to information technology, data protection, and emerging cyber threats. All employees are required to participate to ensure they understand their responsibilities and are equipped to safeguard the Company's information assets effectively.
    - All directors, executives, and employees are required to strictly comply with the Company's Information and Cybersecurity Policy. This includes respecting the privacy of others, refraining from the unauthorized use of confidential information, and avoiding any unauthorized access to other users' data or files. Such actions must be in accordance with the Company's rules and regulations governing the use of computer systems, devices, and related tools.
    - Password policy is set to be in line with business operations and current situation as well as communicated to all employees that they must keep their password and any other codes specified by the company to access the computer system or company information or personal information confidentially. Password must be kept so that others do not know, and do not share with other people to comply with the password policy strictly.
    - Employees shall use the assets of the company with care, responsibility for the equipment. Any received equipment from the company should be always in good condition by contacting repair

department when damage occurs. The company's assets must not be lost or destroyed, even if equipment are not their responsibility directly. Do not bring any property to use for other purposes except for company's benefit. Any equipment that has important information or able to access the information system of the company must be prevented from being used by people who are not authorized, such as setting a password or screen saver of the computer when not in use. If the device is lost or stolen, notify the management information system division as soon as possible to consider the appropriate actions for information security.

- Employees shall acknowledge and follow the guidelines of using computer and network systems appropriately, including information security procedure to prevent confidential information from being unintentionally disclosed. The company supports information security is a part of employee performance evaluation of the development of human resource appropriately.
- During the employment period, employees will aware of company information known as "Trade Secrets", means trade information which has not yet widely known or not yet accessible among the persons who are related to such information. It is the information which is useful commercially trade secret controller uses appropriate measure to maintain its secrecy so this information may be stated in contract or any other agreement of the company or specified in the trade secrets act, B.E.2545 (2002). Employees agree to keep "Trade Secrets" of the company that have known or given because of working for the company and do not send or copied to recipient without permission, including disclose and/or do or refrain from any action that damage to the company's reputation or the company's business.
- Maintain the confidentiality of the Company's customers, business partners, and other related parties.
- Refrain from disclosing any confidential information, documents, or trade secrets for a period of 1 year after the termination of employment or position with the Company.

3. Management of Computer Networks and Information Transmission

- **Communications Security**
  - Shall not bring assets or use the internet of the Company with commercial purpose or personal benefit except for directly benefit to the company, including avoid using the website or electronic mail that is vulnerable to cyber-attack. Additionally, the use of the Company's resources and computer networks for illegal activities or actions that violate public morals is strictly forbidden — for example, creating websites for unauthorized commercial purposes or disseminating content that is unlawful or unethical.
  - Strictly prohibited to access computer systems or data protected by access controls for the purpose of modifying, deleting, or copying information without proper authorization.
  - Shall not install software or record any information in the company's computer without permission.

- Shall not bring the company's software to other persons which includes suppliers, contractors, customers of the company and personal agenda. Furthermore, the use of the internet or connect to the internet by employees to transferring data, dissemination of pornography, sending and receiving information via electronic mail (e-mail) that violates the law or copyright law or the intent or the purpose of the policy or regulations for information security policy of the company or Computer-related Crime Act B.E. 2550 (2007) or other related laws.
- No copyrights infringement of the company and/or of other companies that allow the company to use computer software regardless of the contract and/or any methods and/or whether the action is repeated or modify or distribute to the public or rent or copy whether for profit or not.
- Adequate and appropriate network security measures are in place to safeguard the Company's IT infrastructure. Security software is installed to protect against external threats that may harm the main server and client servers. Such software must be updated regularly and in a timely manner to ensure ongoing protection and effectiveness.
- Access to the Company's network systems is subject to strict security controls to ensure stability and protection. Network segmentation must be implemented to clearly separate internal users from external users who interact with the Company, thereby minimizing the risk of unauthorized access and enhancing overall cybersecurity.

- **Information Transfer**
  - Agreements on Information Transfer must be established to ensure the secure handling of data during transmission. These agreements must take into account data security requirements and clearly define responsibilities. System administrators are responsible for overseeing and ensuring that all data transfer activities maintain security across the three key dimensions: Confidentiality, Integrity, and Availability.
  - A Non-Disclosure Agreement (NDA) must be signed between the Company and any external parties to ensure that the Company's confidential information is not disclosed without proper authorization.
  - Shall not bring the company's software to other persons which includes suppliers, contractors, customers of the company and personal agenda. Furthermore, the use of the internet or connect to the internet by employees to transferring data, dissemination of pornography, sending and receiving information via electronic mail (e-mail) that violates the law or copyright law or the intent or the purpose of the policy or regulations for information security policy of the company or Computer-related Crime Act B.E. 2550 (2007) or other related laws.
  - Sending, using, processing, storing and destroying important information and equipment that has important data must be an appropriate process to ensure that adequate by unauthorized people.

- There is storage of important system (Log) and set the appropriate storage period. Log will be used in the inspection and trace back to usage history that comply with the laws, rules and regulations of related external parties.
- A proactive process is in place to prevent disruptions to the information system and to respond promptly to cybersecurity attacks. This includes timely detection and mitigation measures, root cause analysis, and the implementation of preventive actions to avoid recurrence. Significant incidents are reported to the Executive Committee for oversight and further action.
- There is clear escalation process which employees and stakeholders can make complaint

4. System Acquisition, Development and Maintenance

- Information system development shall have accurate and reliable process which covers the process of system design, development, testing and implementation. There is a separate system for development and the system that actually works, including places importance to designing systems with sufficient security and have security checks before actual use.
- Any modifications to information systems or related equipment must follow appropriate procedures and processes, including impact assessment and communication with relevant stakeholders. Adequate testing must be conducted to ensure system stability, and all related documentation must be updated to reflect the changes accurately and remain current.