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

Policy used of Information Technology (IT)

The background

With the increasing use of information technology systems in organizations, there are also various types of threats and risks that arise. Therefore, organizations that neglect the security of their information technology systems are at risk of being impacted by these threats. To mitigate these risks, it is necessary for organizations to enhance the security of their information technology systems and networks. In today's world, computers have become an integral part of life. They play a role in almost every aspect of work and human interaction. When computers are used in organizational settings, they require interaction with many personnel and practitioners who may have different perspectives and attitudes. Therefore, clear guidelines and practices are necessary to ensure smooth collaboration among these individuals without encountering problems.

Objectives

Plan B Media Company Limited aims to establish a computer network to facilitate convenient and efficient work practices for employees within the organization. This includes ensuring the appropriate and effective use of computer networks and preventing issues that may arise from improper network usage. Additionally, the objective is to ensure that employees, as well as external contracted individuals and departments, understand their roles and responsibilities, thereby reducing risks associated with theft, fraud, unauthorized disclosure of confidential information, misuse of data, and improper use of resources. Therefore, it is essential for the organization to establish clear guidelines and practices for the use of computers and network systems, enabling employees and contracted entities to be aware of the risks and issues related to security and their responsibilities. This includes understanding and complying with the organization's security policies, as well as minimizing the risks arising from errors in performing their duties.

Importance

Employees have the privilege to use the computer network under the provisions of this regulation. Any violation of the policy regarding the use of information technology systems or any action that may cause harm to the organization or any individual will be subject to disciplinary and legal action by the organization. Therefore, the organization must establish and enforce practices, conduct monitoring, and review, and make necessary improvements to the guidelines for the use of computers and network systems to adapt to rapidly changing information technology and comply with the law.

Primary Responsibility

All employees of the organization.

Related Definitions

"Organization" refers to Plan B Media Public Company Limited.

"Computer Network" refers to the computer network of Plan B Media Public Company Limited.

"Commander" refers to the person with the authority to give orders according to the organizational structure of Plan B Media Public Company Limited.

"Employee" refers to the employees and workers of Plan B Media Public Company Limited, including individuals assigned by the organization to work under contracts, agreements, or purchase orders, or individuals who are granted access to the organization's computer network.

"Network Administrator" refers to an employee who is assigned by the commander to be responsible for maintaining and managing the computer network, including accessing network programs for managing network databases.

"Organizational Manager" refers to high-level employees of the organization who are responsible for managing and have decision-making authority over all organizational operations.

"Information Manager" refers to high-level employees of the organization who are responsible for managing and have decision-making authority over the information technology systems within the organization.

"System Administrator" refers to an employee who is assigned the responsibility of maintaining computer systems and has access to computer programs or other data to manage the computer network, such as computer user accounts or email accounts.

"Information Supervisor" refers to an employee who is responsible for controlling and overseeing the work of system administrators, with the authority to give instructions to network and information system administrators within the organization and report to the information management executives.

"External Units" refers to other organizations related to the organization, such as hardware or software vendors, companies providing consulting services related to information technology systems, etc.

"Data" refers to anything that conveys meaning, stories, facts, information, or anything else, regardless of whether it is manifested by the nature of the thing itself or through any means, and regardless of whether it is recorded in the form of documents, files, reports, books, diagrams, maps, drawings, photographs, films, recorded images or sounds, computer records, or any other method that makes the recorded information appear. It also includes electronic data in accordance with the law on electronic transactions, such as text files, image files, sound files, programs, computers, etc.

"Computer System" refers to the equipment or set of computer equipment that work together, with instructions, command sets, or anything else, and guidelines for processing data automatically, including computers, whether connected or not, and mobile phones, etc.

"Service Provider" refers to the provider of services to others in accessing computer equipment or computer systems that work together, with instructions, command sets, or anything else, and guidelines for processing data automatically, including computers (whether connected or not) and mobile phones, etc.

"Computer Traffic Data" refers to data related to the communication of computer systems, which indicates the origin, destination, route, time, date, quantity, duration, type of service, or other information related to the communication of that computer system. This includes log data that records access to the network system, which identifies the identity and access rights to the network, as well as data related to the date and time of communication and the machines accessing the service and the machines providing the service, etc.

Category 1 General Regulations

The personal computer owner is responsible for any damage that occurs to the computer or operating system as a result of improper use or loss.

• New employees are prohibited from using the organization's computer until they have obtained approval and registered for computer access.

• Regularly check if the antivirus program is functioning properly and update the virus definition database at least once a day. If any abnormalities are detected, promptly notify the relevant IT personnel for immediate resolution. (IT personnel should receive training on antivirus program inspection methods.)

• Individuals responsible for publishing data to the public through various channels, such as the organization's website, must verify the accuracy of the data. If any errors are found in the content, they must take responsibility for those errors.

• Individuals responsible for publishing data to the public through various channels must handle the process themselves and should not allow others to handle it on their behalf. They should only disclose the necessary information.

• Personal computers should be shut down when not in use or if there is no activity for more than 1 hour, unless the computer is a server that needs to operate 24 hours a day.

• Configure the screen server of personal computers under your responsibility to lock the screen after 10 minutes of inactivity.

• Delete unnecessary data from personal computers to save storage space on storage media.

• Exercise caution and maintain personal computers and network systems similar to how individuals generally handle personal computers and network systems, depending on the circumstances.

• Do not install additional computer programs beyond those provided by the organization for use.

• Do not modify or alter legally licensed software purchased by the organization.

• Do not install computer programs or devices that infringe on the intellectual property rights of others.

• General employees are prohibited from installing computer programs for data analysis on the network system.

• Do not install additional computer programs or devices on personal computers within the organization to allow others to use those personal computers or the organization's network system.

• Do not use personal computers of employees with the organization's network system, unless it has been approved by the IT department and has been checked beforehand.

• Approval must be obtained from authorized personnel before removing any computer devices from the office area each time.

• Install an Uninterruptible Power Supply (UPS) for personal computers that handle a large amount of data and require high frequency usage.

• Do not make any modifications to the system configuration that was initially installed, as it may cause damage to the computer system's operation.

• Do not remove or relocate installed devices without notifying the responsible IT department in advance.

• Do not install additional peripheral devices for the computer, such as headphones, microphones, or printers, without informing the IT department responsible for installation.

• Do not enter the location where the computer network system is located (server room) without permission.

Computer users must be aware and understand and comply with the Computer-Related Offenses Act BE 2560, announced by the Ministry of Information and Communication Technology on January 23, 2560, strictly.

Category 2 Internet Usage Guidelines

• Prohibited from downloading or sharing illicit media files.

• Prohibited from downloading large files unnecessarily.

• Internet usage should be work-related, and unnecessary usage during peak network hours should be avoided.

• Prohibited from playing games, watching movies, or listening to music online.

• Prohibited from accessing websites related to the following categories:

1. Gambling
2. Auctions
3. Discussions related to nationality, religion, and monarchy

4. Illicit activities as defined in the Computer Crime Act (Version 2) BE 2560, Section 14

5. Any other activities that are illegal or unethical.

• Prohibited from using chat programs in chat rooms (e.g., online social platforms such as Facebook/Instagram/Line/WeChat/WhatsApp/Skype/Twitter, etc.), except for authorized work-related purposes.

• Prohibited from using internet data that violates copyright laws of the data owner.

• Prohibited from using the internet to distribute or disseminate the following:

1. Electronic publications that infringe on copyright.

2. Confidential information of the organization to unauthorized individuals.

3. Personal information without consent.

• Prohibited from using the internet to engage in activities that may damage the organization's image and reputation.

Category 3 Guidelines for Email Usage

• Prohibited for employees or unauthorized individuals to access other people's email without permission.

• Prohibited from registering with an email address provided by the organization for websites unrelated to the organization's work.

• Prohibited from sending spam emails.

• Prohibited from sending chain letters via email.

• Prohibited from sending emails that violate laws or the rights of others.

• Prohibited from intentionally sending viruses to others via email.

• Prohibited from impersonating or disguising one's email address when sending emails to others.

• Prohibited from sending emails that disrupt the computer systems of others.

• Prohibited from falsifying or altering other people's email.

• Prohibited from receiving or sending emails on behalf of others without permission.

• Prohibited from using inappropriate language in email communications.

• Prohibited from sending emails with file sizes exceeding 10 megabytes or as specified by the organization.

• Prohibited from sending confidential emails of the organization unless using the encryption method specified by the organization.

• Use caution when specifying the correct email address of the recipient.

• Always include the sender's name in every email sent.

• Exercise caution in limiting the recipient group of emails to those who need to know.

Note: Category 3 is subject to penalties under the Computer-Related Offenses Act (No. 2) B.E. 2560, Section 4.

Category 4 Rules and Regulations for Preventing Misuse of Resources

Employees must not use the network system with the following objectives:

• To engage in illegal activities or cause damage to computer data or computer systems related to national security, public safety, economic stability, or public services.

• To disrupt public order or good moral conduct.

• For commercial purposes, entertainment, or personal benefits.

• To disclose confidential information obtained from performing work duties for the organization, whether it is organizational or external individuals' data.

• To engage in activities that violate the intellectual property rights of the organization or other individuals.

• To access information without permission from the owner or authorized personnel.

• To express personal opinions regarding the organization's operations on any website in a manner that may cause misunderstandings or deviate from the truth.

• For any other actions that may undermine the organization's interests, cause conflicts, or harm the organization.

• The IT department may conduct random checks on computers or portable devices, along with various peripherals, as deemed appropriate. Computer owners and peripheral device owners must cooperate in the inspection process.

• To tamper with computer data that may cause harm to others or the general public.

• To distribute or forward falsified computer data to others.

• To introduce any computer data into a computer system, where such data is considered, a crime

related to national security or a criminal offense under the law.

• To introduce any computer data into a computer system that has the nature of contagion, and such computer data can be accessed by other employees or the general public.

• To distribute or forward contagious computer data to others.

• To create, edit, or modify images electronically or by any other electronic means that may cause harm to others.

• To collect computer data that represents images of others, and these images are created, edited, or modified electronically or by any other electronic means that may cause harm to the person.

Category 5 Password Policy Guidelines

• Passwords received from the organization must be kept confidential.

• Passwords must have the following characteristics:

- Be at least 8 characters long.
- Include a combination of uppercase letters, lowercase letters, numbers, and symbols.
- Not be based on the individual's name, surname, family members, or closely related individuals.
- Not be based on dictionary words.
- Usernames must be unique (Unique User ID).

• Passwords must be set for accessing shared data files through the network system.

• The use of computer programs to automatically save passwords (Save Password) is prohibited.

• Passwords must not be written down or recorded in easily observable places by others.

• Allowing others to access the computer network using one's own user account is prohibited.

• If it is necessary to disclose the password to others due to work-related reasons, the password must be changed immediately after the task is completed.

• Users who share the same user account and password are jointly responsible for any damage or issues that occur within the accessed system.

• System users must change their passwords every 90 days.

• Setting secret passwords (Set Password) for computer hardware, including BIOS and operating systems, is prohibited unless authorized by the IT authority and assigned personnel.

• Employee passwords are considered company assets. The company strictly prohibits disclosing personal password information to others, and all employees have a responsibility to protect the company's passwords.

• If there is a need to cancel a username and password, it must be directly reported to the supervisor to initiate the cancellation process. This should be done immediately upon discontinuation, and the assigned IT personnel must promptly deactivate the user account and password upon receiving the cancellation request.

• If any employee's username and password are found to be involved in a violation under the Computer Crime Act that causes harm to the company, the person responsible for the username and password must accept sole responsibility.

Category 6 Accessing and Using a Server

• Unauthorized access to the server room is strictly prohibited before obtaining permission.

• Employees are not allowed to enter the server room unless they have relevant duties.

• Food and beverages are not allowed in the server room.

• External individuals visiting the server room must always wear a visitor's badge for clear identification, unless they are company employees.

• Keep a record of entry and exit to the server room by external individuals in a logbook.

• If any abnormalities are observed in the server room, such as missing assets or signs of intrusion, immediately inform the IT manager.

• Prohibit the entry of devices capable of capturing images into the server room, such as mobile phones, digital cameras, and video cameras.

• Strictly follow the instructions provided by the staff responsible for the server room.

Category 7 Code of Conduct for Information Management

For information in paper document format:

• Use a document shredder to destroy confidential or highly sensitive documents.

• Prevent unauthorized access to confidential or highly sensitive documents by ensuring that

printed copies are properly secured.

• Categorize and store confidential or highly sensitive documents separately and ensure they are adequately protected.

• Make copies of confidential or highly sensitive documents only after obtaining permission from the document owner.

• Exercise caution when distributing or disseminating confidential documents within the organization to individuals who have a legitimate need to know.

• Verify the accuracy of documents before using them.

• For confidential or highly sensitive documents sent through postal mail, the document owner should establish secure mailing procedures.

Category 8 Electronic Information
(Electronic files, web data, emails, voice mails, and multimedia data)

• Categorize electronic data that is classified or highly sensitive separately and ensure sufficient security measures are in place.

• Make copies of classified or highly sensitive electronic data only with permission from the data owner.

• Exercise caution when distributing or disseminating classified electronic data to individuals who have a legitimate need to access and be informed of such data.

• Data owners should verify the accuracy of electronic data before using it.

• Prohibit the mailing of classified or highly sensitive electronic data unless encrypted according to organizational guidelines.

• Send computers intended for disposal to the IT department to ensure proper formatting of electronic data on the hard disk.

• Prohibit anyone from making copies (copying) of data from the computer using any method (such as saving on various storage media, including floppy disks, hard disks, CDs, DVDs, handy drives/flash drives, etc.). Such actions are in violation of the Computer-Related Offenses Act (No. 2) B.E. 2560, Section 18.

Note: If there is a necessity to remove such data from the company premises, it must be notified to and authorized by the supervising authority. Failure to do so may be considered as unauthorized intent.

Category 9 Guidelines for Accessing the System

• When a new employee begins their duties, their supervisor should submit a request to access the system of "Plan B Media Public Company Limited" using the "System Access Request Form" (FM-MIS-S-001) to request login credentials for the company's system. The request should be forwarded to the appropriate authorities according to the hierarchy and notified to the Information Technology department.

• Unauthorized access to other systems not approved for use is strictly prohibited. (Approval for system access must be obtained through the company's "System Access Request Form" only).

• Accessing protected computer data and unauthorized systems is strictly prohibited.

• Users must log out of the system immediately upon completing their tasks.

• Users must not disclose any information related to the organization's computer system access security measures to external parties.

• Users must not use the organization's computer resources to intercept or gather data from the organization's or others' computer systems during data transmission and unauthorized system access.

Category 10 Security Incident Reporting Guidelines

The staff members should immediately report the following security incidents to the IT department:

• Malicious software programs.

• Network intrusions or breaches.

• Unauthorized changes or loss of critical data.

• Unauthorized disclosure of sensitive information.

• Misuse of important data.

• Unauthorized use of IT resources.

• Identification of vulnerabilities in software, systems, or hardware.

• System outages due to attacks.

• Theft of IT resources.

• Authorization granted to external individuals to access the organization's systems.

• Covert installation of software to capture or monitor data within a network.

• Other incidents that violate the organization's security policy and require cooperation and facilitation from superiors or network administrators in investigating security incidents that occur within personal computer systems and network security systems, as well as following the recommendations of superiors or network administrators strictly.

Category 11 Punishment

• If an employee violates the policies regarding the use of information technology systems, resulting in damage or potential damage to the organization as determined by the management, the employee involved shall be informed and agree that the organization has the right to impose appropriate penalties. These penalties may include verbal warnings, written notifications, disciplinary actions, or termination of employment, in accordance with the rules and regulations of the organization.

• In the case of severe damage caused intentionally or through deliberate misconduct that significantly affects the organization, the employee involved shall be informed and agree that the organization has the right to take necessary actions as mentioned above. This includes the employee's consent to compensate the actual damages incurred by the organization due to the misconduct.

Effective July 1, 2019

- Pinijsorn Luechaikajohnpan -

(Pinijsorn Luechaikajohnpan, Ph.D.)

Authorized Director