บริษัท เอเชียน มารีน เซอร์วิสส์ จำกัด (มหาชน)

ASIAN MARINE SERVICES PUBLIC COMPANY LIMITED

Announcement No. EXC-A67054

Subject: Cybersecurity Policies

Objectives

1. To establish policies, guidelines, requirements, and operational procedures to ensure that executives, officers, system administrators, and external personnel working with Asian Marine Services Public Company Limited understand the importance of information security and safety and comply with them appropriately.

2. To build confidence in the organization's information security, ensuring that information is accessible only to authorized person (Confidentiality), is accurate and complete (Integrity), and is available for utilization (Availability).

3. To disseminate these policies to officers and information users of Asian Marine Services Public Company Limited for strict compliance.

Scope

1. Establish a written information security policies with guidelines, requirements, and operational procedures for maintaining information security, in compliance with applicable laws, principles, and international standard principles of information security.

2. Provide information, information technology systems, information technology equipment, premises and environments related to information, development and maintenance of information systems, along with anything related to information, with appropriate and sufficient security, and with clearly defined access controls based on the principles of appropriate and secure operational needs.

3. Provide a data backup system, a data recovery system, and a backup system to substitute primary information technology systems in case of emergency. The backup system must be readily available, and an emergency preparedness plan should be in place.

4. Conduct regular information risk assessments aligned with the IT department's risk management approach.

5. Ensure inspection and corrective action are taken when security breaches occur, along with preventive measures to avoid recurrence, and maintain clear records and reports.

6. Users are provided with information on policies, guidelines, standards, and regulations related to information security, and must strictly adhere to and comply with them.

Definitions

1. Information security refers to protecting the confidentiality, integrity, and availability of information in accordance with the security requirements of that particular information, including the security of the organization's information technology and communication systems.

2. Guidelines refer to recommended practices to help achieve objectives more easily.

3. Standard refers to a mandatory rule or benchmark applied in actual operations. to achieve the objectives.

4. Procedure refers to the detailed, step-by-step instructions to be followed in order to achieve the defined objectives.

5. User refers to an authorized individual permitted to access the organization's information and communication technology system according to their rights and responsibilities.

6. Information Technology Officer or "IT Officer" refers to an officer assigned to access and maintain the organization's information and communication technology systems, categorized as follows:

- "System Administrator" refers to an individual designated by their supervisor to be responsible for the maintenance of an organization's information and communication technology systems, including both hardware and software. This role has access to work systems or database management systems, such as setting user permissions, among other tasks.

– "System Developer" refers to a person assigned by their supervisor to be responsible for developing information and communication technology systems.

– "External Personnel" who come to install or maintain information and communication technology systems, and to provide consultation or perform the contract.

7. Computer data refers to data, text, commands, command sets, or anything else within a computer system that the system can process, and includes electronic data under the law on electronic transactions.

8. "Computer traffic information" (Log) refers to data relating to computer system communications, indicating the origin, source, destination, date, time, quantity, duration, type of service, or other information relevant to that system's communication.

9."Information" refers to facts derived from processed data, organized and presented in a systematic form—whether numbers, text, or graphics—that is easily understandable and useful for management, planning, decision-making, and other applications. This includes information in both electronic and non-electronic formats.

10. "Access or control of information usage" refers to authorizing, defining rights, or delegating authority to users and external agencies to access or use information systems, information processing equipment, and networks, both electronically and physically.

11. "Computer System" refers to a device or a set of computer devices connected to work together, programmed with commands or instructions that enable the device or set of devices to automatically process and store data.

12. "Network System" refers to a system used for communication or the transmission of data and information between an organization's various information technology systems, such as intranet and internet systems.

— "Intranet System" refers to an electronic network that connects various computer systems within an organization. It is designed for internal communication, information exchange, and data sharing.

— “Internet System” refers to an electronic network system that connects various organizations’ computer networks to the global Internet.

13. “Information Technology System” refers to an organization’s work system that leverages information technology, computer systems, and network systems to generate information that the organization can use for planning, management, service support, and the development and control of communication. Its components include computer systems, network systems, programs, data, and information.

14. “Computer System Control Room” or “Server Room” refers to a room designated for the installation of core equipment of the organization’ computer and communication system equipment, such as server computers, data storage devices, and network devices, etc.

15. “Data Subject” refers to the individual or department responsible for information and document assets, whereby the data subject is accountable for the data or directly affected by its loss.

16. “System Owner” refers to the individual or department responsible for the system. The System Owner is responsible for the operation of that system and is directly affected if the system is compromised.

17. “Information Assets” refer to information and document assets, software and application assets, hardware assets, service assets, and people assets related to information work.

18. “Electronic mail” (e-mail) refers to a system individuals use to exchange messages via computers and interconnected networks. This information can include text, photographs, graphics, animations, and sound. Senders can transmit messages to one or more recipients, and these messages are stored in a designated mail box for each user on the network. Recipients can then open and read the messages, print them, or delete them.

19. “Username” refers to a combination of letters and numbers assigned for accessing an information system with defined access permissions.

20. “Password” refers to letters, characters, or numbers used to verify a person’s identity and control access to information and information systems, thereby maintaining the security of data and information technology systems.

21. “Malicious software” refers to a set of instructions that cause damage, destruction, alteration, or addition to a computer, computer system, or other programs, resulting in malfunctions or failure to operate as specified.

22. “IT Security Incident” refers to an undesirable or unexpected security event that may compromise the organization’s information system and threaten its security.

23. “Critical and High-Impact Systems of the Organization” include the online project management system and the financial accounting and inventory system.

Roles and Responsibilities

Policy level

Responsible for establishing policies, providing recommendations and consultation, and overseeing, supervising, controlling, and auditing staff at the operational level, including the Information Technology Department Manager.

Operational Level

Responsible for overseeing the work of personnel, studying and reviewing plans, and monitoring risk management and the security of databases and information technology security systems. The responsible person is the IT Support position.

Responsible for maintaining the system and network, including checking, maintaining, and troubleshooting computer and network systems, as well as performing database backups. The responsible person is the IT Support position.

Responsible for maintaining the security of each database system. The responsible person is the Programmer position.

Security Principles

Asian Marine Services Public Company Limited implements usage and access controls for data and information systems in order to establish measures to prevent unauthorized access to data and information systems, physical intrusion, network-based intrusions, and malicious software that could damage data or disrupt systems, while ensuring accurate audit trails and identity verification of persons accessing the organization's data or information systems, based on the following principles:

1. Confidentiality: Access to data is restricted to authorized individuals, and controls are in place to prevent unauthorized disclosure of confidential data.

2. Integrity: Maintain the accuracy and completeness of information, and control errors to prevent unauthorized modification, deletion, or changes to data.

3. Availability: Only authorized users can access data within the agreed timeframe. Responsible personnel must control the systems to prevent disruption, maintain continuous operational performance, and prevent any incidents that could cause system downtime.

1. Information Access Control (Folder/File Shared)

1.1. Users may access information and information technology systems needed for their work only with authorization from their supervisors/ data subjects/ system owners, and only to the extent necessary. Access requests must follow established procedures and utilize designated forms.

1.2 User Registration: Establish a user registration form which must contain at least the following basic information: full name, position, department, and duration of use.

1.3. Deactivate users from the registry by following the user deactivation process when their assignments end, such as with job transfers or resignations.

1.4. Define user rights for accessing information and computer systems, such as the rights to use computer system programs (Application System) and internet access, appropriately based on roles and responsibilities. Grant users only the rights necessary to perform their duties, with written approval from an authorized person, and review these rights regularly.

1.5. Access rights or privileges should be granted to specific individuals or groups only when necessary. In the event that a user who is the owner of critical data needs to grant access privileges to another user to

access or modify their data, such as through file sharing, the duration of usage must be defined and such privileges must be revoked immediately once no longer necessary or upon the expiration of the specified period.

1.6. Review user access rights at least once a year, and re-review them according to the defined schedule or whenever changes occur, such as promotions, demotions, transfers, or job terminations.

2. Protecting Devices When Unattended

2.1 Users should immediately log out of the organization's information technology system when they finish using it, such as logging out of application systems, computers, or devices in use.

2.2 Users should prevent unauthorized access to the computer or information technology system by requiring a correct password before allowing access to the computer.

2.3 Users must configure their computers to automatically lock the screen after a period of inactivity, such as 15 minutes. After the screen locks, a valid password is required to unlock it and access the computer or system.

2.4 Users should turn off their personal computers when they have finished their daily work or have not used them for more than 1 hour, except for computers operating as servers that must be available 24 hours a day. In those cases, the system administrator should log out of the server operating system or lock the screen.

3. Network Access

3.1. Set up a network system to provide services to the organization's personnel and authorized users only.

3.2 Users are prohibited from taking any actions regarding information that violates the law or accepted standards of public morality. Users warrant that any such actions are solely their responsibility and are not the responsibility of the organization.

3.3. Users are not permitted to engage in any activities for commercial purposes or to profit through the use of computers and networks, including posting advertisements, buying or selling products, trading information, charging for information search services, or providing advertising services.

3.4. Prohibited infringement on others: Users must not read, write, delete, alter, or modify content that does not belong to them. Hacking into other users' accounts, disseminating any statements that cause damage or defamation to others, or using improper language or writing statements that cause harm to others are all considered infringements of other persons' rights. The user shall be solely liable, and the organization shall bear no responsibility for any such damages.

3.5. Unauthorized access by any individual is prohibited. Any intrusion into or attempt to intrude into the system will be considered an attempted violation.

3.6 Users are prohibited from transferring or giving this user account to others, as user accounts are assigned to individuals only.

3.7 Users are responsible for any consequences resulting from the use of the user accounts provided by the organization, including any damages, unless they can prove the damage was caused by the actions of others and not by their own negligence.

3.8. Users of the organization's network must authenticate every time they use the service.

3.9 Users of the organization's wireless network are required to use the network name, or SSID (Sub Station Identifier), and will have access for a period determined by their status, permissions, or user type.

3.10. The use of Bring Your Own Device (BYOD) to connect to the corporate network is subject to security verification of the devices before access is granted.

3.11. Users are allowed to access the network only for the information services they are authorized to use.

3.12. The use of all entertainment programs is prohibited during work hours, except for individuals specifically exempted by their supervisor as necessary for their job duties.

4. Route Control on the Network

4.1. Use routing devices or computer network equipment to check the IP addresses of both the source and destination, allowing different networks to communicate and controlling data transfer across networks.

4.2. Implement controls to prevent disclosure of IP address allocation usage plans.

4.3. Require Network Address Translation and domain name translation to segregate subnets, or to separate internal and external networks.

4.4 Limit network routing from a single computer to the network computer or network device, strictly prohibiting users from utilizing any routing paths other than those specifically designated.

4.5. Implement measures to enforce network routing, enabling connections to designated endpoints or restricting network service access based on authorized privileges.

4.6. Any movement, installation of additional equipment, or modification of central network equipment, including routers, switches, and network-connected devices, by unauthorized individuals is prohibited without prior approval from the System Administrator.

4.7 Users are not permitted to change or configure the IP address of any computer within the department without authorization from the system administrator.

4.8. Take any necessary actions to stop users from violating these guidelines, and suspend their access to the network system if required to prevent or mitigate potential damage to the organization.

5. Access to the operating system

5.1 Provide an operating system solely for supporting organizational operations.

5.2. Any modification or configurations of the operating system must be subject to control and require written approval from the respective supervisor.

5.3. Each user shall be assigned a unique username and password for accessing the operating system or computer, limited to their designated role.

5.4. Usernames and passwords must be authenticated every time before accessing the operating system.

5.5. Configure a screen saver program to lock the screen after a period of inactivity. Users must immediately log out from the operating system upon completion of work or when leaving the screen unattended for an extended period. Re-authentication via password entry shall be mandatory to resume operating system access.

5.6. Users shall maintain strict control over their own operating system usernames and passwords, and do not share them with others.

5.7. The privilege escalation or authorization of a specific user's username and password to access another computer system must be strictly controlled and executed solely by the system administrator. The baseline environment of such computer systems must be configured to separate user accounts (Multi-User/Multi-Identity Profiles) and assign access rights based on the principle of role-based access control for that operating system.

5.8. Control the installation of the organization's copyrighted computer software on the operating system. Users must request approval from their supervisor and organizational management for any additional use as needed. Installing or using any software that infringes on copyright on the organization's operating systems is prohibited. If such software is detected, the system administrator must delete it, and the user will be held responsible for the violation.

5.9 Control the installation of general-purpose application programs. Users must request approval from their supervisors, department managers, and executives for any additional usage as needed. Users are prohibited from self-installing any copyrighted application programs on the organization's operating systems. If unauthorized installations are detected, the system administrator will remove them, and the user will be held responsible for the violation.

5.10 Control the installation, uninstallation, or modification of software or application configurations, ensuring the system administrator considers the impact on the operating system before proceeding.

5.11. The use of the organization's operating system software is prohibited for any commercial purpose or personal benefit.

5.12. Users of the operating system are prohibited from attempting to control other computers by connecting from within the system to external networks or allowing external connections to the system without authorization from the system administrator.

5.13. Controls shall be enforced to terminate sessions during prolonged inactivity and lock the screen for critical operating systems.

5.14. Connection session timeouts for accessing critical or high-risk operating systems shall be strictly controlled and restricted to a designated timeframe or as specified by the administrator.

5.15 Maintain a system for logging operating system access, including the username, date, and time of login and logout.

5.16 Users are prohibited from installing, uninstalling, altering, modifying or copying the operating system for use outside of the organization without permission. The operating system provided by the organization is essential and critical for users.

5.17. Do not modify the BIOS without permission from the IT department, as this can impact computer functionality and the operating system.

5.18 It is required to have the preparation and announcement for use of measures of proceeding for offenders.

6. Access to information systems and applications (ERP system)

6.1. The system administrator must control, restrict, or grant access to information, data, and functions of the information system and applications as follows:

— Registration is required for identity verification and authentication.

— Access shall be permitted exclusively to the sub-systems and functions that are necessary for work and that have been authorized only.

— Access shall be restricted exclusively to the data that is operationally necessary and explicitly authorized.

— The transfer or assignment of access privileges to other persons is strictly prohibited; access rights shall be granted strictly on an individual basis.

— Access privileges must be revoked immediately upon the authorized person no longer retaining the right to access the system.

6.2. The system administrator must control or restrict access rights to systems accessed from other systems as follows.

— Access shall be restricted exclusively to the functions that are operationally necessary and explicitly authorized

— Access shall be restricted exclusively to the data that is operationally necessary and explicitly authorized.

— Authentication must be required every time before accessing the system.

— The routing and methods used to access a system from another system must be restricted.

— A review of access privileges must be conducted at least once a year.

6.3. System administrators must control or restrict the exportation of data from the system, allowing only relevant and necessary information for operational use.

6.4. The active system must display only basic information to users, providing access only to the information necessary for their roles and permissions.

6.5. The active system must be configured with constraints to prevent the system from displaying any assistance when undesirable events occur within the system.

6.6. The active system must have a function to check and control logins as follows.

— Display only the necessary details of the application system after the login process has been successfully completed

— Restrict the system from displaying operational or usage error messages in a manner that discloses the internal information of the system.

— Logging of login data must be maintained for both successful and unsuccessful attempts.

— Display the date and time of the last login attempt (for both successful or unsuccessful attempts).

Guidelines for Preventing Cyber Attacks

The Information Technology Department has implemented information technology to improve operational efficiency and enhance employee convenience. However, the information technology system may suffer damage from cyberattacks, computer viruses, personnel, and various internal and external factors, potentially disrupting company operations. Therefore, the Information Technology Department has established the following preventive guidelines:

1. Prevention of Incidents Caused by Officers or Personnel of the Agency (Human Error): Officers or personnel of the agency may lack sufficient knowledge and understanding of computer hardware and software, potentially cause damage to the information technology systems, rendering them unusable, disrupted, or halted, thereby resulting in the inability to utilize the information technology systems at full efficiency. Therefore, to enhance basic knowledge and understanding of information technology system usage, arrangements have been made for personnel to attend training and seminars to acquire fundamental hardware and software skill to minimize the risk of human error.

2. Prevention of Incidents Caused by Computer Viruses.

2.1. Install antivirus software and keep its virus definitions updated. Antivirus software is installed on both the server and client machines to detect viruses entering the network, and virus scans are conducted at least once a week.

2.2 Install a firewall to prevent unauthorized persons from the Internet from accessing the Company's information system and computer network. The firewall will have an "Intrusion Prevention System" (IPS) enabled at all times to monitor for external threats. If the system detects an intruder or cybercriminal, it will immediately block the intrusion.

2.3 Notify users of computer virus alerts via the internet network, including recommendations for preventing and eliminating viruses, and enable them to learn and implement basic protective measures, such as:

2.3.1. Exercise caution against threats from opening files from various storage media such as external hard drives, CDs, and flash drives.

- Avoid opening files with strange, unknown, or suspicious extensions.
- Do not use storage media of unknown origin.

2.3.2 Exercise caution when opening emails.

- Do not open email files from unknown sources.
- Delete emails immediately if the source is unknown.

2.3.3 Exercise caution when downloading files from the Internet

- Do not open unknown files attached to chat programs like ICQ and MSN.
- Do not open websites recommended in emails from unknown sources.
- Do not download files from untrusted websites
- Regularly monitor alerts for various virus attacks.
- Avoid unnecessary file sharing

3. Server Room Access Control and Damage Prevention Measures: Unauthorized personnel are prohibited from entering the server room. If access is necessary, a member of the IT department must escort them. The entrance door is secured with an encrypted lock and monitored by CCTV cameras to prevent theft.

4. Data backup: To prevent potential damage when data is destroyed by computer viruses, intruders destroying or altering data, or disasters, etc., ensuring that backup data can be restored for use. The system is configured to perform automatic daily data backups for the servers. Backup data is stored on storage devices within the Information Technology Department and in the server room. In addition, the department maintains a backup site at the Surat Thani branch to support efficient data backup and recovery during emergency situations.

Therefore, this announcement is made for all employees' acknowledgment

Announced on December 10, 2024

-Signature -

(Mr. Suradej Tanpaibul)

Chief Executive Officer