ORNSIRIN

Information Technology Policy

1. Principles and Rationale

Ornsirin Holding Public Company Limited and its subsidiaries recognize the importance of utilizing information technology in business management. Therefore, this policy has been established to provide a framework for the governance and management of information technology at the organizational level, in alignment with good corporate governance principles as well as relevant laws, and to ensure suitability with the business context.

2. Definitions

Network System = The Company's computer network system.

Server Computer = A computer within the network system that serves as a central unit, such as for data storage or software services for other computers, or for controlling operations within the network.

Computer = An electronic device used for data processing that operates according to software instructions to achieve desired outcomes, such as server computers, personal computers, and notebook computers.

Computer Equipment = Electronic devices used in conjunction with computers to support their operations, including computers.

Information System = The operational system of a unit that utilizes information technology, computer systems, and network systems to generate information for use in planning, management, service support, development, and communication control. Components include computer equipment, network systems, programs, operational systems, and information.

Information = Data that has been processed and organized into formats such as numbers, text, or graphics, making it easily understandable and usable for management, planning, decision-making, and other purposes.

System = The application of information technology systems in operations to achieve defined objectives, such as document management systems or vehicle booking systems.

Operating System = Software that controls the operation of a computer and allocates system resources, including memory management and control of input devices (keyboard, mouse) and output devices (monitor, printer).

Data = Messages, commands, sets of commands, or any other items within a computer system that can be created, transmitted, received, stored, or processed electronically on computer equipment, including electronic data under the law on electronic transactions.

File = Data stored on a recording medium as a single unit with a specific name, such as software programs and document files that are created, named, and stored.

User = An employee or external individual who has the right to use the Company's information technology systems.

Network Administrator = A person responsible for maintaining and managing the network.

Host/Server Administrator = A person responsible for maintaining and managing server computers.

User Account = An account used by a user to access and utilize information technology systems in accordance with the agreement between the user and the system provider.

Administrator Account = An account used by server administrators to manage server systems.

IT Help Desk = A service that provides assistance and resolves issues related to computer systems and networks.

Service Recipient = Executives and employees of the Ornsirin Group.

IT Staff = Personnel responsible for providing support and resolving issues related to computer systems and networks within the Information Technology Department.

Operating Officer = IT staff assigned to provide assistance and resolve issues related to computer systems and networks within the Information Technology Department.

SLA (Service Level Agreement) = An agreement to ensure service standards between the service provider and the service recipient, aimed at increasing confidence that services will be delivered within the specified timeframes for each process. This does not constitute a binding obligation and may be subject to change.

3. Information Security Management

Procedures

1. Establish and regularly update the information security policy.
2. Demonstrate commitment or communicate to all personnel the importance of strictly complying with the organization's information security policy on a regular basis.
3. Arrange regular meetings on information security management, with at least the following agenda items:
   - Review of compliance with the security policy and audit results
   - Preventive/corrective action plans based on audit findings
   - Improvement of the information security policy for the following year
   - Risk assessment and risk mitigation plans, including the provision of adequate personnel, budget, management, and resources for such activitie.
4. Promote information security awareness to ensure that personnel have knowledge, understanding, and the ability to protect themselves at a basic level.
5. Conduct an annual information technology risk assessment and prepare plans to mitigate identified risks or issues.
6. Ensure compliance audits of the information security policy by internal auditors and prepare plans to improve or resolve identified issues.
7. Circulate notices to all personnel to exercise caution and take care of organizational assets under their responsibility to prevent loss.
8. Clearly define network usage policies, specifying which services are permitted and which are prohibited, and update such policies as necessary.
9. Prohibit access to websites in the following categories: content related to criticism of the nation, religion, and the monarchy; gambling; pornography; and other content related to illegal, immoral, or unethical matters during working hours.

4. Management of System-Related Documentation

Procedures

1. Prepare and regularly update operational manuals to ensure they are up to date, and store them in a secure location. Such manuals shall at least cover critical systems, servers, and equipment, including:
    - System manuals for both users and administrators
    - Manuals for monitoring the status of servers and network systems
    - Manuals for inspecting systems and equipment in the server room
    - Data backup manuals
    - Manuals for monitoring system resources
2. Restrict access to operational manuals to only relevant personnel.
3. If operational manuals are stored on the network system, implement access controls to ensure that only authorized personnel can access them.

5. Network Management

Procedures

1. Regularly update the network diagram to ensure it remains up to date.
2. Segment and improve the network into groups based on usage characteristics, such as separating servers, client machines, and critical systems.
3. Restrict connections to servers or critical equipment by allowing access only from computers used by system administrators.
4. Disable unnecessary services on servers.
5. Require the use of standard programs with data encryption for connections from within the network to servers or network devices.
6. Require the use of standard programs with data encryption for remote access from outside the organization to the internal network.
7. Implement automatic patch installation on all users' personal computers within the organization.
8. Configure firewalls in accordance with the network usage policy defined by management.

6. Management of Employee Termination or Transfer

Procedures

1. Revoke access rights of employees who resign or are transferred from all systems in accordance with the Human Resources Department's procedures, within 15 days upon notification from the Human Resources Department.
2. Immediately revoke access rights of employees who resign or are transferred from all systems within 1 day in urgent cases, upon notification from the Human Resources Department.
3. Ensure verification of the accuracy of user access rights across all systems.

7. Server Room Usage

Procedures

1. Only personnel whose duties require them to work within the Data Center are permitted access to the server room.
2. Bringing external persons into the Data Center must be approved by the Chief Financial Officer (CFO).
3. External persons are prohibited from entering the server room without necessity.
4. Food and beverages are prohibited in the server room area.
5. Ensure that doors and windows of the server room are always properly closed and locked.
6. Inspect the operational condition of supporting systems, including power supply, ventilation, temperature control, and UPS systems, to ensure they are always ready for use, at least once per day.
7. Place computers, communication equipment, and other assets in secure locations, ensuring that equipment is installed in a stable position and not easily tipped or tilted.
8. Inspect fire protection equipment at least once a year to ensure it is functioning properly.
9. Maintain cleanliness and orderliness of the server room at all times; cardboard boxes or any combustible materials must not be stored in the server room.
10. Inspect and organize communication cables to ensure they are neat and orderly.
11. Ensure that communication cable rooms are always locked.
12. Establish or renew maintenance agreements for critical systems, including firewalls, routers, UPS equipment for critical systems, and air conditioning systems in the server room.
13. Ensure that critical systems, servers, and important equipment are supported by UPS systems and backup power supply (electricity power generator).
14. For internal audits or management visits to the Data Center, responsible personnel must accompany visitors into the server room and record each entry.

8. Server Resource Management

Procedures

1. Monitor server resources for critical systems. Items to be reviewed include CPU usage, hard disk usage, memory usage, and network usage, as well as overall network utilization.
2. Record resource usage data for analysis of usage trends and for planning future capacity expansion or procurement as necessary.
3. Configure and regularly verify server system time in accordance with the Computer Crime Act and ensure that critical systems maintain accurate time, with reference to “clock.thaicert.org”.

9. Computer Virus Management

Procedures

1. Ensure that antivirus protection on servers is functioning properly and that virus signature databases are continuously updated. If any malfunction is detected, immediate corrective action must be taken.
2. Install antivirus software for users with real-time scanning enabled when files are accessed.
3. Install and regularly update antivirus software on all client machines and servers supporting critical systems.

10. Data Backup

Procedures

1. Identify all critical systems and mail servers.
2. Identify servers as required by law, such as web servers.
3. Assign responsible personnel for data backup.
4. Define the types of data within systems or servers that must be backed up, at a minimum including database data and system-related data such as operating system software and other relevant software.
5. Define the frequency of data backups for such systems or servers.
6. Perform data backups according to the defined frequency and store at least one backup copy offsite.

11. Data Retention in Compliance with the Computer Crime Act B.E. 2560 (2017)

Procedures

1. Retain the following log data for at least 90 days: FTP server logs (FTP.log), Firewall/Proxy/Gateway logs (e.g., FW.log), and Web logs (Access.log).
2. Restrict access to such log data, allowing only network administrators to access it.

12. User Registration and Access Control

Procedures

1. Require registration for new users using the “User Registration Form” and assign user access rights as specified in the form, limited to only what is necessary for usage.
2. Review user accounts and access rights for employees of the Ornsirin Group, document such reviews, and retain records for future audit purposes.
3. Review user accounts and access rights for external parties, document such reviews, and retain records for future audit purposes.
4. Deliver user accounts and passwords in sealed envelopes marked “Confidential” to users, together with the document “Regulations for Computer and Network Usage,” and require users to strictly comply with such regulations.

13. System Development

Procedures

1. Conduct acceptance testing and validation of new systems by relevant users to ensure compliance with specified requirements, and only launch the system once it meets the operational needs of the organization.
2. For critical systems, establish data encryption standards for data transmission between client machines and servers, and ensure system development complies with such standards.
3. Develop systems in accordance with input data validation guidelines.
4. Perform system testing and document the test results in writing in accordance with input validation guidelines.
5. Develop systems to enforce strong password requirements in accordance with password policy, and set password validity to 90 days, after which users must reset their passwords to continue system access.

6. Collect and securely store all system source codes in a centralized location, maintain at least two latest versions, and restrict access to authorized personnel only.

7. Provide training on new systems to all relevant users.

8. Prepare user manuals for new systems, at minimum for both users and system administrators.

14. Virus Protection

Procedures

1. Verify that antivirus software is functioning properly and that virus definition databases are up to date. Such checks must be performed at least once daily. If any malfunction is detected, immediate corrective action must be taken.

2. If a user's computer does not have antivirus software installed, or if a virus is detected and cannot be removed by the antivirus program, the incident must be reported to the Information Technology Department immediately.

3. Service requests must be submitted using the computer service request form or through the IT Department's service system.

15. Copyright and Intellectual Property Protection

Procedures

1. Installation of computer programs that infringe upon the intellectual property rights of others is prohibited.

2. Exercise caution when using documents or data in any format that are subject to usage conditions, and strictly comply with such conditions to avoid infringement of intellectual property rights of others.

16. Storage of Documents and Electronic Data

Procedures

1. General document storage within the information function shall be retained for a period of 2 years.

2. Document storage related to personal data within the information function shall be retained for a period of 2 years from the contract expiration date.

3. General electronic data storage within the information function shall be retained for a period of 5 years, while other departments shall follow ISO-based retention periods applicable to each department.

4. Electronic data storage related to personal data within the information function shall be retained for a period of 2 years from the contract expiration date.

17. Disposal of Damaged or Unused Storage Media

Procedures

1. Disposal of document data shall follow the retention period specified in Clause 16.1. Documents shall be destroyed by shredding or incineration, and such destruction must be approved by an authorized signatory from the Information Technology Department.

2. Disposal of general electronic data that is no longer in use or has reached the retention period, as specified in Clause 16.2, shall be carried out by deleting or wiping the data. Such disposal must be approved by an authorized signatory from the Information Technology Department.

3. In cases where personal data is stored on hard disks, thumb drives/flash drives, external hard disks, or other electronic media, the data shall be wiped within 30 days upon notification. Destruction shall be carried out upon approval from an authorized signatory of the Information Technology Department and the Data Protection Officer (DPO).

4. Disposal of unused storage media, such as hard disks, thumb drives/flash drives, and external hard disks, shall be performed after 3 months by wiping the data so that the devices can be reused. Such disposal must be approved by an authorized signatory from the Information Technology Department.

5. Disposal of damaged storage media, such as hard disks, thumb drives/flash drives, and external hard disks, shall be carried out within 9 0 –1 5 0 days using methods such as crushing, dismantling, or magnetic destruction to render the media unusable. Such destruction must be approved by an authorized signatory from the Information Technology Department.

18. Computer and Network Usage

The regulations governing the use of computers and network systems, including connection policies, aim to provide understanding of the Company's computer and network usage rules under the supervision of the Information Technology Department. These regulations outline the rights, duties, and practices for system users.

1. Definitions under this regulation

"Company" means Ornsirin Holding Public Company Limited.

" Information Technology Department" means the Information Technology Department of Ornsirin Holding Public Company Limited.

"Computer and Network Systems" mean computers owned by the Company, both within and outside the central office, including peripheral devices, network equipment connecting computers within the Company, as well as programs and data that are not designated as public media.

"Department" means various departments of Ornsirin Holding Public Company Limited.

"User" means employees authorized by the Company to use computer and network systems.

"Penalty" means disciplinary actions determined by the Company or penalties prescribed by law.

2. Computer and Network Usage Regulations

The Company's computer and network systems are Company property. Unauthorized access is strictly prohibited.

1. Users must unconditionally acknowledge and comply with all rules and policies established by the Company. Claims of unawareness of such rules or policies shall not be accepted.
2. User Accounts are assigned on an individual basis only. Users are not permitted to transfer, sell, or grant such rights to others.
3. Users are responsible for all consequences arising from the use of their User Accounts, including any damages, unless it can be proven that such damages were caused by another party.
4. Users are prohibited from engaging in any activities involving information that violate laws or public morality. Any such actions shall be deemed outside the Company's responsibility.

5. Users are prohibited from engaging in commercial or profit-seeking activities through the Company's computer and network systems, such as advertising, buying or selling goods, providing paid information services, or offering internet services for profit.
6. Users must not infringe upon the rights of others, including unauthorized reading, writing, deletion, modification, or alteration of data not belonging to them; unauthorized access (hacking) to other user accounts or departmental systems; dissemination of harmful or defamatory content; use of inappropriate language or images; or any actions causing harm to others. Users shall bear sole responsibility for such actions, and the Company shall not be liable for any resulting damages.
7. The Company does not control the content of data stored or transmitted through its systems and does not guarantee the quality, availability, or reliability of such systems. The Company shall not be responsible for any damages arising from system failures, communication issues, delays, data loss, misdelivery, or unauthorized access by other users.
8. Use of the network system for illegal activities or activities that violate information security policies is prohibited.
9. Unauthorized destruction, damage, modification, alteration, duplication, or addition of others' data or information is prohibited.
10. Dissemination of false information or any actions that may cause damage to others or the Company is prohibited.
11. Dissemination or storage of obscene, immoral, or inappropriate content, including altered or manipulated images that may damage others' reputation or cause humiliation, is prohibited.
12. Use of network resources and services for business purposes is prohibited.
13. Any actions that infringe upon the intellectual property rights of others are prohibited.
14. Any actions that disrupt or degrade network performance or interfere with system operations, assets, or services are prohibited.
15. Destruction or attempted destruction of network security systems is prohibited.
16. Access to websites that pose risks of computer viruses, such as gaming, pornographic, or gambling websites, is prohibited.
17. Downloading or storing data, images, or any content that may introduce viruses or infringe copyright is prohibited.
18. Users are prohibited from using personal computers or peripheral devices for Company work or connecting them to the Company's systems without authorization. If necessary, approval must be obtained from the respective department and the device must be registered with the Information Technology Department.
19. Use of social media for obscene, immoral, or unethical activities, profit-seeking business, or activities that infringe copyright or intellectual property rights is prohibited.
20. In cases where users violate information security policies or procedures, termination of user access shall be at the discretion of the user's supervisor and the Chief Financial Officer (CFO).
21. Users agree to comply with all terms, rules, regulations, and guidelines established by the Company, including any future amendments, which shall be effective without prior notice.

22. The Company reserves the right to deny, suspend, or terminate access or usage of its systems for users who violate or attempt to violate these regulations.
23. Users are prohibited from downloading copyrighted music and storing it on Company-owned computers.
24. Requests for Administrator privileges must be approved by the Chief Financial Officer (CFO), with clearly stated justification and duration of access.

3. Email Usage

Procedures

1. Unauthorized access to another person's email is prohibited.
2. Sending spam emails is prohibited.
3. Sending chain letters is prohibited.
4. Sending emails that violate laws or the rights of others is prohibited.
5. Intentionally sending emails containing viruses to others is prohibited.
6. Impersonation or falsification of another person's email is prohibited.
7. Sending or receiving emails on behalf of others without authorization is prohibited.
8. Sending emails exceeding the system's size limit or organizational specifications is prohibited.
9. Sending confidential organizational information via email is prohibited unless encryption methods specified by the organization are used.
10. Exercise caution in specifying recipient email addresses to prevent misdelivery.
11. Limit email recipients to only those who need to know the information.
12. Use polite language in all email communications.
13. Clearly identify the sender's name in every email.
14. Perform email data backup as necessary.
15. For work-related and important information, only the Company's designated email system must be used to prevent data leakage.
16. Employees who need to use non-company email for work purposes must submit a request form to the Information Technology Department.
17. If an employee is found using non-company email for work purposes without approval, the Information Technology Department will report the violation to the Human Resources Department for disciplinary action in accordance with Company regulations.

19. Prevention of Misuse of Resources

Procedures

1. Prohibited from using resources for illegal activities or causing damage to others.
2. Prohibited from using resources in violation of the Computer Crime Act.
3. Prohibited from using resources in ways that contradict public order or good morals.
4. Prohibited from using resources for commercial purposes, personal gain, or political interests.
5. Prohibited from accessing, displaying, storing, distributing, modifying, creating, or recording inappropriate content, such as false information, content affecting national security, religion, or the monarchy,

obscene content, manipulated images of others, or content that may damage the reputation of the organization or individuals.

6. Prohibited from disseminating or allowing others to disseminate information that defames or harms others, resulting in legal action or damage to the organization.

7. Prohibited from disclosing confidential information obtained through work, whether it belongs to the organization or external parties.

8. Prohibited from obstructing or attacking the network systems of the organization or other external entities.

9. Prohibited from distributing viruses, worms, trojans, spyware, spam emails, or other malicious programs.

10. Prohibited from expressing personal opinions related to the organization's operations through websites or communication channels in a manner that may cause misunderstanding.

11. Prohibited from posting on any website or discussion forum in a way that may lead to misinterpretation or misunderstanding of facts.

12. Prohibited from any other activities that may conflict with the organization's interests or cause disputes or damage to the organization.

20. Notebook Computer Usage

Procedures

1. For shared notebook computers, a borrowing and return form must be completed to obtain approval for usage and to prevent loss.

2. Regularly verify that the antivirus software is updated with the latest virus definitions.

3. Exercise caution and safeguard notebook computers when used outside the workplace to prevent loss or unauthorized access to data.

4. Do not leave notebook computers unattended in public places or meeting rooms.

5. Ensure that a screensaver with automatic screen lock is configured to activate after no more than 15 minutes of inactivity.

21. Password Policy and Protection

Password Requirements

1. Passwords must be at least 8 characters in length for both computer access and the Real Estate Management System (RMS).

2. Passwords must include a combination of lowercase letters, uppercase letters, numbers, and symbols.

3. Passwords must not be based on dictionary words.

4. Passwords must be changed every 3 months.

22. Password Management and Protection Procedures

Users must keep their passwords confidential and must not disclose them to others.

1. Passwords must comply with the defined password policy requirements.

2. Passwords must not be saved in computer programs for convenience (e.g., browser password saving features).

3. Passwords must not be written down or stored in places that are easily visible to others.

23. Public Disclosure of Information

Procedures

1. The owner of the information to be disclosed to the public, such as through the Company's website, must verify the accuracy of the information prior to publication. If any errors occur in the content, the information owner shall be responsible for such errors.

24. Security and Protection Against Loss of Electronic Files

Procedures

Ornsirin Holding Public Company Limited utilizes the Real Estate Management System (RMS) for storing accounting and customer data within computer systems. The following procedures apply:

1. Employees responsible for data entry must be assigned a username and password for system access, with access rights (Access_menu) limited strictly to their job responsibilities.

2. All employees are trained on customer data protection and must comply with confidentiality requirements.

3. All users of the Real Estate Management System (RMS) must log out of the system whenever they are not actively using the computer.

4. All users of the Real Estate Management System (RMS) must change their passwords every 3 months.

5. The system must be able to detect errors and provide audit trails to trace access, data entry, or modifications, including timestamps.

6. The system must prevent unauthorized access to data and restrict unauthorized use, such as limiting the ability to print reports.

7. Install software to protect data from viruses, malware, trojans, and worms, with automatic updates enabled.

8. Implement controls to prevent the use of portable devices such as external hard disks and USB flash drives.

9. Ensure electrical wiring within the organization is in good condition and safe to prevent fire hazards.

10. Conduct emergency drills and preparedness exercises for situations requiring server relocation.

11. Provide fire protection equipment and ensure regular inspections for effective operation to prevent or mitigate physical damage.

12. Maintain server storage rooms in accordance with information technology standards, including housing servers in rack cabinets, installing air conditioning, and securing the server room to prevent unauthorized access.

13. Define username and password access controls for server usage and database access.

25. Information System Access Control

Procedures

1. Access Control for Information Systems (Access Control)

1.1 Define user groups and assign access rights for each group.

1.2 Establish criteria for granting access to information systems, including authorization and access rights assignment:

(1) Define access rights for each user group, such as:

- Read-only
- Create data
- Input data
- Modify data
- Approve
- No access

(2) Define criteria for suspending or delegating access rights in accordance with user access management.

(3) Users requesting access to the information system must submit a written request and obtain approval from their supervisor and the designated system administrator.

1.3 Establish business requirements for access control, consisting of:

(1) Defining guidelines for controlling access to information systems and related access rights.

(2) Updating access control measures to align with business requirements and information security requirements.

2. User Access Management

Establish procedures for user registration covering the following:

- Prepare a system access request form for users to complete, for verification and processing of user registration
- Specify user's name and surname
- Specify user's network account
- Specify user's position and department
- Require approval signature from the user's supervisor
- Verify and assign appropriate access rights according to job responsibilities
- Prepare documentation outlining user rights and responsibilities, requiring user acknowledgment
- Record and retain system access approval documentation
- Establish criteria for granting access and removing users from the system upon resignation, transfer, reassignment, or termination
- Conduct periodic access rights reviews and update user accounts at least once per year

3. Access Control Based on Data Classification Levels

3.1 System administrators must define procedures for data storage and access control, including both direct access and access via information systems, as well as data destruction methods for each data type.

3.2 Data owners must review the appropriateness of user access rights at least once per year to ensure continued relevance.

3.3 System administrators must assign usernames and passwords to verify user identity for both direct and system-based access.

3.4 Transmission of sensitive data over public networks should be encrypted using recognized standards such as SSL, VPN, or email encryption.

3.5 3.5 Security measures should be in place to protect data during computer maintenance or when computers are moved outside the office, such as when sending them for repair. Data stored on storage media should be backed up and deleted beforehand.

Effective form 15 March 2025 onward.