UAC Global Public Company Limited
บริษัท ยูเอซี โกลบอล จำกัด (มหาชน)
www.uac.co.th | 02-936-1701-6

INFORMATION TECHNOLOGY SECURITY POLICY AND GUIDELINES

Purpose

To ensure that the Company has policies and guidelines for managing information technology security appropriately and effectively, maintains the security of information technology systems, and is able to operate continuously. Furthermore, to provide all parties involved with the Company, including management, employees, and external parties, with clear guidelines and operational frameworks, leading to efficient coordination, maximum service security, and higher standards.

Network Usage Regulations

1. The use of the network system shall be conducted only through Company-owned computers.
2. The use of the network system through computers that are not Company-owned computers must be approved by the system administrator in advance. If unauthorized use is detected, the system administrator may immediately disconnect such usage from the network system.
3. Employees are prohibited from accessing prohibited websites, including websites that are contrary to the Company's core principles and/or business interests, websites containing pornographic or obscene content, copyright infringement websites, hacker-related websites, and all types of gambling websites.
4. Employees are prohibited from using the Company's Internet service for personal gain or business activities.
5. Employees are prohibited from posting or sharing false information that may affect the Company's image and reputation.
6. Employees are prohibited from using computer resources and networks to engage in unlawful activities or activities contrary to public morals, such as creating websites for commercial purposes or disseminating illegal content or content contrary to public morals.
7. Employees are prohibited from intercepting data transmitted within the Company's computer network or that of others during transmission through computer networks.
8. Employees are prohibited from accessing computer systems and data protected against access by others for the purpose of modifying, deleting, adding, or copying information.
9. Employees shall not access computer networks or computer systems using another person's user account, whether authorized or unauthorized by the account owner.
10. Employees are prohibited from publishing information belonging to other persons or departments without authorization from the owner of such information.

Information Technology Security Governance Guidelines

Purpose

To ensure that information security management is effective and efficient and that there is a mechanism for controlling and overseeing information technology security, leading to consistent practices throughout the organization, the Company has designated responsible authorities to oversee information technology security.

The roles and responsibilities are as follows:

1. Establish objectives and develop information security policies, standards, procedures, and guidelines to ensure confidentiality, integrity, and stability of information systems.
2. Oversee compliance with information technology security policies.
3. Manage and assess risks that may affect the Company's business operations.
4. Control and manage the Incident Response Team to ensure readiness to respond to information technology emergencies within the organization, such as computer virus outbreaks.
5. Maintain preparedness and continuously learn new techniques in Information Security.
6. Provide information security consultation to other departments that utilize information technology in their operations.

Information Technology Risk Assessment and Risk Response

Purpose

1. To prepare for and respond to emergency situations that may occur to information databases and information systems.
2. To provide guidelines for maintaining the security, stability, and readiness of information databases and information systems.
3. To ensure that operations are systematic and continuous and that situations can be resolved promptly in the event of uncertainty and disasters.

Risk Factors

Factors that may cause damage to information databases and information systems may arise from both internal and external sources, including:

1. Internet network system failure.
2. Electrical system failure/power outage.
3. Virus attacks causing damage to databases and application programs.
4. Unauthorized intrusion or hacking of databases by external persons (Hackers).
5. Unauthorized access to information systems.

Risk Management

Information Technology Risk Management is a process used to identify, analyze, assess, and prioritize risks that may affect the achievement of objectives of the department or organization, including risk management and the establishment of operational guidelines or control measures to prevent, reduce, or mitigate risks. The risk management process and procedures are aligned with COSO ERM 2017.

Information Security Management Guidelines

Purpose

Information is an important business asset that must be properly protected and secured.

The Company has established information security measures by implementing key security technologies within the organization to support operations and reduce security risks at an appropriate level while maximizing operational efficiency. The Company recognizes the importance of information and manages information systems in accordance with the CIA principles as follows:

1. Confidentiality – Only authorized persons shall have access to and view information. Confidential information must not be disclosed to unauthorized persons.
2. Integrity – Information accuracy, completeness, and correctness shall be protected. Controls shall be in place to prevent unauthorized persons from changing, modifying, or altering information.
3. Availability – Only authorized persons shall have access to information whenever required. Controls shall be in place to prevent system failures, ensure continuous operation, and prevent unauthorized persons from causing system disruptions.

Disciplinary Measures for Violations of Information Technology Security Regulations

The Company has established the Information Technology Security Manual as a guideline for information technology security practices to prevent any individual from violating the regulations established for the security of the Company's information technology systems. If any employee or user violates these regulations, resulting in risks to the security measures of the Company's systems and networks, such actions may lead to suspicion and legal proceedings under applicable laws. The Company shall consider disciplinary actions in accordance with Company regulations and shall cooperate with police officers responsible for investigating suspicious activities.