(Translation)

Information Technology Policy

Bangkok Aviation Fuel Services Public Company Limited

and its subsidiaries

Edition	3.0
Effective Date	22 February 2024
Approved by	Resolution of the Board of Directors' Meeting No.1/2024 dated 22 February 2024
	..... (Mr.Palakorn Suwanrath) Chairman

Table of Contents

1. Principles and Rationale

Bangkok Aviation Fuel Services Public Company Limited and its subsidiaries recognize the importance of utilizing information technology in business management. Therefore, this policy is established to provide a framework for good corporate IT governance and management, referencing principles from relevant guidelines and practices, including those from the Securities and Exchange Commission and other applicable laws, tailored to the company's business context.

1) Information Technology Resource Allocation and Management Policy
2) Information Technology Risk Management Policy
3) Information Technology Security Policy

2. Objective

To ensure that the company and its subsidiaries have a framework for governance and management of enterprise information technology that aligns with the business needs, as well as to oversee the implementation of information technology to support and enhance business operations and risk management. This is also to enable the organization to achieve its objectives and core goals, utilizing resources and managing risks appropriately in accordance with good corporate governance practices.

3. Scope of Application

This policy shall apply to Bangkok Aviation Fuel Services Public Company Limited and its subsidiaries. The policies, guidelines, regulations, and orders that were in effect prior to this policy shall remain in force as long as they do not conflict with or contradict this policy.

4. Definitions

Term	Definition
Company	Bangkok Aviation Fuel Services Public Company Limited
subsidiary	A company or legal entity in which Bangkok Aviation Fuel Services Public Company Limited holds more than 50% of the shares
Board of Directors	Board of Directors of Bangkok Aviation Fuel Services Public Company Limited

Term	Definition
Management	Chief Executive Officer, Deputy Chief Executive Officer, and Directors of various departments of the company and its subsidiaries
Policy	Information Technology Policy
Information Technology Department	Units within the organizational structure of the company and its subsidiaries responsible for information technology functions
User	Permanent employees, contract employees, external users, partners, or customers of the company and its subsidiaries
External Service Provider	Individuals or legal entities from outside the organization that the company and its subsidiaries hire to provide services related to information systems
External User	Individuals or legal entities from outside the organization that need to use the information technology system
Information Technology System	Computer systems provided by the Information Technology Department
Computer Network System	Systems that can be used for communication or the transmission of data and information between information technology systems
Computer System	Devices or sets of computer equipment that connect operations together by defining commands, sets of instructions, or other guidelines to enable the devices or sets of devices to automatically process data
Information System	A system used for storing and processing data that operates in coordination between hardware, software, data, users, and processing procedures to generate information that can be utilized for planning, management, and support services
Information	Facts derived from data that have been processed and organized into a system that may be in the form of numbers, text, or graphics, making it easy for users to understand and usable for management, planning, decision-making, and other purposes
Staff	Officials or personnel under the Information Technology agency and external service providers
Information Technology Resources	Information assets, IT personnel, IT knowledge and capabilities, and budget

Term	Definition
Information Assets	1) Information Assets of System Type: This includes computer network systems, computer systems, computer applications, and information technology systems 2) Information Assets of Equipment Type: This includes computer hardware, computer devices, data recording devices, network equipment, and other related equipment 3) Information Assets of Data Type: This includes information data, electronic data, and computer data 4) Information Assets of Copyright Type: These are assets developed or rights to use from the product owner

5. Roles and Responsibilities

5.1 Board of Directors

5.1.1 Establish the information technology policies of the company and its subsidiaries

5.1.2 Oversee the management to ensure compliance with the policies, aligning with the company's needs, supporting and developing business operations, and risk management to achieve the main objectives and goals of the company and its subsidiaries

5.1.3 Review or update the policies at least once a year or whenever any events occur that may significantly impact the governance and management of information technology

5.2 Management

5.2.1 Establish guidelines, criteria, and procedures related to the policies

5.2.2 Monitor, control, and oversee relevant departments to ensure compliance with the established policies

5.3 Information Technology Department

5.3.1 Monitor and ensure that users comply with the relevant policies, guidelines, and procedures correctly and appropriately. Report any non-compliance to the management

5.3.2 Communicate the policies to users in an easily accessible manner to ensure that they understand and can correctly follow the policies

6. Policy on the Allocation and Management of Information Technology Resources

The company mandates that the allocation and management of information technology resources must align with the organizational strategic plan. This ensures that IT resources, particularly human resources, are sufficient and that risks associated with resource shortages are managed. Additionally, it ensures that IT operations achieve the objectives, strategies, and operational plans set forth. The implementation includes the following practices

6.1 Establish criteria and factors for prioritizing information technology plans, such as alignment with the company's strategic plan, impact on business operations, urgency of use, etc

6.2 Procure information technology resources and develop information resources to be sufficient and appropriate, aligning with the company's strategic plan

6.3 Prepare and approve the information technology budget in alignment with the organizational budget plan and strategic plan

6.4 Ensure that there are sufficient human resources for information technology tasks and develop the skills of personnel to have adequate knowledge and skills for their duties

6.5 Manage risks in cases where resources cannot be sufficiently allocated for information technology operations, whether it be personnel, budget, or demands exceeding the specified limits

6.6 Define the roles and responsibilities of the personnel in the Information Technology Department for the allocation and management of the company's information technology resources

6.7 Review the responsibilities related to information assets to ensure they align with the duties of personnel when there are changes in roles and responsibilities

6.8 Establish appropriate usage guidelines for information assets

6.9 Information technology resources used must be reliable and secure, complying with international standards

6.10 Information assets of system or equipment type must have an asset register created and maintained, and this register should be reviewed at least once a year or whenever there are significant changes to the information assets

7. Policy on Information Technology Risk Management

The company mandates that the management and handling of information technology risks must align with the organizational risk management policy and business continuity management, with the following practices

7.1 Define acceptable risks

7.2 Identify risks related to information technology

7.3 Assess risks, including the likelihood or frequency of occurrence and the significance or impact

7.4 Establish risk level indicators for significant risks identified in 7.2, including monitoring and reporting these indicators to manage and handle risks appropriately within acceptable levels

7.5 Define the roles and responsibilities of those accountable and those performing duties in managing and handling information technology risks

8. Policy on Information Technology Security

The company establishes an information technology security policy, considering the nature, size, and complexity of the business operations, as well as relevant regulations. This policy aims to ensure that users and related parties are aware of the importance of information system security, understand their responsibilities, and follow the guidelines for risk control. The company's implementation guidelines are as follows

8.1 Employee Practices

Employees must understand, acknowledge, and strictly adhere to the policies, regulations, measures, rules, and laws related to the use of the organization's information technology systems and computer networks when using computers, the internet, social networks, and email.

8.2 System Administrator Practices

System Administrator Practices The management of the company's and its subsidiaries' information systems must establish information technology security standards for controlling access to and use of the company's and its subsidiaries' information systems. These standards should be appropriate for the type of data, its priority, or confidentiality level, as well as the access level and access channels. Additionally, there should be measures to prevent intrusions through the network from intruders and unwanted programs that could damage the company's and its subsidiaries' information data. There should also be processes for reporting and responding to incidents that impact the company's information system operations.

8.2.1 Information Management and Confidentiality

8.2.1.1 Backup data to prevent data loss.

8.2.1.2 Control data encryption to ensure the encryption system is appropriate, effective, and can prevent unauthorized access or modification of confidential or important data.

8.2.1.3 Control access levels to information technology systems according to roles and responsibilities.

8.2.2 Personnel and User Supervision

8.2.2.1 Establish employee guidelines for using the computer network.

8.2.3 External Service Provider Supervision

8.2.3.1 Control the security of information technology systems from external service providers to protect the company's information assets from inappropriate access by external providers.

8.2.3.2 Control the delivery of services by external providers to comply with the agreements made with the business operators.

8.3 Cybersecurity Practices

A policy and guidelines for information technology security must be established to ensure that the company's and its subsidiaries' information technology systems are appropriate, effective, secure, and capable of continuous operation. This includes preventing issues that may arise from improper use of information technology systems and threats. Therefore, the company and its subsidiaries deem it necessary to establish an information security policy, which includes standards, guidelines, and procedures to cover the security of information technology systems and prevent various threats.

8.3.1 Protection Against Information System Threats

Establish measures to prevent malicious software to ensure that the information system is protected from such threats.

8.3.2 Information System Development and Maintenance

Ensure security in the information system development process to guarantee that the development or modification of information systems is accurate, complete, and meets user requirements. This also includes maintaining the security of the information system throughout its development lifecycle.

8.3.3 Management of Incidents Affecting Information System Security

The company establishes procedures and processes for Information Security Incident Management to handle incidents that may impact the security of information systems. This includes assigning responsible personnel with the necessary knowledge, skills, and experience, and ensuring rapid and timely reporting of incidents through designated individuals or departments. This ensures that incidents and vulnerabilities related to information system security are addressed correctly and efficiently within an appropriate timeframe.

9. Internal Control for Policy Compliance

The company ensures internal control measures are in place to comply with IT policies and conducts audits to ensure compliance with laws, regulations, and appropriate practices.