 Synergetic Well-being Community Builder	Information Technology Policy	
	Document Code : PD-IR-035	Revision No. : REV00
	Effective Date : 07 November 2025	Page :1/10

Information Technology Policy



	Information Technology Policy	
	Document Code : PD-IR-035	Revision No. : REV00
	Effective Date : 07 November 2025	Page :2/10

Table of Contents

Topics	Page
Introduction	3
Principles and Rationale	3
Objectives	3
Scope of Application	4
Definitions	4
Scope of the Information Technology Policy	5-9
Policy Monitoring and Review	9
Revision History	10

	Information Technology Policy	
	Document Code : PD-IR-035	Revision No. : REV00
	Effective Date : 07 November 2025	Page :3/10

Introduction

JAS Asset Public Company Limited, together with its joint ventures and subsidiaries, recognizes the importance of information technology in business operations and effective data management. These are essential for supporting continuous, secure, and well-governed operations.

Accordingly, the Company has established this Information Technology Policy as a framework for guiding the management and operation of the organization's IT systems to ensure that they are appropriate, transparent, and secure in alignment with good corporate governance principles.

Principles and Rationale

The Company recognizes information technology as a key enabler in business operations, service delivery, and communication with all stakeholders — enhancing efficiency, accuracy, and timeliness in operations. At the same time, the Company acknowledges the importance of mitigating risks from cyber threats and data breaches that may affect the Company or its stakeholders.


Accordingly, the Company has established this Information Technology Policy as a framework for managing, operating, and governing IT systems in compliance with international standards and applicable laws, to ensure effective, secure, and reliable use of information technology across the organization.

Objectives

1. To establish guidelines for managing the Company's information technology systems effectively, securely, and in compliance with applicable laws and regulations.
2. To promote understanding and awareness among employees regarding the proper and responsible use of information technology.
3. To prevent potential risks arising from the use of information technology, including unauthorized access, data leakage, and cyber threats.

Scope of Application

This Policy applies to all directors, executives, and employees at every level of JAS Asset Public Company Limited, as well as to business partners engaged in business activities with the Company.

	Information Technology Policy	
	Document Code : PD-IR-035	Revision No. : REV00
	Effective Date : 07 November 2025	Page :4/10

Definitions

Information Technology (IT)

Refers to systems, tools, equipment, or software used for storing, processing, transmitting, or exchanging information within the Company.

Personal Data

Refers to any information that can directly or indirectly identify an individual, in accordance with the Personal Data Protection Act.

Malware

Refers to malicious programs or software designed to damage, disrupt, or interfere with computer systems, such as viruses.

Backup System


Refers to a system or process for storing copies of data in a secure location for the purpose of data recovery in case of emergencies.

Data Recovery

Refers to the process of restoring lost or damaged data to its normal, usable state.

Cyber Threat

Refers to any event or action that intentionally or potentially causes damage, loss, or unauthorized access to the Company's IT systems, data, or devices.

 Synergetic Well-being Community Builder	Information Technology Policy	
	Document Code : PD-IR-035	Revision No. : REV00
	Effective Date : 07 November 2025	Page :5/10

Scope of the Information Technology Policy

1. Information Technology Management

The Company shall establish and maintain an efficient and standardized information technology management system to ensure smooth and secure business operations while minimizing potential risks associated with the use of technology.

Good Practices


1. The Information Technology Department should regularly develop and maintain IT risk management and business continuity plans to ensure preparedness and effective response to potential disruptions.
2. Conduct regular system inspections and maintenance to prevent issues that may affect business continuity or cause operational disruptions.
3. Provide training or awareness programs for employees on the safe and responsible use of technology, particularly for departments that rely heavily on IT systems in their daily operations.

2. Use and Maintenance of IT Equipment and Systems

All employees shall use the Company's information technology resources solely for business purposes and must properly maintain all equipment to ensure operational readiness at all times. Employees must refrain from any actions that could damage or disrupt the Company's systems, data, or technological equipment.

Good Practices

1. Use Company-owned equipment with care and only for legitimate business purposes.
2. Avoid installing any unauthorized software or applications on Company devices.
3. Regularly inspect hardware and software to ensure proper functionality. In case of any issues, promptly notify the Information Technology Department for inspection and resolution.

	Information Technology Policy	
	Document Code : PD-IR-035	Revision No. : REV00
	Effective Date : 07 November 2025	Page :6/10

3. Data Security

The Company shall collect, use, and manage data accurately, securely, and in compliance with all applicable laws — particularly the Personal Data Protection Act (PDPA) — to prevent loss, unauthorized access, misuse, or disclosure of information.

Good Practices


1. Departments responsible for storing or accessing sensitive information shall organize and manage data systematically, with appropriate security measures in place.
2. Access to personal data shall be restricted only to authorized personnel and must be supervised by their direct supervisors or designated responsible persons.
3. The Information Technology Department should regularly communicate and provide ongoing training to employees on personal data protection through easily accessible channels and self-learning resources.

4. Information System Access Control

The Company shall assign access rights to information and information systems based on each individual's roles and responsibilities, ensuring that data access is appropriate, secure, and subject to continuous monitoring.

Good Practices

1. For departments that require access to sensitive information, supervisors shall assign access rights in accordance with job responsibilities and operational necessity.
2. Employees and executives must set strong passwords for accessing the Company's systems and devices, and change them regularly.
3. The Human Resources Department shall promptly notify the Information Technology Department to revoke system access rights when employees resign or change positions.
4. The Information Technology Department shall maintain a system for logging and monitoring access to information systems, to facilitate follow-up, auditing, or technical investigation when necessary.

 Synergetic Well-being Community Builder	Information Technology Policy	
	Document Code : PD-IR-035	Revision No. : REV00
	Effective Date : 07 November 2025	Page :7/10

5. Data Backup and Recovery

The Company shall regularly back up critical data and establish a data recovery plan to ensure business continuity and minimize potential damage arising from data loss.

Good Practices


1. The Information Technology Department shall regularly back up critical data using secure systems, and store backup data separately from the main system to prevent loss or damage due to system failure or cyber threats.
2. Develop and periodically test a Data Recovery Plan (DRP) to ensure effective execution in the event of an emergency.
3. Continuously verify the integrity of backup data and update procedures to align with evolving technologies and best practices.

6. Cybersecurity and Threat Management

The Information Technology Department shall monitor, prevent, and respond to potential cyber threats to maintain the security of the Company's information systems and data. The Company shall also promote employee awareness of cybersecurity risks and encourage proactive vigilance to prevent potential incidents.

Good Practices

1. The Information Technology Department shall regularly install and update antivirus, anti-malware, and network security systems.
2. Employees shall avoid opening attachments or clicking links from unknown sources or suspicious emails that may contain malware.
3. The Information Technology Department should implement a continuous monitoring system to detect and respond promptly to any irregularities or security incidents.
4. Conduct periodic cybersecurity simulations and incident response drills to assess readiness and enhance preventive measures.
5. Continuously promote cybersecurity awareness and best practices among executives and employees through regular training and communication.

	Information Technology Policy	
	Document Code : PD-IR-035	Revision No. : REV00
	Effective Date : 07 November 2025	Page :8/10

7. Use of Internet and Email Systems in the Organization

Employees shall use the Company's internet, email, and online communication systems solely for work-related purposes. Personal use or any activity that may cause damage to the system, compromise security, or harm the Company's reputation is strictly prohibited.

Good Practices


1. Employees shall use the Company's internet and email systems exclusively for business-related activities.
2. The Company's internet and email systems must not be used to access inappropriate websites, content, or media, or for any activity that violates laws or regulations.
3. Executives and employees shall verify the accuracy of recipients' email addresses before sending information, especially documents containing internal or confidential data.
4. Executives and employees should refrain from forwarding information, news, or content that has not been verified by credible sources.
5. Executives and employees shall not use their Company email accounts to subscribe to websites or personal online services unrelated to their work.
6. If any unusual or potentially unsafe use of the Company's internet or email system is detected, the Information Technology Department must be notified immediately for investigation and appropriate action.

8. Reporting of Information Technology Incidents

In the event that executives or employees detect any irregularities, damages, or threats related to the Company's information technology systems, they must immediately report the incident to their supervisors or the Information Technology Department. This ensures that appropriate investigation, corrective action, and preventive measures can be implemented to avoid recurrence in the future.

Good Practices

1. All employees at every level shall promptly report any IT-related incidents they encounter — including unauthorized access to data, system outages, data loss, or suspicious emails — to the Information Technology Department.

	Information Technology Policy	
	Document Code : PD-IR-035	Revision No. : REV00
	Effective Date : 07 November 2025	Page :9/10

2. Reports should include relevant details such as the date, time, nature of the incident, and any supporting information to assist in identifying the cause and determining appropriate corrective measures.
3. The Information Technology Department shall investigate, analyze, and prepare a report on the incident, including recommendations to prevent recurrence.
4. All employees shall cooperate fully with the Information Technology Department during investigations to ensure timely and effective resolution.
5. If an incident is likely to cause severe impact or involves personal data, the Information Technology Department must coordinate with management and relevant departments to report and proceed according to the Company's established procedures.

Policy Monitoring and Review

The Company assigns relevant departments to monitor the implementation of this Information Technology Policy to ensure that it remains appropriate, comprehensive, and aligned with technological advancements or changes in the Company's operational structure.

The Company shall review this Policy at least once a year, or whenever there are significant changes in technology, organizational structure, or legal requirements, in order to ensure that it remains current, relevant, and consistent with the Company's operational needs and circumstances.

This policy shall take effect from 07 November 2025 onwards.



Approved by
Mr.Sukont Kanjana-hattakit
Chairman of the Board

