INFORMATION TECHNOLOGY SECURITY AND ARTIFICIAL INTELLIGENCE GOVERNANCE POLICY

MR. D.I.Y. HOLDING (THAILAND) PUBLIC COMPANY LIMITED AND ITS SUBSIDIARIES

7 August 2026

Version: 1
Approved by the Board of Directors' Meeting: 7 August 2026

MR. D.I.Y. Holding (Thailand) Public Company Limited
บริษัท มิสเตอร์. ดี.ไอ.วาย. โฮลดิ้ง (ประเทศไทย) จำกัด (มหาชน)
No. 777 WHA Tower, 12th floor, Moo 13 Debaratana Road (Bang Na-Trat) KM.7 Bang Kaeo, Bang Phli, Samut Prakan 10540 Registration No. 0107566000721
เลขที่ 777 อาคารดับบลิวเอชเอ ทาวเวอร์ ชั้น 12 ม.13 ถ.เทพรัตน (บางนา-ตราด) กม.7 ตำบลบางแก้ว อำเภอบางพลี จังหวัดสมุทรปราการ 10540 เลขทะเบียนนิติบุคคล 0107566000721

INFORMATION TECHNOLOGY SECURITY AND ARTIFICIAL INTELLIGENCE GOVERNANCE POLICY

MR. D.I.Y. Holding (Thailand) Public Company Limited (the "**Company**"), together with its subsidiaries (the "**Group**"), has adopted information technology systems in its operations to support business activities, enhance operational efficiency, and facilitate relevant stakeholders.

To ensure that the use of information technology systems is appropriate and secure, and to prevent risks or cyber threats that may affect the Group's operations and information, the Group has established this Information Technology Security and Artificial Intelligence Governance Policy as a framework for oversight and implementation for employees, suppliers and business partners, service providers, consultants, contractors, data processors, and external parties who interact with the Group's systems or data.

OBJECTIVES

This Policy is intended to:

- protect the Company's information assets and support business continuity;
- establish a clear framework and security expectations for relevant external individuals and organizations;
- promote appropriate compliance with laws, rules, and regulations related to data protection;
- maintain the confidentiality, integrity, and availability of the Company's data and information systems;
- reduce and prevent security risks arising from unauthorized access to, use of, or disclosure of information;
- promote the integration of information security management and data protection into the Group's risk management and compliance governance systems; and
- promote the safe and accountable use of artificial intelligence (AI), and prevent misuse or inappropriate use.

Scope of Application

This Policy applies to all individuals and organizations that meet any of the following conditions:

- those who access the Group's information technology systems or networks;
- those who manage, process, or otherwise handle important information of the Group;
- suppliers or business partners, service providers, consultants, contractors, data processors, or external parties who provide information technology, data processing, or other related services to the Group;
- those who perform work under the Company's projects or contracts relating to the Group's information technology systems; and
- all suppliers and business partners, service providers, consultants, contractors, data processors, and external parties, as a condition of access to the Group's systems and information.

This Policy covers the entire operations of the Group, including employees, suppliers and business partners, service providers, data processors, consultants, contractors, and external parties involved in accessing, using, or processing the Group's information

GUIDELINES

1. ROLES, DUTIES, AND RESPONSIBILITIES

1.1 Board of Directors

The Board of Directors oversees the overall information security posture of the Company, acknowledges material risk issues and significant matters that may affect business operations, and provides policy-level guidance as appropriate

1.2 AUDIT AND RISK MANAGEMENT COMMITTEE

The Audit and Risk Management Committee oversees, reviews, and assesses cybersecurity risks, including potential impacts, and ensures that progress is reported regularly to the Board of Directors**.**

1.3 CHIEF EXECUTIVE OFFICER

The Chief Executive Officer oversees and supports the implementation of information security at the enterprise level by setting direction and promoting awareness of the importance of information security in alignment with the Company's strategy and business operations, supporting the allocation of appropriate resources, and monitoring material risk issues that may affect the Company's operations.

1.4 INFORMATION TECHNOLOGY DEPARTMENT

The Information Technology Department shall have the following roles and responsibilities:

(1) to define and ensure the implementation of information security measures appropriate to the nature of the organization's operations and level of risk;

(2) to manage and maintain the Company's information technology assets in order to support business operations and information security controls;

(3) to monitor, assess, and continuously improve information security operations in order to ensure effectiveness and alignment with changes in risks and technology;

(4) to coordinate with relevant functions, employees, and suppliers and business partners, service providers, consultants, data processors, contractors, and external parties in order to promote the appropriate and secure use of information technology systems and compliance with relevant requirements;

(5) to promote and support information security awareness among employees and relevant parties;

(6) to report material information security issues or risks to management, as appropriate;

(7) to support compliance with laws, rules, and regulations relating to information technology and information security

1.5 EMPLOYEES

Employees are responsible for using information technology systems and related resources appropriately and securely, and must comply with the Group's information security policies and requirements. All employees are responsible for complying with information security requirements according to their roles and responsibilities, including helping to prevent, detect, and report information security incidents or risks that may arise.

1.6 EXTERNAL PARTIES

External parties, suppliers, business partners, service providers, consultants, contractors, data processors, and other relevant parties must strictly comply with the Group's information security requirements and relevant contractual conditions. In particular, parties who have access to or are involved with the Group's information technology systems or information may use the Group's information and systems only for authorized business purposes and must cooperate in implementing the information security measures required by the Group.

2. INFORMATION TECHNOLOGY SECURITY MANAGEMENT GUIDELINES

2.1 ACCESS CONTROL OVER INFORMATION AND INFORMATION TECHNOLOGY RESOURCES

(1) User authentication shall be required before access is granted to the Company's information systems, data, and information technology resources.

(2) Access rights to data and systems shall be granted based on the user's role, responsibilities, and business need, in accordance with the principle of least privilege.

(3) Access to critical or sensitive data and systems shall be controlled and restricted in order to prevent unauthorized access or use.

(4) User accounts and access rights shall be managed throughout their lifecycle, including access approval, access modification, and revocation when access is no longer required.

(5) Access rights to data and information systems shall be reviewed periodically, or whenever there is a change in role, employment status, or related project.

(6) Appropriate logging and monitoring of information system usage shall be maintained so that user activities can be reviewed and traced to the responsible user in the event of an information security incident

2.2 PHYSICAL AND ENVIRONMENTAL SECURITY

(1) Access to areas relating to information systems, infrastructure, and critical equipment shall be restricted to authorized persons who have a business need based on their duties.

(2) Measures shall be implemented to prevent environmental risks that may affect information systems and equipment, such as fire, power outages, or other emergencies.

(3) Information technology equipment and infrastructure shall be protected from damage or unauthorized access.

2.3 SECURITY OF INFORMATION TECHNOLOGY OPERATIONS

(1) Information systems and information technology resources shall be used for business purposes and in accordance with the Company's policies, rules, and requirements.

(2) The use of information systems in a manner that may cause damage to the Company's systems, information, or operations shall be prevented.

(3) Information technology operations shall be governed under appropriate information security guidelines and measures.

(4) Information systems shall be maintained at an appropriate level of availability in order to support business continuity.

(5) Information security threats shall be monitored, detected, assessed, and responded to appropriately and in a timely manner.

2.4 INFORMATION SECURITY INCIDENT MANAGEMENT AND CONTINUITY

(1) Appropriate channels and processes shall be established for reporting information security incidents or suspicious events that may affect the security of information systems.

(2) Information security incidents shall be managed, remediated, and mitigated, including incident analysis and review, as appropriate.

(3) IT contingency and preparedness arrangements for systems and data shall be established in order to support the Company's business continuity.

(4) Incident management and contingency arrangements shall be reviewed and improved on a continuous basis, as appropriate.

2.5 INFORMATION TECHNOLOGY AWARENESS

(1) Personnel shall be encouraged to understand their roles, duties, and responsibilities in relation to information security. Persons who are involved in using or accessing information resources shall receive appropriate information or communication before access is granted.

(2) New employees shall receive orientation on the Company's information technology security policy in order to build an understanding of the use of information systems and data protection.

(3) Awareness of information technology risks shall be promoted among personnel who have access to information or internal systems in order to prevent risks arising from inappropriate use of systems or information.

2.6 INFORMATION TECHNOLOGY ASSET MANAGEMENT

(1) Information technology assets used in the Company's operations shall be identified and managed appropriately.

(2) Information technology assets shall be maintained in a usable condition in order to reduce risks that may affect systems and information.

(3) Information relating to information technology assets shall be reviewed and updated, as appropriate, to support information security management.

2.7 MANAGEMENT OF RELATIONSHIPS WITH SUPPLIERS AND EXTERNAL PARTIES

(1) Access to the Company's information systems or information by suppliers and external parties shall be limited to the authorized scope of work and purpose.

(2) Roles, duties, and information security responsibilities of suppliers and external parties shall be defined appropriately.

(3) Access to systems and information by suppliers and external parties shall be monitored and supervised as necessary in order to prevent risks that may affect the Company.

3. ARTIFICIAL INTELLIGENCE (AI) GOVERNANCE GUIDELINES

The Group recognizes the importance of using or developing artificial intelligence (AI) to support more efficient operations. To ensure that such use or development is appropriate, accurate, governed, and aligned with ethical principles, the Group has established the following guidelines:

(1) The Group shall use or apply AI appropriately, safely, transparently, and in compliance with applicable laws, relevant standards, and ethical principles.

(2) The Group shall protect personal data and privacy in the use or development of AI.

(3) The Group shall safeguard the security of AI systems and related data in order to prevent unauthorized access, use, or disclosure.

(4) The Group shall use AI with fairness, reduce the risk of bias or discrimination that may arise from AI outputs or system functioning, and require that significant uses of AI remain subject to appropriate human oversight, including the ability to review, intervene, or override when necessary.

(5) The Group shall clearly define the objectives, scope of use, and responsible persons for the use and governance of AI, and shall communicate the limitations of AI and explain its outputs to relevant parties, as appropriate.

(6) The Group shall not use AI in a manner that causes deception, exploitation, or inappropriate harm to individuals.

4. INFORMATION SECURITY AUDIT AND ASSESSMENT

(1) The Group shall conduct internal audits or periodic reviews of compliance with this information security policy in order to assess the adequacy and effectiveness of the relevant control measures.

(2) The Group shall assess or review compliance with information security requirements by suppliers, service providers, data processors, or external parties, as appropriate and based on the level of risk.

5. REVIEW OF POLICY

This Policy shall be reviewed at least once a year by the Information Technology Department. If there is any proposed modification required to be made to this Policy, it shall escalate to the Board for consideration.

This Policy shall be effective from 7 August 2026 by approval of the Board of Directors' Meeting No. 3/2026.

_____

(Mr. Ong Chu Jin Adrian)

Chairman of the Board of Directors

MR. D.I.Y. Holding (Thailand) Public Company Limited