Information Security Management System Policy

AddTech Hub Public Company Limited (the "**Company**") and its subsidiaries (the "**Group**") has arranged for the use of information technology systems to facilitate, increase efficiency, and provide efficiency for the entire system to work so that the use of services and the provision of services can be used together appropriately in accordance with business policy. The system is used in a correct manner consistent with the requirements of the Computer Crime Act and other related laws and prevent problems that may arise from using the information technology network system in an incorrect manner both from users and various threats which may affect the business systems of the Group causing damage. In order for the information technology systems of the Group to maintain confidentiality, accuracy, integrity, and availability of information, including users and related persons are aware of the importance of maintaining information system security and are aware of the duties, responsibilities and guidelines for controlling various risks, the Group has therefore established Information Security Management System Policy to be considered as a guideline for the same practice as follows:

- Management Directions for Information Security
  - Policy for Information Security
    - The Company is required to have a written Information Security Management System Policy in place, the content of which must be prior approved by the Chairman of the Board of Directors or by a C-suite executive entrusted by the Chairman.
    - The Company shall disseminate the Policy for acknowledgement and compliance of users and external organizations. Such dissemination must be conducted through a platform that is easily accessible.
  - Review of the Policies for Information Security
    - The Information Technology Department shall assess and review the Information Security Management System Policy as required by the provision outlined under Section "Policy Review".

1. Organization of Information Security

To formulate measures to monitor, supervise and track responsibilities that concern safeguarding of information system used by different departments within the Company. Moreover, it is aimed to be a guideline for the use of mobile devices to ensure its alignment with the Information Security Management System Policy.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

1.1 Internal Organization

1.1.1 Information Security Roles and Responsibilities

Divisional executives shall define responsibilities of personnel in safeguarding information security in writing, the outline of which must be aligned with the Information Security Management System Policy.

1.1.2 Segregation of Duties

Divisional executives shall ensure the segregation of duties to clearly disperse critical functions and responsibilities of information security to facilitate cross-checking between entities.

1.1.3 Contact with Authorities

The Information Technology Department shall prepare a contact list providing all essential contact information such as that of legal departments or related agencies, etc., for emergency purposes. In this regard, such contact list must be regularly updated.

1.1.4 Contact with special interest group

The Information Technology Department shall prepare a directory of information security specialists and provide more communication options to facilitate users' subscription and coordination with the specialists, or acquisition of prompt advice in the case where an unprecedented incident takes place and affects information security. In this regard, such directory must be regularly updated.

1.1.5 Information Security in Project Management

The divisional executives shall have a risk control measure in place while also monitoring and assessing the overall performance of projects, whether they are organized internally or conducted by external suppliers.

1.2 Mobile Computing and Teleworking

1.2.1 Mobile Computing and Communication

- The Information Technology Department shall have an adequate measure in place to ensure the security of mobile devices, considering risk exposure when a specific device is connected to internal server or used remotely.
- All users using mobile devices for the purpose of connecting them to the internal information system shall comply with the Information Security Management System Policy and be strictly aware of information security.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

1.2.2 Teleworking

- All users working remotely shall comply with the Information Security Management System Policy in the same strict manner as when they are working onsite.
- Any user who requires access to the Company's information system for the purpose of teleworking must provide a sufficient reason and be prior approved by his/ her department and the nominated owner of such asset.
- Any user who requires remote access shall obtain permission from the system administrator prior to the access.

2. Human Resources Security

To formulate measures to monitor, supervise and track recruitment process, human resources management of current and former employees, or those who have been rotated.

2.1 Prior to Employment

2.1.1 Screening

- The Company shall conduct pre-employment / pre-procurement screening and background check on all applicants and external parties that are to provide services within the Company.

2.1.2 Terms and Conditions of Employment

- The Human Resource Management Department shall advise personnel / supplier to sign an employment contract or work agreement, or a supplier contract, in which all responsibilities related to information security are outlined. The users shall acknowledge and agree with the regulations set forth by the Company by thoroughly reading and understanding the policies, rules and regulations contained therein.

2.2 During Employment

2.2.1 Management Responsibilities

- Divisional executives shall supervise and guide personnel or suppliers of the Company to comply with applicable Information Technology Policy and information security regulations enforced by the Company.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

2.2.2 Information Security Awareness, Education and Training

- The Information Technology Department shall define available channels from which personnel can acquire knowledge and understanding about the Information Security Management System Policy, as well as their own roles and responsibilities regarding information security prior to onboarding with the Company.
- The Information Technology Department shall regularly provide training about general operations. Such training must be led by the department responsible for each matter to ensure that employees can learn and clearly understand the topics such as workflow system, applications, basic troubleshooting techniques, legal and regulatory compliance, etc.
- The Information Technology Department shall regularly provide training about and strengthen awareness on information security to ensure that employees can learn and understand related topics and be able to perform their duties and responsibilities in a preferable and secure manner.

2.2.3 Disciplinary Process

- The Company shall apply a disciplinary punishment against users who violate or breach the applicable Information Technology Policy and information security regulations, or any work procedures that concern information security.

2.3 Termination or Change of Employment

2.3.1 Termination or Change of Employment Responsibilities

- The Human Resource Management Department shall formulate written regulations that require personnel and external organizations to be responsible for information security subsequent to their termination or change of employment.
- The Human Resource Management Department shall encourage strict compliance of personnel and external organizations with applicable regulations.

3. Asset Management

To ensure that the Company's assets and information system have been safeguarded at an adequate level in order to mitigate potential risks of unauthorized disclosure, as well as to prevent misuse and damages caused to information assets of the Company.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

3.1 Responsibility for Assets

3.1.1 Inventory of Assets

- The Information Technology Department shall supervise and advise its department to provide an asset account for appropriate asset management and control. In this regard, such account must be updated on a regular basis.

3.1.2 Ownership of Assets

- The information technology executives shall require an appropriate nomination of asset owner, who is to monitor and be responsible for the respective assets.

3.1.3 Acceptable Use of Assets

- The Information Technology Department shall provide a guideline for the use of assets to optimize computer management and ensure that every access is safeguarded from possible damages. Such guideline must be communicated to personnel of the Company for acknowledgement and further compliance.

3.1.4 Return of Assets

- The Human Resource Management Department or supervisors shall advise and ensure that the Company's personnel or suppliers serving onsite have returned all assets such as laptops, documents, keys, employee badges, which belong to the Company, to the specified department.

3.2 Information Classification

3.2.1 Classification of Information

- The Company shall conduct asset categorization and classification. The classification of information must incorporate applicable laws and regulations for suitability.
- Internal departments shall classify information assets utilized for Company's operations and conduct classification of such information.
- Internal departments shall monitor the classification of information assets according to the operation guideline outlined in the Information Security Practices.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

3.2.2 Labeling of Information

- The Company shall regulate and ensure that all filed data have been adequately safeguarded and maintained secure, starting from the processes of printing, labelling, storing, duplicating, distributing, to destroying. Such practices shall be set forth as a regulation to be complied by personnel and stakeholders to ensure that all information assets are well monitored and safeguarded.
- The Information Technology Department and nominated entities shall attach labels, based on asset accounts, and user instructions to every computer device.

3.2.3 Handling of Assets

- The Information Technology Department shall supervise and provide work procedures regarding handling of assets to prevent information leakage and misuse of such assets.

3.3 Media Handling

3.3.1 Management of Removable Media

- The Information Technology Department shall provide written work procedures regarding handling of medium that store removable information, which must also be updated on a regular basis. Such procedures shall be communicated to internal users for acknowledgement and further compliance.
- Handling of medium that contain removable information shall be in alignment with the classification of information.

3.3.2 Disposal of Media

- The Information Technology Department shall provide an instruction for disposal of media to prevent leakage of confidential or sensitive data.
- The Information Technology Department shall formulate control measures for disposal of media by referring to internationally recognized standards.

3.3.3 Physical Media Transfer

- The Information Technology Department shall determine work procedures or regulations to safeguard information in the case where there is a physical media transfer from a specific installation or operating area.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

4. Access Control

To formulate guidelines for information security in order to monitor access and use of information system, and to prevent unauthorized access and access gained by unpatched software, which may cause damage to information assets of the Company.

4.1 Business Requirement for Access Control

4.1.1 Access Control Policy

- The Company shall develop a written Access Control Policy. Such policy must be regularly updated and internally communicated for further compliance.

4.1.2 Access to Networks and Network Service

- The Information Technology Department requires that all users shall submit an access request, which must be prior approved only by their line manager.
- The Information Technology Department shall strictly limit access to authorized users. Such authorization must be based on duties, responsibilities and necessity.

4.2 User Access Management

4.2.1 User Registration and Deregistration

- The Information Technology Department and the nominated owners of assets shall collaboratively determine written procedures for user registration and deregistration with regular updates and internal communications for compliance.

4.2.2 User Access Provisioning

- The Information Technology Department and the nominated owners of assets shall assign or authorize each user for the use of data or information system based on their responsibilities.
- The Information Technology Department and the nominated owners of assets shall provide a document of authorization for the use of data or information system. Such document shall be filed as proof of operations.
- The Information Technology Department and the nominated owners of assets shall set out a procedure for user access provisioning in the case where a user needs access that goes beyond their authorization.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

4.2.3 Review of User Access Rights

- The Information Technology Department and the nominated owners of assets shall provide written procedures for the review of users' authorized access to information, information technology system and applications with regular updates and internal communications for acknowledgement and compliance.
- The Information Technology Department and the nominated owners of assets shall set a clear cycle of the review over access rights to information and information technology system, which must be communicated to relevant parties for their acknowledgement.
- During the review of user access rights, the following matters shall be taken into consideration:

  - Defined review cycles;

  - Termination of employment;

  - Change of position and duties;

  - Request for additional access.
- After completing the review process, the nominated owner of assets or administrator shall keep review records. Such records shall be categorized based on cycles of review.

4.2.4 Removal of Access Rights

- The nominated owner of assets and administrator shall determine written criteria for deregistration of access rights, which must be internally communicated for acknowledgement and further compliance.

4.3 User Responsibilities

4.3.1 Use of Secret Authentication Information

- Users shall not use a password of which the structure or characteristics are too generic; for example, a vocabulary from a dictionary, user's name or a combination thereof, or a password of alphabetical order, or personal information, or a sentence / phrase which is easy to guess.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

- Users shall not write down, save, keep or display their passwords in proximity to the system or any device accessible by such password.
- Users shall be responsible for all actions taken if it is provable that such action was done under the username and password attributed to them, or by them using an account of other users who do not have authorized access.
- Users are required to comply with other password-related regulations set forth by the Company.

4.4 Application and Information Access Control

4.4.1 Information Access Restriction

- The nominated owners of assets and administrator shall restrict access to data, information system and functions. In this regard, the restrictions must conform to the Access Restriction Policy.
- The nominated owners of assets and administrator shall provide instructions for the use of information system, including computers, applications, e-mail messaging, wireless LAN and the internet. Access rights must be aligned with responsibilities and require prior approval by the line manager of such user.

4.4.2 Secure Log-on Procedures

- The Information Technology Department shall provide written instructions to ensure access to the information system by referring to international standards with regular updates and internal communications for acknowledgement and compliance of all personnel.

4.4.3 Password Management System

- The Information Technology Department shall provide a management system over usernames and passwords used to access the information system in order to ensure the same standard throughout.

4.4.4 Use of Privileged Utility Programs

- The Information Technology Department shall restrict the use of privileged utility programs and delimit the use of privileged utility programs on the information system

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

or key computer software in order to prevent breach or noncompliance with security measures set forth.

4.4.5 Access Control to Program Source Code

- The Information Technology Department shall determine access control to program source code and avoid unintended changes to program source code in order to minimize the potential for errors in the development of information system and workflow system of the Company.

5. Cryptographic

To formulate cryptographic procedures and ensure that the information system maintains the confidentiality of all information, self-authentication, and/ or to adequately and efficiently prevent unintended changes by unauthorized users with guidelines as follows:

5.1 Cryptographic Controls

5.1.1 Policy on the Use of Cryptographic Controls

- The Information Technology Department shall formulate the use of cryptography measures, which must suit potential risks to each classification of information defined.

5.1.2 Key Management

- The Information Technology Department shall provide key management procedures that extend to the key management life cycle, as well as to consistently monitor compliance with applicable policies and such procedures.

6. Physical and Environmental Security

To formulate prevention measures that are to be taken to monitor use and physical maintenance of information system and information devices, which are supporting infrastructures of the Company's information system, to ensure that it is readily available for use, and to prevent unauthorized access to and disclosure of information assets.

6.1 Secure Areas

6.1.1 Physical Security Perimeter

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

- The Company shall consider and secure physical security perimeter, which consists of enclosed boarding surrounding rooms, entry and exit points and adequate security system.

6.1.2 Physical Entry Controls

- The Company shall limit access to operation centers and locations in which critical cyber assets are housed, to which access is restricted to only authorized personnel.
- The list of personnel authorized to access operation centers and locations in which critical cyber assets are housed must be consistently examined, improved and updated.
- The Information Technology Department shall limit physical access to secure areas including computer rooms and system administrator areas to authorized personnel only. All access to computer rooms must be logged with details of such person, time of access, purposes of access, and such log must be regularly examined.

6.1.3 Securing Offices, Rooms, and Facilities

- The Information Technology Department shall configure and install a physical security system to safeguard operation centers and locations in which critical cyber assets are housed, computer rooms, system administrator areas, and information devices used for the operations, from damage and unauthorized access.

6.1.4 Protecting Against External and Environmental Threats

- The Information Technology Department shall monitor and supervise to ensure physical security protection has been configured and installed to prevent external threats, including both human-caused and natural disasters such as fire, flood, earthquake, explosion, civil disorder, epidemic etc.

6.1.5 Working in Secure Areas

- The Information Technology Department shall have guidelines for physical security for those who work in secure areas, including operational areas and data center rooms, and shall require rigorous compliance with such guidelines.

6.1.6 Delivery and Loading Areas

- The Information Technology Department shall ensure that unauthorized persons are not able to access restricted areas. Delivery/ loading areas and preparation or

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

assembling points of information devices to be used in computer rooms must be clearly designated, organized and marked to avoid unauthorized access.

6.2 Equipment

6.2.1 Equipment Setting and Protection

- The Information Technology Department shall locate information devices within a secure room or location. Safety cabinets that house routers and networking hardware must invariably be locked and shall be unlocked only by authorized technicians for maintenance or reconfiguration in order to reduce risks of unauthorized access.

6.2.2 Supporting Utilities

- The Information Technology Department shall ensure system failure prevention equipment and supporting utilities are installed within computer rooms including fire protection equipment, smoke detectors, error monitoring system, etc. In this regard, all equipment must be well maintained and readily available.

6.2.3 Cabling Security

- The Information Technology Department shall ensure that installation and maintenance of communication cables within operation centers and computer rooms are in line with the applicable industrial security standards in order to prevent unauthorized access, data interception, or physical damage.

6.2.4 Equipment Maintenance

- The Information Technology Department shall ensure there are maintenance services provided for all major processing information devices used at the operational level and supporting utilities in a timely manner and in accordance with the requirements of respective manufacturers in order to facilitate their consistent operations and availability.
- The Information Technology Department shall ensure maintenance activities are logged. Moreover, detected issues and deficiencies of devices must be recorded for further assessment and improvement to achieve invariable availability.

6.2.5 Removal of Assets

- The person responsible for monitoring areas and premises that require security safeguard shall not allow relocation of information assets to outside of the

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

organization, except for the case where such removal is permitted by an entrusted approver.

- Users shall not take information devices, assets or software out of the Company, except for the case where such removal is permitted by an entrusted approver.
- The Information Technology Department shall have written procedures for removal of assets in place and ensure they are regularly updated and communicated to internal users for acknowledgement and further compliance.

6.2.6 Security of Equipment and Assets Off-Premises

- It prescribes that executive of at least the department level shall have authority to allow use of information devices off-premises. Such devices used off-premises must be protected to prevent potential damage and possible risk exposures must be taken into consideration.
- The Information Technology Department shall formulate security measures to safeguard information assets utilized off-premises in order to minimize risks caused by the use of such devices or assets outside the Company.

6.2.7 Secure Disposal or Re-Use of Equipment

- Users shall recheck such devices in which there is a storage unit to reassure that critical cyber data or licensed software have already been adequately removed, transferred or destroyed based on the classification of data prior to the disposal or reuse of such devices.
- The Information Technology Department shall have procedures in place for the destruction of data or information assets, and measures or techniques for further disposal of data and reuse of information devices. In this regard, such procedures must correspond to the classification of data.
- The Information Technology Department shall assign a person to be responsible for disposal of information assets stored in storage media, which are no longer necessary for the operations of the Company.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

6.2.8 Unattended User Equipment

- The Information Technology Department shall formulate protection measures to safeguard computers and information devices which are left unattended in order to prevent unauthorized access.
- Administrator shall require users to not allow other persons to access their computer hardware or the information system and to fill in correct username and password prior to access to such computer.
- Users shall immediately log off from the information system, active computer system and computer hardware once they no longer use it or after completing an operation.
- Users shall lock their computer screen or that of critical devices when it is not in use or when they are not in the proximity to such hardware.

6.2.9 Clear Desk and Clear Screen Policy

- Administrators shall ensure that all users have locked their screens when the system is not currently used; for example, session time out and lock screen, etc.
- Users shall not leave critical information assets such as physical documents or storage media unattended in a non-secure, area, public space, or location in which such assets are easily found. Users shall house information assets in proper locations as well as having prevention measures in place to restrict unauthorized access.

7. Operations Security

To set out control measures to ensure there are explicit guidelines and secure procedures for information security operations and communications.

7.1 Operating Procedures and Responsibilities

7.1.1 Documented Operating Procedures

- The Information Technology Department shall provide information operations procedures in writing. Personnel responsibilities must be defined based on clear business structures to ensure they are able to discharge their duties correctly and in compliance with the Information Security Management System Policy enforced by the Company.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

- Sections in the Information Technology Department shall provide handbooks, system manuals and knowledge database to ensure that relevant parties deliberately understand all workflows, nature of work and process.
- Sections in the Information Technology Department shall invariably review such practices, handbooks, system manuals and knowledge database to ensure that they are readily available, accessible, and are communicated to all stakeholders for acknowledgement and further compliance.

7.1.2 Change Management

- The Information Technology Department shall monitor the implementation of structural change management, workflows and the information system in order to place transformation, correction, or any activity that affects the work system under control. In this regard, the provisions contained herein under “Part 1. Change Management Policy” shall be complied.

7.1.3 Capacity Management

- Administrator shall monitor performance of work systems and major information devices to ensure their continuity and efficiency.
- Administrator shall evaluate capacity and sufficiency of information assets such as use of servers and network devices such as CPUs, memory units, disks, bandwidth, etc.; and shall conduct resource planning to ensure the information system is adequately efficient and capable of accommodating future use.

7.1.4 Separation of Development, Testing, and Operational Environments

- The Information Technology Department shall monitor and direct separation of system development, testing and operational environments.
- The Information Technology Department shall ensure authorization of access to each specific environment and assigning custodianship is clearly performed. Operational results must be reported to the line manager. In the case where a problem is detected, such problem and its solutions must be logged and further reported to the line manager for his/her acknowledgement.

7.2 Protection from Malware

7.2.1 Controls Against Malware

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

- The Information Technology Department shall formulate measures to detect, prevent and restore system to safeguard assets from malware. Moreover, awareness of all stakeholders should be adequately reinforced.

7.3 Backup

7.3.1 Information Backup

- The Information Technology Department shall outline measures concerning information backup and consistent backup cycles for critical information to prevent loss of data.
- Nominated owners of assets shall make extra copies of data, or require consistent backup of information, and conduct backup data testing to ensure that data will readily be restored for further use.
- Users shall be responsible for backing up data to an external storage such as external hard disks on a regular basis. Such data must be stored in proper media which are not exposed to risks of data leakage.

7.4 Logging and Monitoring

7.4.1 Event Logging

- Administrator shall sufficiently log events concerning information security for further assessment.
- Administrator shall monitor the use of information system. Results of such monitoring shall be reviewed on a consistent basis to identify abnormal activities.
- Administrator shall monitor and direct logging of fault events that involve information use, including analysis, correction and provision of preventive approaches to prevent potential recurrence of such problems.

7.4.2 Protection of Log Information

- Administrator shall ensure protection of information, event and evidence logging system available on the information system against modification, destruction and unauthorized access.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

7.4.3 Administrator and Operator Logs

- Administrator shall require logging of activities by administrators and operators who are involved in system operations; for example, time of system activation and deactivation, modification of system settings, system errors and actions taken for correction. In this regard, such activity logs must be regularly reviewed.

7.4.4 Clock Synchronization

- Administrator shall ensure and direct clock synchronization for all information devices and system throughout the Company based on the legal and universal time.
- Administrator shall examine the clock of information devices and system of the Company, as well as updating it on a regular basis in order to prevent incorrect timestamps.

7.5 Control of Operational Software

7.5.1 Installation of Software on Operational Systems

- The Information Technology Department shall provide work procedures and measures to guide the installation of software on the operational systems in order to limit and prevent installation of unauthorized software carried out by users.
- The Information Technology Department shall define a list of standard software allowed to be installed on the Company's computer devices in writing with regular updates. Such list must be communicated to internal users for acknowledgement and compliance.

7.6 Technical Vulnerability Management

7.6.1 Management of Technical Vulnerabilities

- The Information Technology Department shall identify potential technical vulnerabilities of the Company's information system at least on a yearly basis.
- Administrator shall preserve and maintain the state of being secure of the information system on a regular basis, including identifying technical vulnerabilities, assessment of risk exposures derived from detected vulnerabilities and improvement of such vulnerabilities.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

7.6.2 Restrictions on Software Installation

- Users shall comply with the regulations on restrictions of software installation and shall not install any pirated software on the Company's computers.

7.7 Information System Audit Considerations

7.7.1 Information System Audit Controls

- The Information Technology Department shall provide information system audit plans that are aligned with the risks having been assessed through, for example, vulnerability assessment.
- The Information Technology Department shall inform relating entities in advance every time before they audit the information system.
- The Information Technology Department shall define the scope of technical audit tests to ensure that it covers critical vulnerabilities and shall control such audit tests to not affect normal operations. In the case where any technical audit test may affect system availability, such test must be conducted outside business hours.

8. Communications Security

To formulate control measures for network management and transmission of information via computer networks, either internally or externally, for the purpose of cybersecurity.

8.1 Network Security Management

8.1.1 Network Controls

- Administrator shall control and monitor network security management to prevent threats and safeguard information system and applications operating on the computer network, including information exchanged thereon.

8.1.2 Security of Network Services

- Administrator shall ensure that security characteristics, service levels and network management needs are defined in network service agreements or contracts, both for services provided internally or by external suppliers

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

8.1.3 Segregation in Network

- The Information Technology Department shall ensure segregation in network as deemed appropriate by taking the access demands of users, impacts against information security, and priority of data available on such network into consideration.

8.2 Information Transfer

8.2.1 Information Transfer Policy and Procedures

- The Information Technology Department shall monitor and ensure to have information transfer procedures in place, which are suitable for specific types of communications, types of information and classification of data.

8.2.2 Agreements on Information Transfer

- The Information Technology Department shall monitor and ensure to settle written agreements on information transfer, whether internally or between the Company and external entities, according to the Information System and Technology Operation Manual.
- In transferring information between the Company, such transfer must be prior approved by the nominated owner of the asset every time and conducted under a written agreement. Moreover, the transfer shall be subjected to specific terms and conditions and be protected based on data classification.

8.2.3 Electronic Messaging

- The Information Technology Department shall have a measure in place to monitor electronic messaging such as e-mail, EDI (Electronic Data Interchange), instant messaging, etc. Critical email messages need to be adequately protected from accessing, editing, interrupting attempts by unauthorized users.

8.2.4 Confidentiality or Non-Disclosure Agreements

- Department executives must procure their personnel and external suppliers working for the Company to sign a written confidentiality or non-disclosure agreement.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

9. System Acquisition, Development, and Maintenance

To reduce errors in requirements specification, design, development, and testing of newly developed or enhanced information systems, including controlling the developed or acquired systems to comply with the specified agreements.

9.1 Security Requirements of Information Systems

9.1.1 Information Security Requirements Analysis and Specification

- The Information Technology System Development Section, Information Technology Project Management Section, and any assigned units developing or acquiring information systems for the Company use must clearly specify the information security requirements for the systems being developed or acquired.
- The Information Technology System Development Section, Information Technology Project Management Section, and any assigned units must monitor the development of information systems to ensure that they meet the specified security and functional requirements.

9.1.2 Securing Application Service on Public Networks

- Information that passes through application services, both in general usage and when using public networks, must be secured to prevent fraudulent activities, incomplete transmission or mis-routing, unauthorized disclosure, copying, or modification.

9.1.3 Protecting Application Service Transactions

- Information related to application service transactions must be protected from incomplete transmissions, mis-routing, unauthorized changes, unauthorized disclosure, and unauthorized copying.

9.2 Security in Development and Support Processes

9.2.1 Secure Development Policy

- The Information Technology Department must establish regulations to ensure the security of information system development throughout the entire development lifecycle.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

9.2.2 System Change Control Procedures

- The Information Technology Department must establish written procedures for controlling changes throughout the information system development lifecycle.

9.2.3 Technical Review of Applications after Operating Platform Changes

- System administrator must perform technical reviews to analyze potential impacts when changing or updating operating systems, such as version changes or security fixes. Testing must be conducted in a testing environment until it is ensured that all processes work normally and securely before making changes in the operational environment.
- System administrator must also perform technical reviews after operating system changes in the real environment to ensure that there are no adverse impacts on system functionality and security.

9.2.4 Restrictions on Changes to Software Packages

- Off-the-shelf software used within the Company should be used without modifications. If changes are necessary, the assigned unit must strictly control these modifications.
- Changes to off-the-shelf software must follow the change control procedures established by the Information Technology Department.

9.2.5 Secure System Engineering Principles

- The Information Technology System Development Section, Information Technology Project Management Section, and assigned units must adhere to the following minimum-security principles in system development:
  - Least Privilege: Grant the minimum necessary privileges to system users to prevent unauthorized modifications.
  - Need to Know: Grant access only to the necessary information to prevent leaks of critical information.
  - In-Depth Defense: Design systems with multiple levels of protection to reduce the risk of unauthorized access.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

- Open Design: Use standard mechanisms or algorithms in system design that can be audited.

9.2.6 Secure Development Environment

- The Information Technology System Development Section, Information Technology Project Management Section, and assigned units must control the development and integration environment to ensure security, including protecting system data during development, transmission, backup, and access control.

9.2.7 Outsourced Development

- The Information Technology Department must establish written agreements for external units developing software for Company use.
- The assigned unit must regularly oversee, monitor, and follow up on the development activities performed by external entities to prevent any damage affecting information security.

9.2.8 System Security Testing

- The Information Technology System Development Section, Information Technology Project Management Section, assigned units, and users must collaborate to test both the functional and security aspects of newly developed or modified information systems.
- Testing must be conducted during development and before the system goes live, with official documentation of the test results.

9.2.9 System Acceptance Testing

- The Information Technology Department must establish criteria for accepting new or enhanced information systems, whether developed internally or procured externally, and ensure these systems are tested before going live.

9.3 Test Data

9.3.1 Protection of Test Data

- The Information Technology System Development Section, Information Technology Project Management Section, assigned units, and users must avoid using actual data

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

from operational systems for testing. If copies of real data are used for testing, the test data must be controlled as stringently as operational data.

10. Supplier Relationships

To establish various requirements and operational frameworks for external entities in providing or utilizing information technology services efficiently, securely, and to the Company's maximum benefit.

10.1 Information Security in Supplier Relationships

10.1.1 Information Security Management System Policy for Supplier Relationships

- The Information Technology Department must establish an Information Security Management System Policy related to external entities. Relevant parties must consider or assess potential risks and establish preventive measures to reduce those risks before allowing external entities or individuals to access the Company's information systems or use its information.
- Administrator and designated departments coordinating with external entities must ensure that external entities or individuals providing services to the organization comply with the specified service agreements or contracts. This compliance should cover security, the nature of the services, and the level of service provided.

10.1.2 Addressing Security within Supplier Agreements

- The Information Technology Department must ensure the establishment of agreements in writer form regarding information security related to granting external entities access to information systems or using information for reading, processing, managing, or developing information systems.
- Administrator and designated departments coordinating with external entities must ensure that external entities can access only the necessary information and that access is granted solely with the written consent of the information owner.
- Administrator and designated departments coordinating with external entities must ensure that external entities comply with the terms or agreements established between the Company and the external entities.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

10.1.3 Information and Communication Technology Supply Chain

- The Information Technology Department must ensure the inclusion of agreements and responsibilities related to information security risks in contracts with external entities providing information technology and communication services, including the subcontractors hired by these external entities.

10.2 Supplier Service Delivery Management

10.2.1 Monitoring and Review of Supplier Services

- Administrator and designated departments coordinating with external entities must monitor and review the operations of external entities responsible for managing the system and processing information for the Company. This review should cover financial status, operational processes, and service efficiency on a regular basis.

10.2.2 Managing Changes to Supplier Services

- In cases where external service providers change processes, procedures, operational methods, or security practices, administrator and designated departments coordinating with external entities must assess the risks associated with these changes. They must report these risks to management and relevant parties and establish appropriate risk management processes.

11. Information Security Incident Management

To establish guidelines for managing information security incidents, learning from mistakes, and making improvements to prevent recurrence of information security incidents.

11.1 Management of Information Security Incidents and Improvements

11.1.1 Responsibilities and Procedures

- The Information Technology Department must define responsibilities for managing unforeseen or unexpected information security incidents and clearly assign operational rights to personnel within the department.
- The Information Technology Department must classify unforeseen or unexpected information security incidents separately from general operational disruptions to determine appropriate corrective measures.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

- The Information Technology Department must establish channels and criteria for reporting incidents, vulnerabilities, or disruptions related to information security and communicate these to Company personnel and external entities.

11.1.2 Reporting Information Security Events

- Users and external entities must report information security-related incidents of the Company to their supervisors and the Information Technology Department through the designated reporting channels as quickly as possible.

11.1.3 Reporting Information Security Weaknesses

- Users and external entities must report information security-related weaknesses of the Company to their supervisors and the Information Technology Department through the designated reporting channels as quickly as possible.
- Users and external entities who discover information security breaches or any weaknesses in the Company's information systems must not disclose the incident to others, except their supervisors and the Information Technology Department, and must not investigate the suspected information security weakness themselves.

11.1.4 Assessment of and Decision on Information Security Events

- Administrator must assess information security-related incidents, classify the incidents or security weaknesses, prioritize them according to the established criteria, and inform the relevant parties to address the issue if the incident or weakness is found to potentially impact information security.

11.1.5 Response to Information Security Incidents

- Personnel assigned to resolve information security incidents, and external entities contracted to do so, must follow the established procedures for addressing information security incidents.
- Personnel assigned to resolve information security incidents, and external entities contracted to do so, must respond to and resolve information security incidents within the specified timeframe. If they are unable to resolve the incident within the given time, they must inform their supervisors as soon as possible.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

11.1.6 Learning from Information Security Incidents

- Personnel assigned to resolve information security incidents and contracted external entities must prepare reports on the analysis and resolution of incidents, weaknesses, or vulnerabilities related to information security. These reports should be stored as knowledge resources to facilitate future learning and reduce the likelihood of recurrence.

11.1.7 Collection of Evidence

- Personnel assigned to resolve information security incidents and contracted external entities must collect evidence related to the information security incidents that occurred. This evidence should be sufficient to present to relevant management and for use in legal proceedings, if necessary.

12. Information Security Aspects of Business Continuity Management

To prevent disruptions or halts in the Company's business operations and safeguard critical business processes from information system failures, ensuring that information systems can be restored within an appropriate timeframe.

12.1 Information Security Continuity

12.1.1 Planning Information Security Continuity

- Data owners and the Information Technology Department must collaboratively identify events that could impact business processes, assess the risks of these events, and evaluate critical systems to obtain accurate and complete information for developing the information security continuity plan.

12.1.2 Implementing Information Security Continuity

- The Information Technology Department must develop an emergency response plan that includes information security measures as an integral part of the plan, ensuring alignment with the Company's business continuity management plan.

12.1.3 Verify, Review, and Evaluate Information Security Continuity

- The Information Technology Department must test the emergency response plan at least once a year and document the test results to ensure the plan's accuracy and effectiveness in supporting operations.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

- Personnel involved in the recovery of information systems must possess the necessary technical knowledge for system recovery and participate in plan drills.
- Data owners and system users involved in the business continuity plan must participate in the plan tests and execute the actions outlined in the plan.

12.2 Redundancies

12.2.1 Availability of Information Processing Facilities

- The Company must ensure an assessment of the availability requirements for highly critical information systems.
- The Company must ensure the installation of backup information systems, backup equipment, or sufficient systems to support services, ensuring appropriate business continuity.

13. Compliance

To ensure that the Company's operations comply with laws, agreements, contracts, and security requirements that the Company and its personnel must follow, including auditing compliance with established Information Technology Policy.

13.1 Compliance with Legal and Contractual Requirements

13.1.1 Identification of Applicable Legislation and Contractual Requirements

- The Information Technology Department must collaborate with the legal department and the Human Resources Department to compile laws, regulations, criteria, and requirements related to information security. These must be documented as written operational guidelines and regularly updated.
- All personnel must strictly adhere to the specified requirements.
- The Company officials are prohibited from using the Company's assets and information technology systems in any manner that conflicts with the laws of the Kingdom of Thailand and international laws under any circumstances.

13.1.2 Intellectual Property Rights

- The Information Technology Department must establish processes for managing the use of licensed software and intellectual property to ensure that the use of information

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

that may be considered intellectual property or the use of software developed by third-party businesses complies with laws and contractual requirements.

- Users must not copy or distribute software that the Company has purchased licenses for, except for making copies solely for emergency use or as backup copies for the original software.
- Users are strictly prohibited from using, copying, or distributing images, articles, books, or any documents that infringe on copyrights or from installing pirated software on the Company's information systems.
- Software developed for the Company, whether by external entities or the Company personnel, is considered the Company's property. Unauthorized copying or distribution of the Company's proprietary software by external entities or the Company personnel is prohibited.
- Users of software on the Company's information systems must strictly adhere to copyright laws, the Company's information security policies, and the software manufacturers' requirements.

13.1.3 Protection of Records

- Data owners must comply with legal requirements related to certain types of information, such as accounting and customer data, and establish guidelines for managing information, including retention periods, to align with these legal requirements.
- Data owners must ensure that logs and other records are protected from damage, loss, alteration, unauthorized access, or unauthorized distribution. The controls must align with applicable laws, regulations, and business requirements.

13.1.4 Privacy and Protection of Personally Identifiable Information

- The Company must protect personal data in accordance with laws, announcements, regulations issued by the government, and various regulations that are applicable to the Company.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

- Information about customers is considered critical. The responsible units must ensure that only authorized personnel and employees, as assigned by their duties or authorized by supervisors, can alter such information.
- Personal information of staff, employees, and customers is considered confidential and can only be disclosed to individuals authorized by the Company.

13.1.5 Regulation of Cryptographic Controls

- The Information Technology Department must ensure that cryptographic controls comply with laws, announcements, regulations issued by the government, and various regulations that are applicable to the Company.

13.2 Information Security Reviews

13.2.1 Independent Review of Information Security

- The Company must conduct information security assessment by Internal Audit Department or independent external auditor to verify compliance with policies, standards, and procedures related to information security, and to review the adequacy of information system controls and compliance with these controls.

13.2.2 Compliance with Security Policies and Standards

- Supervisors of each department are responsible for regularly reviewing the compliance of their personnel with information security policies, standards, and procedures.
- If a supervisor identifies non-compliance with policies, standards, and procedures that does not impact the company's information security, the supervisor must explain the issue to the personnel for understanding. However, if the non-compliance affects the Company's information security, the supervisor must enforce disciplinary action according to the Company's regulations.
- The Information Technology Department must support and provide guidance to other departments regarding the implementation and compliance with information security policies, standards, procedures, and related requirements when requested.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com

13.2.3 Technical Compliance Review

- Regular technical reviews of information systems, such as penetration tests, must be conducted to ensure compliance with the Company's information security policies and international information security standards.
- The Internal Audit Department must examine the technical controls of information systems to verify their adequacy and adherence to the required controls.
- Administrator must regularly conduct security standard tests, such as vulnerability assessments or penetration tests, to ensure compliance with the Company's information security policies and international information security standards.

This Information Security Management System Policy has been considered and approved by the Board of Directors' Meeting No. 3/2567 on 10 May 2024, and is effective immediately.

บริษัท แอดเทค ฮับ จำกัด (มหาชน)
ADDTECH HUB PUBLIC COMPANY LIMITED
อาคารเอ็มไพร์ทาวเวอร์ ห้องเลขที่ 4106-7 ชั้นที่ 41 เลขที่ 1 ถนนสาทรใต้ แขวงยานนาวา เขตสาทร กรุงเทพมหานคร 10120 (ทะเบียนเลขที่ 0107562000068)
Empire Tower, Unit 4106-7, 41st Floor, 1 South Sathorn Road, Yannawa, Sathorn, Bangkok 10120 (Registration No. 0107562000068)
+66 (0) 2835 3957-8 +66 (0) 2835 3959 www.addtechhub.com