

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 1 / 43

Verification and Approval

	Signature		Position	Date
Prepared by	(Jedsada Chaivongsa)		Department Head - IT Technical Infrastructure	April 20, 2023
Verified by	(Natchamon Kaweepisitkul)		VP - IT	April 20, 2023
	(Pavaravadee Wichaidit)		SVP - Supply Chain & IT	April 20, 2023
* Approved by	(Kridchanok Patamasatayasonthi)		MD	April 20, 2023

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 2 / 43

Document History

Revision Number	Revised Topics and Changes	Effective Date
00	A Complete Document	November 1, 2023

Document Distribution Record

☐ Every Department
☐ Specific Department/Line of Work that Issued the Documents
☐ Related Department, please specify

Copy	Agency

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 3 / 43

SCOPE

This policy applies to full-time employees and representatives acting on behalf of Index Living Mall Group Companies.

Policy enforcement encompasses all Index Living Mall Group Companies, including the headquarters, branches, furniture centers, distribution center (DC), The Walk, and branch offices, both current and future.

OBJECTIVES

1. Establish the Information and Communications Technology Security Policy to instill confidence in Information and Communications Technology (ICT) Security and Cyber Security to ensure the operational effectiveness and efficiency of Index Living Mall Group Companies.
2. Establish an ICT Security framework and maintenance system as an ICT standard operating procedure for executives.
3. Establish the scope of the ICT security management system in accordance with the ISO/IEC 27001 standard, and aim for ongoing enhancements.
4. Establish ICT standard operating procedures to promote awareness and strict compliance among executives, system administrators, employees, and external stakeholders of the Company.
5. To be used as a basis for the development and improvement of Information Technology Security.
6. ICT security-related policies and procedures are subject to the determination and approval of the steering committee. It must be communicated to employees and external stakeholders for their acknowledgment. Once approved, all employees shall strictly comply with this policy.
7. An annual review of ICT security is required. Any significant modifications shall be approved by executives.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 4 / 43

Policy Elements

Definitions

Section 1 Information Security Management

Section 2 Computing System Control Room

Section 3 Access Control

Section 4 User Access Management

Section 5 User Responsibilities

Section 6 Network Access Control

Section 7 Operating System Access Control

Section 8 Application Information Access Control

Section 9 Data Backup and Data Encryption

Section 10 Inspection and Risk Assessment

Section 11 Internet Security Policy

Section 12 Use of Electronic Mail

Section 13 Terms of Use and Disclaimer

Section 14 Third-Party Access Control

Section 15 Wireless Policy

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 5 / 43

DEFINITIONS

1. **Group Company** refers to Index Living Mall Public Company Limited and its subsidiaries.
2. **The Company** refers to Index Living Mall Public Company Limited, including the authorized signatories or assigned persons.
3. **Subsidiary** refers to a company in which the Company holds more than 50% of the shares.
4. **Authorized Person** refers to those who are assigned by the Chief Executive Officer to perform duties and responsibilities.
5. **User** refers to authorized users who have the right and responsibilities to access, manage, or maintain the Company's information technology system based on their roles.
 - The Chief Executive Officer (CEO) refers to the Chief Executive Officer of the Company.
 - The Chief Information Officer (CIO) refers to an executive who oversees the management of information technology.
 - An employee refers to a part-time or full-time employee.
 - A third party refers to any individual to whom the Company grants temporary access to its information technology system for the purpose of facilitating the Company's operations. This includes employees or workers of external companies who interact with or maintain the system for the Company, consultants, or contract employees.
6. **Assets** refer to information and communication technology assets or anything of value to the Company. This consists of servers, network infrastructure, software systems and applications, data, database systems, components, and computer systems that are owned, used, and under the responsibility of the Company. The use of information systems includes internal and external services such as internet or e-mail access, etc.
7. **Access or Access Control** process that restricts access, privileges, and authorization to use the Company's network, communication, and information systems, whether in digital or physical form. This includes third-party access restriction to information and service provisions to safeguard against both internal and external unauthorized access.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 6 / 43

8. **Information Security** refers to confidentiality, integrity, and availability of information. This includes other properties such as authenticity, accountability, non-repudiation, and reliability.
9. **Management Security** refers to administrative procedures related to policies, measures, criteria, or any procedures utilized in the selection, development, implementation, or management of information asset security.
10. **Physical Security** refers to policies, measures, criteria, or any procedures that safeguard information assets, buildings, or any other assets against threats, natural disasters, accidents, or any other physical disasters.
11. **Security incidents** refer to events that could indicate potential jeopardy of service or network security and security policies, as well as an inadequacy of security measures or unexpected events that may result in security breaches.
12. **An unwanted or unexpected security event** refers to an unwanted or unexpected security situation that may result in an intrusion or attack on the Company's system.
13. **External agency** refers to organizations or departments authorized by the Company to access and use its information or assets. They are also liable for maintaining the confidentiality of the information.
14. **Password** refers to letters, characters, or numbers used to authenticate users, restrict access to information and database systems, and maintain information technology security.
15. **Computer data** refers to data, commands, or sets of instructions stored and processed by computers, including electronic data, according to the Electronic Transactions Act.
16. **A network system** refers to a system that can be used to communicate or transmit data and information technology systems in the Company, such as LAN systems, intranet systems, and internet systems.
 - LAN systems and intranet systems are electronic network systems that connect multiple computer systems within the Company to build a network for communication and information sharing.
 - Internet system refers to electronic network systems that connect the Company's networks to the global internet network.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 7 / 43

- 17. Information Technology System** refers to the Company's work system that incorporates information technology, computer, and network systems to help generate information for administrative management, service development, and communication control. This includes computer systems, network systems, data, and information programs, etc.
- 18. Information System Workspace** refers to the area where the Company permits the use of information and communications technology systems, as follows:
- General working area refers to the area where personal computers are installed.
 - IT equipment or network area.
 - Data storage area.
- 19. Data owner** refers to an authorized person appointed by the supervisor to manage system data. The data owner bears direct responsibility for data loss.
- 20. The Information Technology Department** refers to the department responsible for computers and information systems. It serves as the hub for the Company's information network, conducts research and analysis to support the Company's information and computer systems, as well as collaborates with or supports the operations of other related departments.
- 21. Electronic mail (email)** refers to a system that enables people to exchange and receive messages using computers and networks. Messages can be sent to a single or several recipients, including letters, images, graphics, animations, and audio.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 8 / 43

Section 1

Information Security Management

1. Objective

To define a responsible person in the event of a breach or compromise of the Company's computer systems or information, and to evaluate policies and practice guidelines to address emerging issues and enhance the quality of information security management.

2. Management Guidelines

2.1.The Chief Executive Officer (CEO) bears responsibility for any risk, damage, or dangers that result from insufficient information security control. This includes breaches or compromises of computer systems, as well as negligence, defects, or violations of policies and practices pertaining to information security maintenance. At least once a year, the Chief Executive Officer shall convene a meeting of the Information System Management Committee, consisting of the Chief Information Officer and other executives, to review information security policies and practice guidelines. It is the responsibility of the Chief Information Officer (CIO) to oversee the Company's information security.

2.2.To promote understanding and support compliance with the information security policy by preparing minutes of the Information System Management Committee Meeting and informing relevant employees to acknowledge and strictly comply with the policy.

2.3.Regularly review the Company's information security policies and practice guidelines at least once a year in order to proactively mitigate any evolving risks that may emerge in the future.

2.4.Evaluate the information security practice guidelines to improve its efficiency in the following year.

2.5.The information security policy must be prepared in writing and aligned with the objectives described in the scope of duties and responsibilities approved by the CEO or CIO for organization-wide dissemination and implementation. This applies to all employees as well as third parties who access the Company's data and information assets.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 9 / 43

- 2.6. Provide human resources, funding, management, and sufficient raw materials for security management in each fiscal year. This includes the information security plan that will be implemented during that fiscal year.
- 2.7. Educate employees on information security in order to foster awareness of the imprudent or careless use of information systems through training at least once a year.
- 2.8. Establish an annual inspection and assessment of operational risks once a year. Develop improvement strategies to review or solve any identified issues.
- 2.9. Conduct IT disaster recovery plan training and drills at least once a year.
- 2.10. Conduct a review and update policies and practices as well as the responsibilities of personnel involved with the Company's information security and IT disaster recovery plan to ensure they are always up to date.
- 2.11. Executives are responsible for establishing and clearly separating areas of the information system workspace which includes the general working area, system administrator area, IT equipment area, data storage area, and wireless LAN coverage area.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 10 / 43

Section 2

Computing System Control Room

1. Objective

Determine preventative measures for user access or access control to computing system control room, network components, and information technology systems based on the information technology components and data, which are valuable assets and must be kept confidential. This measure will be implemented for all users who have access to the Company's information technology system.

2. Access Control

2.1 Install an automatic access control system in the Company to control third-party access to the central control room by using a biometric finger scanner and proximity card technology.

2.2 Install a CCTV system in the Company to monitor and prevent any potential damages from unauthorized persons.

2.3 Determine the appropriate access level for employees to perform assigned duties, including:

2.3.1 Prepare an "Access Control List" to specify the access rights allowed for employees according to their assigned duties.

2.3.2 Assign personnel to record the "Entry/Exit Form for Information System Workspace".

2.3.3 Assign personnel to monitor the records of the Entry/Exit Form for Information System Workspace on a regular basis and update the access control list at least once a year.

2.4 Third parties must sign their names accurately on the Entry/Exit Form for Information System Workspace and must always be accompanied by the contact person.

2.5 Anyone who does not have work-related duties to enter the area must obtain authorization from the responsible department. The responsible department must investigate the reasons and necessities before granting permission.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 11 / 43

Section 3

Access Control

1. Objective

To determine access control measures for the Company's information and communication technology systems to prevent network intrusion from unauthorized command messages that will damage data or disrupt the operation of information and communication technology systems. To accurately identify users that access the Company's information and communication technology system.

2. Access Control Procedures

2.1 The location of information technology systems must be secure; only authorized personnel are permitted to enter.

2.2 Prior to authorizing access to an information and communications technology system, the system administrator must grant users and employees the proper access rights based on their responsibilities. Access rights must be reviewed regularly. System users must receive permission from the system administrator as deemed necessary.

2.3 The system administrator or authorized persons are exclusively responsible for modifying access control rights to information and databases.

2.4 The system administrator should establish a recording system to monitor the use of information technology and any breaches of database security.

2.5 As evidence for an investigation in the event of a problem, the system administrator must maintain a log of who has accessed the system, what permissions have been modified, and who has entered and exited the system's location. This includes both authorized and unauthorized users.

3. Access Control to Information Technology Systems

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 12 / 43

3.1 The system administrator confirms the approval of user requests and determines access rights for users. Requests for login access must be documented with an approved signature and such documents must be kept as evidence.

3.2 The data owner and system owner shall grant users access only to the information employees need to carry out their tasks. Granting more rights than necessary increases the risk of abuse. As a result, access rights to the system should be determined based on minimum necessity.

3.3 Users must obtain permission from employees responsible for the information and work systems to access the information technology system.

4. User Access Management

4.1 Registration of new employees - a formal procedure shall be established to register new employees with access rights. This includes the procedures for canceling access rights. For example, access cancellation must be completed within 24 hours of resignation and changes to access rights due to internal transfers must be completed within 7 business days.

4.2 Define the access rights required to use important information technology systems, such as computer systems, applications, electronic mail (email), and internet systems. The system administrator must grant users written authorization for access in order to perform their duties. Access rights must be regularly reviewed.

4.3 Users must affix their signatures to acknowledge the rights and duties regarding the use of the information technology system and strictly follow the policy.

4.4 User Accounts and Passwords for Employees

4.4.1 The system administrator is responsible for determining employee access to information technology systems. Access rights must align with duties and responsibilities outlined in the "User Access Management" guidelines.

4.4.2 Password changes and cancellations must follow the "User Access Management" guidelines.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 13 / 43

4.4.3 In the event of an emergency, “privilege accounts may be granted”. This means that the highest privileged accounts must be considered for approval based on the following factors.

4.4.3.1 The system administrator must request approval from the supervisor prior to granting the privilege accounts.

4.4.3.2 It should only be used in emergency situations and under strict control.

4.4.3.3 Determine the duration. Upon the expiration of the designated period, the privileged access right shall be promptly revoked.

4.4.3.4 Passwords must be changed frequently. For example, when access is no longer required or when continuous access is necessary, the password should be changed every three months, etc.

4.5 Access Control in Accordance with Levels of Confidentiality

4.5.1 The system administrator must determine the data's level of confidentiality, the procedures for storing the data, the procedures for controlling access to each type of data, and the confidentiality levels, both direct and indirect access via the work system. This includes methods for disposing of confidential data at all levels.

4.5.2 Data owners must review the suitability of user access rights at least once a year to ensure that the various rights provided remain appropriate.

4.5.3 Determine access control methods for data confidentiality at all levels, including direct and indirect system access. The system administrator is responsible for creating user accounts and passwords to ensure that data users' true identities are verified at all levels of confidentiality.

4.5.4 Sensitive data transmitted over public networks should be encrypted in accordance with international standards.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 14 / 43

4.5.5 Passwords should be changed at scheduled times based on the level of data sensitivity specified in the "User Access Management" guidelines.

4.5.6 Data security measures should be put in place when computers are removed from the Company's premises. For example, when sending computers for repairs, data should be backed up to an external hard drive before deleting data on the computer.

5. Network Access Management

5.1 To ensure control and prevent systematic intrusion, system administrators must design the network system in accordance with groups of information technology services utilized by groups of users and groups of information systems, such as internal zones, external zones, etc.

5.2 System administrators must have methods to limit user access rights so that users can only access the networks that they are authorized to use.

5.3 Administrators should have methods to restrict access to shared networks.

5.4 System administrators should have methods to restrict the use of enforced paths from client-server networks, preventing users from accessing alternative paths. Assign a responsible person to edit or modify parameters.

5.5 Protect networks and devices that are clearly linked to the network system. Check the configuration of the parameters at least once a year. Additionally, any changes to parameters should be communicated to relevant parties.

5.6 All network systems connected to external systems should use an intrusion prevention device or packet filtering program, such as a firewall or malware detection hardware.

5.7 Install an intrusion detection system (IPS/IDS) to monitor users who access the Company's network in an abnormal way. This includes checking for intrusions, abnormal use, and unauthorized changes to the system.

5.8 To ensure accuracy, users must log in and authenticate when accessing the Company's network system via the internet.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 15 / 43

5.9 The Company's internal IP address should be hidden from connected external entities to prevent outsiders from discovering the network infrastructure.

5.10 A network diagram detailing the boundaries of internal and external networks, as well as devices, must be prepared and updated on a regular basis to remain current.

5.11 System administrators should approve the use of various network monitoring tools and they should be used only as needed.

5.12 Only employees from the Information Technology Department are authorized to install and connect network equipment.

6. Server Management

6.1 Assign the person in charge of server maintenance to edit server settings and modify system software configurations.

6.2 A procedure or practice should be in place to check the server system in case of abnormal usage or changes. Corrective actions must be taken and reported immediately.

6.3 Telnet, FTP, Ping, and other services should only be enabled when necessary. However, if the required service poses a threat to the security system, additional security measures must be implemented.

6.4 Install and update the software system on a regular basis to prevent system software flaws, such as web servers.

6.5 Test system software for security and effectiveness before installation and after modifications or maintenance.

6.6 Only Information Technology Department employees may install and connect software to the server.

7. Recording and Monitoring Management

7.1 The server and network systems should have application logs that record details about the intrusion prevention system, such as system entry and exit logs, login attempt logs, command line and firewall logs, and so on. These records must be kept for a minimum of three months.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 16 / 43

7.2 Application logs should be monitored regularly.

7.3 There must be a method for preventing record alteration and restricting access to only relevant personnel.

8. External Control Access to the System must be determined and controlled by the system that the system administrator has installed to ensure security, as follows:

8.1 Users attempting to access the company's network via remote access must be controlled. Additional security measures should be stricter than internal access.

8.2 Remote access to data or information systems requires approval from the Chief Information Officer or the director of the relevant department. Users must strictly adhere to the Company's regulations when accessing the system and information.

8.3 In order to receive remote access, users must present sufficient proof of their need to collaborate with the Company, which must receive approval from authorized personnel.

8.4 The port used for logging in should be closely monitored.

8.5 Remote access should only be permitted when it is necessary, with no ports left open unnecessarily. Such channels should be disconnected when they are no longer in use and reopened only when requested.

9. Authentication for External Users

9.1 When accessing the Company's system, every user must complete identity verification as follows:

9.1.1 Username

9.1.2 Password

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 17 / 43

Section 4

User Access Management

1. Objective

To determine measures for users who access information technology systems. Personnel who do not have work-related responsibilities should not be permitted to access the information technology system or internal network without permission. This includes restricting access to information technology systems so that the Company can monitor, track, and verify the identity of those who access its information and communication technology.

2. User Registration

- 2.1 Prepare user registration forms for the Company's information technology system.
- 2.2 System administrators must verify user accounts, especially those who have not registered as users before.
- 2.3 System administrators must review and grant appropriate access to their responsibilities.
- 2.4 System administrators must provide users with written documentation outlining their rights and responsibilities when accessing the information technology system. Users must sign their names once they have read and understood their rights and responsibilities.
- 2.5 When a user resigns or changes jobs, the system administrator must remove their access to the information technology system immediately.
- 2.6 System administrators must examine or review all user accounts to prevent unauthorized access to information technology systems.

3. User Management

- 3.1 System administrators must define the rights to use the information technology system, limiting them to the performance of duties and reviewing such rights on a regular basis.
- 3.2 System administrators must establish appropriate access levels for information technology systems.
- 3.3 System administrators must grant rights in accordance with access control policies.
- 3.4 System administrators are responsible for storing access-right documents.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 18 / 43

3.5 When it is necessary to grant privilege accounts, a duration must be specified, and the privileged access should be revoked immediately upon expiration or retirement. The level of privileged accounts must be determined and the privileged accounts must be distinct from those of general users.

4. User Password Management

4.1 To prevent the disclosure of passwords, the system administrator must require users to sign a document outlining their rights and responsibilities when accessing the Company's information technology system.

4.2 System administrators must establish procedures for creating and changing secure passwords.

4.3 System administrators should remind users to change temporary passwords immediately and create new passwords that are difficult to guess.

4.4 System administrators must create a temporary password that is difficult for others to guess and create different passwords.

4.5 System administrators must send the password to the user without using email and the user must respond after receiving the password.

5. Review Of User Access Rights

5.1 System administrators should review user access rights at least once a year.

5.2 System administrators should review the access rights of high-privilege accounts more frequently than general users such as those with privileged access rights equal to system administrators.

5.3 System administrators should schedule access rights reviews whenever there is a change, such as a promotion, demotion, department transfer, or termination of employment.

5.4 System administrators must document changes to high-privilege accounts for future review.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 19 / 43

Part 5

User Responsibilities

1. Objective

To control and establish measures for users who require access to the Company's information technology in order to carry out their assigned duties. To prevent unauthorized access or disclosure of information.

2. Password Use

Users of information technology systems should comply with the password requirements listed below:

2.1 Users should set a password that is difficult for others to guess.

2.2 Users must not reveal their passwords.

2.3 Users should store their passwords in a secure location.

2.4 Users should change their password immediately when they become aware that their password may have been disclosed or known by others.

2.5 Users should set a password that is longer than the minimum required.

2.6 Users should create a password that is easy to remember.

2.7 Users should not create passwords from words that appear in the dictionary.

2.8 Users should avoid setting passwords that contain a sequence of characters such as 123, abcd, or a group of identical characters such as 111, aaa, etc.

2.9 Users should change their passwords according to the specified period of time.

2.10 Users should change their password without using the same password they have used previously.

2.11 System administrators should change passwords more frequently than other users, such as every 3 months for system administrators and 6 months for system users.

2.12 Users should immediately change the temporary password they received when logging into the system for the first time.

2.13 Users should not require their passwords to be saved or memorized for their convenience when logging in later.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 20 / 43

2.14 Users should not share their passwords with others.

2.15 Users should avoid using the same password for different systems in use.

3. Protection when the device is not in use

3.1 System administrators must require users to immediately log out of the information technology system after completing their tasks, including work systems, computers, and notebooks.

3.2 When not in use or left unattended for an extended period of time, users should lock important devices.

3.3 System administrators should require employees to enter the correct password before using their computers or information technology systems to prevent others from accessing them.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 21 / 43

Part 6

Network Access Control

1. Objective

To determine control measures to prevent unauthorized users from accessing, acquiring, and modifying the critical network and communication system which could harm the Company's data and information systems. The VLAN network defines the process of controlling access to various networks within different network groups.

2. Access Control Process and Network Services

2.1 Network Services

2.1.1 Users are prohibited from using information in manners that violate the law or public morals.

The user agrees that if such an action is taken, it will be considered beyond the Company's responsibility.

2.1.2 The Company prohibits users from making commercial gains from the computer and network, such as announcing the filing of a report, purchasing or distributing products, trading information, charging for information search services, advertising a product, or offering internet services to the general public for a profit.

2.1.3 Users must not violate the rights of others, which means they must not read, write, delete, change, or edit any content that is not their own without permission. Users must not infiltrate (hack) another user's account. Any messages that may cause damage or embarrassment to others, use impolite language, or write messages that harm others are considered a violation of the rights of others, and the user bears sole responsibility for these actions. The Company is not liable for such damages.

2.1.4 Never allow unauthorized access to the system. Hacking or attempting to infiltrate the system is considered an invasion of the Company's restricted area.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 22 / 43

2.1.5 User accounts are assigned to specific individuals. Users are not permitted to transfer or distribute this right to others.

2.1.6 Users are responsible for the results of their assigned user account. This includes any damages or effects caused by that user account unless it can be proven that the damage was caused by the actions of others.

2.2 The Guidelines for Network Control Room Administrator and Staff are as follows:

2.2.1 The network control room administrator must grant access rights for people to enter and exit the control room and network systems, particularly those who perform internal duties and are recorded under "Access Control List," such as computer operators and system administrators.

2.2.2 The Chief Information Officer must grant each employee written authorization to enter and exit the network control room. The rights of each staff member are determined by their duties in the network control room.

2.2.3 The network control room administrator collects fingerprints from employees using fingerprint collection machines and records them on key cards to track the entry-exit history in the network control room.

2.2.4 If an employee who is not on regular duty needs to enter and exit the network control room, they must contact the network control room administrator and request permission to enter the network control room, as well as specify the reason for their visit.

2.2.5 After the process is completed, the employee who has no relevant duties must be informed to notify the network control room administrator to check the completeness and accuracy.

2.3 Guidelines for Visitors from External Agencies:

2.3.1 Visitors from external agencies must contact the network control room administrator and explain the reason for entering the network control room.

2.3.2 After the process is completed, the visitors must be informed to notify the network control room administrator to check the completeness and accuracy.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 23 / 43

Part 7

Operating System Access Control

1. Objective

To inform users of their duties and responsibilities while using the operating system and ensure their understanding and strictly adhering to the policy in order to protect the Company's resources and information by maintaining confidentiality, accuracy, and availability of the Company's resources at all times.

2. Establishing Procedures for Secure Access

2.1 Users should set a password to use the computer they are responsible for.

2.2 Users should enable a screen saver program to lock the screen when not in use. After that, users must enter their password to gain access.

2.3 A username and password must be entered to log in to the system.

2.4 Users must not share their username and password to access the Company's computers.

2.5 Log out immediately if the device is not being used or will be away from the screen for an extended period of time.

3. User Identification and Authentication

3.1 To prevent unauthorized access, users must verify their identification when logging into the information technology system. If there are any difficulties in identifying and verifying the user's identity or if an error occurs, the user must notify the system administrator so that corrections can be made.

3.2 The user account is responsible for any consequences that may result from using the computer and network system under the assigned account unless it can be proven that the damage was caused by the actions of others.

3.3 Users must keep their user accounts confidential and not disclose them to others. Users may not transfer, sell, or distribute the account to others without the supervisor's permission.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 24 / 43

3.4 Users must log in using their own user account and log out once finished or temporarily stop using the device.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 25 / 43

Part 8

Application Information Access Control

1. Objective

To determine access control measures for unauthorized persons to access the Company's information and communication technology systems. To prevent network intrusion from unauthorized command messages that will damage data or disrupt the operation of information and communication technology systems. To accurately identify users that access the Company's information and communication technology system.

2. Information Access Control

2.1 System administration must establish a formal procedure to register new employees with access rights. This includes the procedures for canceling access rights due to resignation or internal transfers, etc.

2.2 The system administrator must establish permissions for accessing critical information technology systems such as computer systems, applications, electronic mail (email), wireless LAN, internet systems, etc. Specific rights must be granted for the performance of duties and approved in writing by the supervisor. The access rights must be regularly reviewed.

2.3 The system administrator must manage access rights and employee passwords as follows:

- 2.3.1 Change and cancel passwords when users resign, leave their position, or stop using them.
- 2.3.2 Deliver temporary passwords to users in a secure manner. Passwords should not be sent to other people or via unprotected email.
- 2.3.3 Require users to confirm that they received their passwords.
- 2.3.4 Users must not record or store passwords in the computer system that allows unauthorized access.
- 2.3.5 Create different user names or accounts.
- 2.3.6 When it is necessary to grant privilege accounts, a duration must be specified and the privileged access should be revoked immediately upon expiration or retirement. The level of

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 26 / 43

privileged accounts must be determined and the privileged accounts must be distinct from those of general users.

2.4 The system administrator must determine the data's level of confidentiality and the procedures to control access to levels of confidentiality both direct and indirect access via the work system. This includes methods for disposing of confidential data as follows:

- 2.4.1 Control access to data's levels of confidentiality whether direct access or indirect access through work systems.
- 2.4.2 Create usernames and passwords to verify the identification of data users for each level of data confidentiality.
- 2.4.3 Set a usage duration period and terminate the use as soon as that period has expired.
- 2.4.4 Important information transmitted over public network systems should be encrypted in accordance with international standards such as SSL, VPN, and XML Encryption.
- 2.4.5 Schedule password changes based on the specified period of data importance.
- 2.4.6 Determine data security measures for computers taken outside the Company's premises.
For example, when sending computers for repairs, data should be backed up to an external hard drive and then it can be deleted from the computer.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 27 / 43

Part 9

Creating a Data Backup System

1. Objective

To define data backup and system recovery procedures to enable computer and network administrators to backup and restore data as needed.

2. Guidelines for Backing Up Data and Computer Systems

2.1 Computer administrators must provide backups and regularly test the backed-up data in accordance with the Company's data backup policy.

2.2 Create operator logs - computer administrators must keep records of backup details such as start and end times, name of the backup operator, data types recorded, etc.

2.3 Fault logging - computer administrators must create fault reports for any errors that occur during backups as well as the methods used to resolve them.

2.4 Computer administrators must delegate backup responsibilities to other personnel in the event that the computer administrators and/or network administrators are unable to perform their duties.

2.5 If a problem is discovered while backing up that prevents the operation from being completed entirely, the computer administrators must solve the problem, summarize the results, and report them to the Chief of Information Officer

2.6 Computer administrators and network administrators must properly schedule data backups and determine the device used to store data. Backup formats are classified as full backup and incremental backup.

2.7 Encrypting backups - to prevent backups from being disclosed, computer administrators must encrypt important backup data using appropriate encryption technology.

2.8 Backup policy - the computer administrators must strictly follow the backup procedures.

3. System Recovery

3.1 In the event that a problem is discovered that may cause damage to the computer system and/or the system network and require a system recovery, the computer administrators and/or network

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 28 / 43

administrators must take corrective actions, keep records, and report the results to the Chief of Information Officer or the designated person assigned by the Chief of Information Officer.

3.2 To restore the system, use the latest backup update or whatever is most effective.

3.3 If damage to the computer system or network system disrupts service or user access, users must be notified immediately. System recovery progress notifications should be sent on a regular basis until the process is completed.

4. Prepare an IT Disaster Recovery Plan

The policy regarding the IT Disaster Recovery Plan must be assigned to relevant departments to carry out the following actions:

4.1 Establish a process for disaster recovery plans for high-priority systems.

4.2 Determine the types of disasters that affect high-priority systems and require response planning.

4.3 Evaluate the risks of high-priority systems being disrupted or unavailable due to disasters.

4.4 Develop a disaster recovery plan for high-priority systems.

4.5 Test, evaluate, and improve disaster recovery plans for high-priority systems at least once a year.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 29 / 43

Part 10

Risk Inspection and Assessment

1. Objective

To establish measures for risk control and prevent incidents that could jeopardize information security.

2. Risk Assessment Guidelines

2.1 Identify risks and risk events in accordance with the Company's risk management plan to assess the risk of damage to the information technology system as a result of human error, computer viruses, electrical system failures, fire damage, theft, and computer theft.

2.2 Establish risk assessment methods and the severity of impacts resulting from those risks.

2.3 Risk assessment must take into account the following elements:

2.3.1 The severity of the effects of the identified risks.

2.3.2 Threats or potential threats and the likelihood of its occurrence.

2.3.3 A weakness or vulnerability that could be exploited to cause the risk event.

2.4 Establish risk management measures.

2.4.1 Conduct a review of the IT Disaster Recovery Plan.

2.4.2 Prepare guidelines, policies, and regulations for the use of computers and the Company's network.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 30 / 43

Part 11

Internet Security Policy

1. Objective

Users will acknowledge and comply with internet security policies and refrain from violating the Computer Crime Act, such as sending messages, command sets, or anything else to the computer system that interferes with normal computer system use or causes the Company's computer system to be disrupted, delayed, or obstructed to the point of being unable to perform normal tasks.

2. Guidelines for Using the Internet

2.1 The system administrator must connect to the internet using the Company's security system, such as a proxy, firewall, or IPS-IDS. Users are prohibited from connecting to the computer system through other channels unless there is an appropriate reason and written permission from the Information and Technology Department.

2.2 Before connecting PCs and laptops to the internet through a web browser, antivirus software must be installed to guard against potential vulnerabilities from the web browser.

2.3 Users should regularly update patches and hotfixes, which can be downloaded from the Microsoft website to solve vulnerability problems.

2.4 Install an antivirus program and scan any data sent or received over the internet.

2.5 Users must not use the Company's internet network to seek personal gain and enter inappropriate websites that violate morals, have harmful content to the nation, religion, and monarchy, or websites that pose a threat to society, etc.

2.6 Users will be assigned access rights according to their duties for the efficiency of the Company's network and information security.

2.7 Users must not disseminate information for personal gain, morally inappropriate information, information that violates the rights of others, or information that may cause damage to the Company.

2.8 Users are prohibited from disclosing important, confidential information that the Company has not yet publicly announced on the internet.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 31 / 43

2.9 The user is prohibited from using data that contains another person's image or image that was created, edited, added, or modified using electronic or other means that will harm the other person's reputation, causing them to be despised, hated, or ashamed.

2.10 After using the internet, close the web browser to prevent others from accessing it.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 32 / 43

Part 12

Use of Electronic Mail

1. Objective

- 1.1 To ensure that message exchanges via electronic mail can support the Company's operations and management in an accurate, convenient, quick, up-to-date, efficient, and effective manner.
- 1.2 To ensure that message exchanges via electronic mail between employees and departments comply with legal requirements.

2. Guidelines for Sending Electronic Mail

- 2.1 The system administrator is responsible for assigning appropriate access rights in accordance with the duties and responsibilities of users and reviewing them on a regular basis, taking into account resignations and other changes, etc.
- 2.2 To verify the true identity of the user of the Company's electronic mail system, the system administrator must grant access rights to new user accounts and create default passwords for first-time users.
- 2.3 New users will be given a default password to use to log into the electronic mail system, and the system will require a password change immediately upon the first login.
- 2.4 An email verification code must not be shown or displayed while entering the password, but it must be displayed as a symbol, such as 'x' or 'o'.
- 2.5 System administrators should limit incorrect password entries to 5 attempts.
- 2.6 System administrators should configure the email system to automatically log users out after a set time, such as 15 minutes. To continue using the system, users must enter their username and password.
- 2.7 Users should not save their password in the email program.
- 2.8 Users should change their passwords regularly. For example, passwords should be changed every 3-6 months.
- 2.9 Users should exercise caution when using electronic mail to avoid causing damage to the Company, infringing on the rights of others, creating a nuisance, committing illegal acts, violating

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 33 / 43

morals, and seeking or allowing others to seek business benefits from the use of electronic mail via the Company's network system.

- 2.10 Users should not use other people's email addresses to exchange messages without their consent. The user account is liable for any actions taken using the email address.
- 2.11 Users should only use the Company's email address for work-related purposes.
- 2.12 To prevent others from accessing electronic mail, the user should log out of the system after each use.
- 2.13 Users should scan attachments from electronic mail for viruses before opening them, using an antivirus program to open Executable Files such as .exe, .com, etc.
- 2.14 Users must not open or forward email or messages from unknown senders.
- 2.15 Users must not send impolite messages or inappropriate information via electronic mail as this may damage the Company's reputation and cause division.
- 2.16 To send confidential information, a user must not state its importance in the email's subject line.
- 2.17 Users should check their email inbox every day and keep their files and electronic mail as small as possible.
- 2.18 To save space on the electronic mail system, users should delete unnecessary emails.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 34 / 43

Part 13

Terms of Use and Disclaimer

1. Objective

- 1.1 To ensure that message exchanges via electronic mail can support the Company's operations and management in an accurate, convenient, quick, up-to-date, efficient, and effective manner.
- 1.2 To ensure that message exchanges via electronic mail between employees and departments comply with legal requirements.

2. Terms of Use and Disclaimer

- 2.1 The Company's email users must adhere to the following laws, regulations, orders, and recommendations:
 - 2.1.1 Computer Crime Act B.E 2550 (2007)
 - 2.1.2 Electronic Transactions Act B.E. 2544 (2001)
 - 2.1.3 Personal Data Protection Act B.E. 2562 (2019)

3. Terms of Use and Disclaimer

- 3.1 Department/personnel must use the Company's electronic mail service for the benefit of the Company only.
- 3.2 Do not use the Company's electronic mail system to conduct business or seek personal benefits.
- 3.3 Do not use electronic mail service to publish, reference, refer to, disrespect, or do any other action that may cause damage to the institutions of the nation, religion, and monarchy.
- 3.4 Do not use the Company's electronic mail system to commit computer crime or any action that is against the law, orders, rules, regulations, and the Company's confidential information measures.
- 3.5 Do not use the Company's electronic mail system for the dissemination of inappropriate information, images, sounds, and messages, or to cause damage to others.
- 3.6 Do not use an email address to express personal opinions that have a negative impact or may cause disgrace or damage to a person or organization.
- 3.7 Do not use an email address for impersonation.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 35 / 43

3.8 Do not take actions that cause problems with system resources, such as:

- 3.8.1 Creating chain mail
- 3.8.2 Sending spam mail
- 3.8.3 Letter bombs
- 3.8.4 Spreading computer viruses

3.9 Users are prohibited from any actions that may lead to damage or cause damage to the Company's electronic mail server system.

3.10 Users must maintain the confidentiality of their personal or organizational password for electronic mail.

3.11 Do not send the Company's confidential information to persons or agencies that are not related to the Company's business.

3.12 When sending confidential information to persons or agencies outside the Company, such information must be encrypted in accordance with the Company's information security practices and measures.

3.13 The password and email address of the organization or individual must be kept confidential. In the event of a breach suspension, the password must be reset to a strong password.

3.14 Email users or persons responsible for the electronic mail address must read the user manual, regulations, instructions, and terms and conditions to use the Company's electronic mail properly of use to correctly use the Company's electronic mail.

3.15 In the event that the Company receives complaints, requests, or incident reports indicating that users are not complying with the regulations or laws, the Company reserves the right to temporarily cancel or suspend service to users in order to investigate and examine the cause.

3.16 Any action related to dissemination, whether via electronic mail or the service user's home page, will be considered an action for which the service user is responsible. The Department of Information Technology is not involved.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 36 / 43

Part 14

Third Party Access Control

1. Objective

Third-party access can pose risks such as unauthorized access, inaccurate corrections, and unauthorized access to work processes. To ensure the safety and security of third-party access to the Company's information and communication technology systems, the Company established practice guidelines for controlling and selecting third-party agencies, including the consultant service development system and using information technology services from external organizations.

2. Guidelines

2.1 The Chief Information Officer must assess the risks associated with accessing information and communication technology or processing devices from external organizations. Appropriate support or corrective measures should be established before granting access to information and communication technology systems to third parties.

2.2 Control third party access to information and communication technology systems.

2.2.1 Third parties requiring access to the Company's information and communication technology systems must obtain written permission from the Chief Information Officer or authorized person.

2.2.2 Create a document form for external agencies that specifies the reason for accessing the information and communication technology system. This must include at least the following details:

- Reason for requesting use
- Duration of use
- Verifying the security of network-connected devices
- Verifying the MAC address of the connected computer
- Establishing measures for disclosure of information

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 37 / 43

- 2.2.3 All external agencies employed by the Company, whether on or off-site, must sign a non-disclosure agreement. The contract must be completed prior to granting access to the information technology system.
- 2.2.4 The Company should consider conducting a risk assessment or establishing internal controls measures for external agencies, depending on the sensitivity of the information and communication technology system in use.
- 2.2.5 Project owners in charge of projects that require access to information from external agencies must designate a primary contact person to have access to the Company's information and sign non-disclosure agreements.
- 2.2.6 For large projects involving external agencies that have access to the Company's important information, the system administrator must control their access in three areas: confidentiality, integrity, and availability.
- 2.2.7 According to the contract, the Company has the right to inspect the use of information and communication technology systems to ensure third party access control.
- 2.2.8 External agencies must prepare and maintain up-to-date operational plans, manuals, and related documents so that the Company can thoroughly supervise and monitor the service providers to meet established standards.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 38 / 43

Part 15

Wireless Policy

1. Objective

To establish control access measures for wireless LAN, assign appropriate user rights based on duties and responsibilities, and review access rights on a regular basis. To enhance the security of the wireless network and system users must pass an identity verification before receiving permission from the system administrator.

2. Guidelines

1. Wireless network administrators must perform the following responsibilities:

- 1.1 The network of the Company is the Company's property. It cannot be used by unauthorized users. Attempting to intrude on the system is considered an invasion of a restricted area and will result in punishment from both the Company and the law.
- 1.2 The system administrator must place the wireless router (access point) in a suitable location so that data does not leak beyond the wireless network usage area of the Company.
- 1.3 Wireless network installation must be installed by separating the wireless network from the LAN internal network for third-party access control.
- 1.4 Wireless access must be determined in accordance with the needs of the user, and the password must be configured per the purpose of use.
- 1.5 Access to the network system is limited to computers that have permission and verification that match the specified username and password.
- 1.6 Change the SSID (Service Set Identifier) provided by the manufacturing factory.
- 1.7 The system administrator is responsible for supervising and preventing unauthorized access from external agencies to the Company's intranet system and database.
- 1.8 The system administrator should use software or hardware to monitor wireless network security and record any suspicious events. An inspection report must be prepared and submitted every

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 39 / 43

3 months. Any abnormal use of the wireless network must be reported to the Chief Information Officer.

2. The duties and responsibilities of the Company's wireless users are as follows:

- 2.1 Users are prohibited from installing or activating their own wireless equipment in the Company, whether it be an access point, wireless router, wireless USB client, or wireless card.
- 2.2 The Company provides user accounts for individual use only. Users may not transfer, sell, or distribute this right to others.
- 2.3 Users are responsible for the use of their assigned user account. This includes the consequences of various damages resulting from that user account unless it can be proven that the damage was caused by the actions of others.
- 2.4 Users are prohibited from using information in manners that violate the law or public morals. The user agrees that if such an action is taken, it will be considered beyond the Company's responsibility.
- 2.5 The Company prohibits users from making commercial gains from the computer and network, such as announcing the filing of a report, purchasing or distributing products, trading information, charging for information search services, advertising a product, or offering internet services to the general public for profit.
- 2.6 Users must not violate the rights of others, which means they must not read, write, delete, change, or edit any content that is not their own without permission. Users must not infiltrate (hack) another user's account or develop any programs or hardware to destroy security mechanisms, access the computers of other departments, publish any messages that may cause damage and disgrace to others, use impolite language, or write messages that harm others. These are considered a violation of the rights of others, and the user bears sole responsibility for these actions. The Company is not liable for such damages.
- 2.7 Users must abide by the Company's regulations and policies, without denying that the users are not aware of the regulations and policies.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 40 / 43

2.8 The Company reserves the right to disconnect and/or terminate use, as well as cancel or suspend any connection and/or use by users who violate or attempt to violate the Company's rules, without prior notice.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 41 / 43

Respond to Information Security Incidents

1. Intruder Protection System

Daily action plan

Examine log files or reports from the intrusion prevention system and the following:

- 1.1 How many attacks occurred? What types of attacks are taking place in large numbers?
- 1.2 Is the type of attack predictable?
- 1.3 How severe is the situation?
- 1.4 The IP address of the attacker's network.

2. Firewall System

2.1 Review the rules of the intrusion prevention system at least once a month.

2.2 Examine log files, firewall reports, and the following:

- 2.2.1 Packets that the firewall blocked.
- 2.2.2 Characteristics of Blocked Packets.
- 2.2.3 A significant quantity of IP address packets belonging to which networks are blocked?

2.3 If an attack on the system or a violation of information security is detected, the Chief Information Officer must be notified to take corrective actions.

3. Internet Threat Protection System

Internet threats or malware include viruses, internet worms, trojans, and spyware.

Daily/weekly/monthly action plan

3.1 Examine log files and reports from cyber threat detection devices and the following:

- 3.1.1 What types of malware are being found in large numbers?
- 3.1.2 What networks is the malware sent from? And where was it sent?
- 3.1.3 Was malware sent from the Company's internal network to the outside?

3.2 Research how to fix a computer infected with malware, particularly the type of malware discovered in the Company's network.

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 42 / 43

3.3 If it is discovered that computers have been infected with or are transmitting malware, the infected device that is connected to the system must be disconnected and restored immediately.

8. Compulsion

All personnel of Index Living Mall Company Limited (hereinafter referred to as "the Company") which includes third parties, whether they are business partners, subcontractors, relevant parties allowed to use the computer system, and all of the Company's information systems are hereinafter referred to as "users".

"Users" are responsible for complying with the policy and other regulations related to the use of computer systems and information systems as strictly defined by the organization. If it is discovered that the "user" has used the computer system and/or the Company's information system in any manner that violates or conflicts with the policy and other regulations mentioned above, the Company reserves the right to take disciplinary action in accordance with the Company's Articles of Association to the highest level and will consider taking immediate legal action in accordance with relevant laws.

9. Termination of Employee Status

Confidential information, formulas, working methods, the Company's internal information, and any other information classified as the Company's intellectual property, including other information communicated through the computer system or the information system to which the "user" has access through a computer system or information system in accordance with the policies and regulations related to the use of computer system. "Users" are obligated to prohibit the dissemination of such information for at least three years from the date the "user" ceases to be a "user" of the Company (or is prohibited from disseminating such information in accordance with the Company's regulations or other contracts with "users" by enforcing the conditional contract with strictest period).

 <u>Information Technology</u>	Information Technology Policy Index Living Mall Public Company Limited and Affiliated Companies		
	TITLE:		CONFIDENTIAL: 01
	TOPIC:		DOCUMENT CODE: ILM-IT-CBS01-00
	EFFECTIVE DATE: November 1, 2023		REVISION: 00 PAGE: 43 / 43

Reference Documents and Forms

No.	Document Code - Name	Description of Use

Tables, References, and Forms