Computer System and Information Security Policy

Triple i Logistics Public Company Limited and Subsidiaries

Security Policy

1. The Company shall take all necessary measures to ensure that various service systems essential to business operations — namely data systems, computer systems, telephone network systems, communication network systems, or what is referred to as Information Technology Systems — are available for use continuously at all times. Data must be accurate and reliable. The Company therefore places the utmost importance on maintaining the security of such systems.
2. The Company has legal obligations to customers, business partners, investors, and employees regarding the protection of data entrusted to the Company, as well as news and information of individuals or juristic persons obtained through the Company's computer systems or through communications via the Company's network, which must be kept confidential. Therefore, executives and employees at all levels must strictly comply with the standards, recommendations, and security maintenance procedures to prevent data and important information from being disclosed, or from being accessed by unauthorized persons through force or intent.
3. The Company has designated a unit responsible for overseeing the security of computer systems and information systems in accordance with this policy. It monitors and audits the operational practices of various units on a regular basis to ensure that the security of the Company's computer systems and information systems is maintained within the standards set by the Company.

Objectives

1. To build knowledge and understanding so that employees comply with correct regulations, including laws related to computer systems and information systems.
2. To enable employees and authorized users or those connected to the Company's computer systems to use the Company's computer systems and information systems correctly and appropriately.
3. To prevent the Company's computer systems and information systems from being attacked, stolen, damaged, sabotaged, or subjected to any form of criminal activity that may cause damage to the Company's business operations.

Duties and Responsibilities

1. Duties of Supervisors

1.1 Inform employees of the Company's various regulations, orders, and guidelines related to computer system and information security.

1.2 Supervise, advise, and warn in cases of non-compliant practices.

1.3 Consider appropriate disciplinary action against offenders consistently and fairly.

2. Duties of Employees

2.1 Must study, understand, and strictly comply with the Company's various regulations, orders, and guidelines related to computer system and information security.

2.2 Fully cooperate with the Company in protecting the Company's computer systems and information systems.

2.3 Immediately notify the Company upon discovering non-compliant practices, or discovering attacks, theft, damage, sabotage, or any criminal activity that may cause damage to the Company.

3. Employees Authorized to Use Computer Equipment Must Comply with the Following:

3.1 Must log out and log off all systems and shut down computers and other peripheral devices immediately when not in use for an extended period or after finishing work.

3.2 Must set a password to lock the screen (Lock Screen) when not in use or when performing other activities briefly or for a short period, to prevent unauthorized persons from accessing the system.

3.3 Must check all data brought into their own computer every time, using up-to-date anti-virus software.

3.4 Passwords and other credentials assigned by the Company to employees for accessing the Company's computer systems or data are personal and confidential, and must not be shared with others. Employees must change their passwords and other credentials when the old password has expired within the set timeframe, or when an employee suspects that the password may have been compromised. Passwords and other credentials must not be set as repetitions of old passwords, set to passwords easily guessable by others, or set as the same password across all systems where the employee has access rights.

4. **Employees with Duties Related to External Parties** must ensure that such external parties comply with the Company's computer system and information system usage regulations.

Definitions

1. **"Company"** refers to Triple i Logistics Public Company Limited and all subsidiary companies.
2. **"Employee"** refers to employees hired as permanent employees, fixed-term employees, employees under special contracts, and executives at all levels under the Company's employment.
3. **"Computer System"** refers to any computer device or equipment of any size, both Hardware and Software, network equipment connecting data of all types — wired and wireless — storage devices, data transfer devices of various types, the Internet system and Intranet system, as well as electrical equipment and communications devices of various types that can perform tasks, or are used in a similar manner or are linked to computers. All are the property of the Company, the property of the Company's customers or other companies that are under installation, or have not yet been handed over, or are the property of employees who bring them in for installation or use within the Company's business premises.
4. **"Computer Data"** refers to information represented as electrical signals, light, sound, or any other form that can be changed or presented in a way that humans can understand, such as letters, images, moving images, sounds, or any other symbol that can communicate meaning between individuals, which can be transmitted from one point to another via electronic devices or computer equipment, or stored in a device or equipment that can be retrieved for later use, whether instantly or after some delay.
5. **"Information System Data"** refers to data, news, records, histories, content in documents, computer programs, computer images, sounds, symbols, and various characteristics — regardless of how it is stored — in a format that enables communication of meaning for individuals to directly understand, or through any device or equipment.
6. **"Important Data"** or **"Confidential Data"** refers to information system data that is significantly important to the Company's business operations, or that the Company is obligated to protect under the law, business conduct regulations, or agreements with the Company that must not be disclosed to other individuals, or used for any other purpose than the Company's business operations. Leakage of important data or confidential data as described above may cause the Company to cease operations or be significantly damaged, or the Company to lose its reputation.
7. **"Critical System"** refers to a computer system or information system used by the Company for business purposes, including systems that directly generate revenue and systems that support revenue generation, as well as other electronic systems that support the Company's business operations, whether in normal operation or systems designated by the Company's information

system. If such a critical system ceases to function or has reduced capacity that affects the Company's business operations, it must be urgently restored or its capacity improved.

8. **"System Administrator"** refers to employees authorized (generally referring to all information technology employees of Triple i Logistics Public Company Limited (internal employees) and information technology service companies (external parties) that have been hired or authorized by Triple i Logistics Public Company Limited to be responsible for overseeing the Company's information systems), to oversee, use, and maintain the Company's computer systems, including all Hardware, Software, and peripheral devices that constitute the system. The system administrator is authorized to modify, add, fix, or improve the system's computer systems of the Company to operate correctly, with optimal performance aligned with business needs and security.

9. **"Security Maintenance"** or **"Security"** refers to processes and actions such as prevention, inspection, careful attention, caution in use, and maintenance of computer systems and information systems that are part of the system, as well as important data, to prevent both internal employees and external parties from accessing them for the purpose of committing crimes, causing damage, or sabotaging, which could cause damage to the Company's business operations.

Discipline and Penalties

1. Supervisors at all levels are responsible for ensuring that employees comply with discipline and do not neglect any actions that constitute a violation. If there is a violation or neglect, the supervisor shall impose a penalty on the offender as appropriate.

2. The following actions constitute disciplinary violations:

    2.1 Altering, modifying, or correcting data in another person's communications without authorization.

    2.2 Disclosing knowledge or business news information that is confidential or a matter not to be disclosed by the Company to others without the Company's authorization.

    2.3 Fraudulently decoding or cracking passwords or other credentials in order to access or use computer systems with the intent to commit fraud against the Company's property, money, or customers, or to cause damage to the Company's reputation.

    2.4 Using another person's password or credentials to access the Company's computer system to read, select, copy, approve, modify, change, or delete data — for any purpose, whether for one's own or another person's benefit.

2.5 Carelessly, negligently, or failing to keep passwords or other credentials confidential, or consenting to allow others to use one's password, other credentials, and access rights to one's own computer system.

2.6 Deliberately and intentionally stealing or taking the Company's data to disclose, sell, distribute, or give to others for personal benefit or for others' benefit without authorization, or causing the Company to suffer damage.

2.7 Carelessly and negligently failing to prevent others from being able to steal or disclose, sell, or distribute the Company's data.

2.8 Attempting to access computer data, information system data, important data, confidential data, or critical systems without authorization or without being authorized to use them.

2.9 Deliberately and intentionally sabotaging, damaging, or destroying information system data, computer systems, or other equipment to cause damage to the Company.

2.10 Committing espionage, eavesdropping, intercepting, or decoding information system data to obtain information or secrets of others or of the Company, with intent to cause damage to others or to the Company.

2.11 Installing, possessing, or using Hacking Tools or any other software related to inspection and security maintenance of computer systems and information systems — except for individuals or units with responsibilities related to the security maintenance of computer systems and information systems specifically, or those who have received approval from the unit responsible for computer system and information system security exclusively, or the Company's information systems only.

2.12 Connecting computers that are not the Company's property to the Company's computer system or network, whether from inside or outside the Company, without authorization from the responsible unit.

2.13 Independently setting, installing, or changing IP Addresses or MAC Addresses without authorization from the responsible unit.

2.14 Modifying, cutting, removing, installing additional items, or relocating any component of the computer system through personal actions or by bringing in components or other computer equipment that are not the Company's property, which may cause damage to the Company, or installing additional items or adding to the Company's property without authorization.

2.15 Transmitting data, sending, importing, viewing, or possessing content that is inappropriate or illegal, such as content, images, obscene content, gambling, or anything else that undermines institutions such as national institutions, religion, the monarchy, or that incites conflict among the public or employees, or causes damage to the Company.

2.16 Sending messages or inappropriate content using the Company's Email system or communications devices, such as threatening messages, harassment, stalking, blackmail, or sending junk mail (spam), etc.

2.17 Using the Internet, Intranet system, or Email for matters unrelated to the Company's business.

2.18 Using the Company's computer equipment and other devices as personal property for personal entertainment or personal benefit.

2.19 Using Software that is illegally copyrighted, or that the Company has not authorized for use, or that may cause damage to the Company.

2.20 Assisting or cooperating with external parties to access the Company's computer system or information system, causing data to be stolen or the Company's information system or computer system to be destroyed.

2.21 Deliberately, carelessly, negligently, or supporting the commission of offenses under the Computer Crime Act or any other related laws.

3. The Company reserves the right to audit the use of computer systems and information systems by all employees to ensure that the security of information systems and computer systems is appropriate as prescribed by the Company. The Company may audit data passing through the Company's computer systems at any time.

4. Penalties

4.1 Verbal warning

4.2 Written warning

4.3 Suspension

4.4 Termination

For employee penalties, the Company is not required to follow the above order. The Company may choose to impose penalties by considering the severity of the offense committed.

5. The Computer System and Information Security Policy shall be considered part of the regulations related to employment.

This policy is effective from December 16, 2025, by approval of the Board of Directors at the Meeting No. 8/2025.