primo
SERVICE SOLUTIONS

# Information Technology Security Policy and Guidelines

PRIMO SERVICE SOLUTIONS PUBLIC COMPANY LIMITED
496 Moo 9 Sukhumvit 107 Road, Samrong Nuea,
Muang Samut Prakarn District, Samut Prakarn 10270
T 02 081 0000 E info@primo.co.th
WWW.PRIMO.CO.TH

primo
SERVICE SOLUTIONS
PUBLIC COMPANY LIMITED

## Table of Contents




**PRIMO SERVICE SOLUTIONS PUBLIC COMPANY LIMITED**
496 Moo 9 Sukhumvit 107 Road, Samrong Nuea,
Muang Samut Prakarn District, Samut Prakarn 10270
**T** 02 081 0000 **E** info@primo.co.th
WWW.PRIMO.CO.TH

**PRIMO SERVICE SOLUTIONS PUBLIC COMPANY LIMITED**
496 Moo 9 Sukhumvit 107 Road, Samrong Nuea,
Muang Samut Prakarn District, Samut Prakarn 10270
**T** 02 081 0000 **E** info@primo.co.th
WWW.PRIMO.CO.TH

primo
SERVICE SOLUTIONS
PUBLIC COMPANY LIMITED

# Information Security Policy

To ensure that the information technology systems, information systems, computer systems, and network infrastructure of Primo Service Solutions Public Company Limited, its subsidiaries, and affiliated companies utilizing shared information systems and computer networks are managed appropriately and securely, and are capable of continuously supporting the Company's business operations, the Company has established this Information Security Policy.

This Policy is intended to ensure that all information systems are used appropriately and in compliance with the Computer Crime Act and other applicable laws and regulations, while protecting the Company's information assets against threats that may result in loss, damage, or disruption to its operations. The Company therefore establishes the following Information Security Policy.

## Definitions

The following definitions are provided to ensure a common understanding of the terms used throughout this Information Security Policy and its related security procedures.

**"Company"** means Primo Service Solutions Public Company Limited, its subsidiaries, and affiliated companies that utilize shared information systems, computer systems, and network infrastructure.

**"Human Resources Department"** means the Human Resources Department of Primo Service Solutions Public Company Limited.

**"Information Technology Department"** means the Information Technology Department of Primo Service Solutions Public Company Limited.

**"Building and Facilities Management Department"** means the Building and Facilities Management Department of Primo Service Solutions Public Company Limited.

PRIMO SERVICE SOLUTIONS PUBLIC COMPANY LIMITED
496 Moo 9 Sukhumvit 107 Road, Samrong Nuea,
Muang Samut Prakarn District, Samut Prakarn 10270
T 02 081 0000 E info@primo.co.th
WWW.PRIMO.CO.TH

**"User"** means directors, executives, personnel, authorized related users, and authorized external users who have been granted permission to access the Company's information systems or network infrastructure.

**"Personnel"** means permanent employees, probationary employees, temporary employees, and other personnel employed by the Company.

**"Related User"** means any individual or juristic person that has entered into a contractual relationship with the Company and performs activities within the Company's premises or accesses the Company's information systems in connection with such engagement.

**"External User"** means any individual or juristic person other than the Company's personnel or related users.

**"System Administrator"** means the Manager of the Information Technology Department or any other personnel formally assigned by a department director or higher authority to be responsible for the development, modification, maintenance, administration, and operation of the Company's information systems and network infrastructure, or any organizational unit directly responsible for managing such systems and networks.

**"Information"** means facts or data that have been processed, organized, or structured into meaningful forms that are easily understood and can be utilized for management, planning, decision-making, or other business purposes. Information may exist in various forms, including numerical data, text, documents, diagrams, maps, photographs, films, images, audio recordings, computer-generated records, graphics, or any other media.

**"Information System"** means the Company's system for collecting, storing, processing, managing, and disseminating information through the coordinated operation of hardware, software, data, users, and processing procedures, enabling information to support business planning, management, decision-making, and the Company's operational processes.

**"Network"** means the communication infrastructure used for transmitting data and information among the Company's information technology systems, including but not limited to Local Area Networks (LAN), Wireless Networks, Intranet, Internet, and other communication networks.

**"Asset"** means any tangible or intangible item that has value to the Company, including information, information systems, and information and communication technology (ICT) assets, such as personnel, hardware, software, computers, servers, information systems, network infrastructure, network devices, IP addresses, licensed software, or any other asset of value to the Company.

**"Information Security"** means the protection of the Company's information systems and network infrastructure by preserving the confidentiality, integrity, and availability (CIA) of information, together with other security properties, including authenticity, accountability, non-repudiation, and reliability.

**"User Access Rights"** means the authorization levels assigned to personnel and related users for accessing the Company's information systems and network infrastructure, including general privileges, privileged access, and any other access rights granted in accordance with their duties and responsibilities.

**"Access Control"** means the process of granting authorization, assigning access privileges, or delegating authority to users to access or use the Company's information systems or network infrastructure through electronic or physical means, including the establishment of controls to prevent unauthorized access.

**"User Account"** means an employee identification number, e-mail account, username, and password assigned to personnel, related users, and external users for authorized access to the Company's information systems.

**"Information Security Event"** means an identified occurrence involving a system, service, or network that indicates a possible breach of the Company's Information Security Policy, the failure of a security control, or any event that may be relevant to information security.

**"Information Security Incident"** means an unwanted or unexpected event that may compromise the confidentiality, integrity, or availability of the Company's information systems or network infrastructure, or otherwise threaten the security of the Company's information assets.

**"Encryption"** means the process of converting information into an encoded format to prevent unauthorized access. Encrypted information can only be restored to its original form through the use of an appropriate decryption method or key.

**"Authentication"** means the security process used to verify the identity of a user before granting access to an information system, typically through the use of a username and password or other approved authentication mechanisms.

**"SSL (Secure Sockets Layer)"** means an encryption technology used to secure communications and data transmission over the Internet between a server and a web browser or application.

**"VPN (Virtual Private Network)"** means a secure virtual network that enables encrypted data transmission over public communication networks, such as the Internet, ensuring that transmitted information remains confidential and cannot be intercepted or viewed by unauthorized parties during transmission.

primo
SERVICE SOLUTIONS
PUBLIC COMPANY LIMITED

## Chapter 1

### Governance of Enterprise Information Technology (IT Governance)

The objective of Information Technology (IT) Governance is to ensure that the Company achieves its strategic and operational objectives through the effective use of information technology as a key business enabler. Information technology shall support the Company's operations by improving efficiency, productivity, and service quality while enabling the effective management of risks arising from the use of technology, whether such risks originate from internal or external factors.

Effective IT Governance requires the integration of IT management processes, technology resources, information assets, and business continuity planning to support the Company's policies, strategies, business objectives, and enterprise risk management framework. It also requires appropriate monitoring, reporting, and performance evaluation to ensure that information technology continuously supports the Company's business strategies, achieves organizational objectives, strengthens its competitive capabilities, and creates sustainable value for the Company.

To support the above principles, the Company shall implement the following requirements:

### Information Security Policy

- The Company shall establish and maintain a documented Information Security Policy. The responsibility for developing, maintaining, and overseeing the implementation of the Policy shall be clearly assigned to appropriate personnel.
- The Company shall communicate the Information Security Policy throughout the organization to ensure that all personnel understand and comply with its requirements. Effective communication and coordination shall be maintained between the Information Technology Department and all other business units to support efficient operations and the achievement of the Company's business objectives.

- The Company shall review the Information Security Policy at least **once annually**, or whenever significant changes occur that may affect the Company's information security environment, business operations, legal or regulatory requirements, or information technology infrastructure.

**Information Technology Risk Management Policy**

The Company's Information Technology (IT) Risk Management shall be aligned with the **Enterprise Risk Management Policy** and shall cover, at a minimum, the following requirements:

**1. Roles and Responsibilities for IT Risk Management**

The Company shall clearly define roles and responsibilities for the management of information technology risks.

The Manager of the Information Technology Department shall be responsible for identifying, evaluating, and proposing appropriate information technology solutions, controls, or mitigation measures to reduce or manage IT-related risks. Such proposals shall be submitted to Management for consideration and implementation in accordance with the Company's IT Risk Management framework.

**2. Identification of Information Technology-Related Risks**

The Company shall identify and assess information technology-related risks, including but not limited to the following:

- **Physical and Environmental Risks**
  Risks associated with the Data Center, server rooms, network equipment, and other critical IT facilities shall be appropriately managed through physical access controls, environmental monitoring, and security measures, including temperature monitoring systems, fire detection and suppression systems, and other relevant environmental controls.
- **Software and Endpoint Security Risks**
  Risks arising from the installation or use of unauthorized or insecure software on Company

computers shall be effectively controlled. Unauthorized software downloads or installations that may contain malware, computer viruses, or security vulnerabilities capable of compromising Company systems or networks shall be prohibited.

- **Network Security Risks**

  The Company shall continuously monitor and protect its internal network and Internet connectivity through appropriate security measures. These measures shall include, where appropriate, firewalls, anti-malware and antivirus solutions, Internet access controls, email security and filtering, intrusion prevention mechanisms, and other cybersecurity controls for servers, client devices, and network infrastructure.

- **Personnel and Access Risks**

  Access to computer systems, network devices, and information assets shall be granted strictly on the basis of business necessity and authorized responsibilities. Appropriate access controls shall be implemented to prevent unauthorized access, modification, or disclosure of information.

**3. IT Risk Assessment**

The Company shall conduct regular IT risk assessments by evaluating both the likelihood of occurrence and the potential business impact of identified risks in order to prioritize risk treatment activities.

IT risks shall, at a minimum, be classified into the following categories:

- **Technical Risks**, including cyberattacks or other threats affecting computer systems, applications, or network infrastructure.
- **Personnel Risks**, arising from inappropriate user access management or excessive access privileges that may result in unauthorized access to or misuse of information.
- **Disaster and Emergency Risks**, including natural disasters, utility failures, power outages, civil unrest, or other emergency situations that may affect the Company's information systems or business operations.
- **Management Risks**, arising from policies, procedures, or management practices that are no longer adequate or aligned with the Company's evolving risk environment.

**4. IT Risk Treatment**

The Company shall establish appropriate methods, controls, and tools to manage IT risks within the Company's acceptable risk tolerance.

Risk management documentation shall include, at a minimum, a **Risk Register** containing the risk description, risk category, risk characteristics, risk factors, potential impacts, and proposed risk treatment measures.

The Company shall also establish criteria for assessing the likelihood and impact of identified risks and maintain a **Risk Matrix (Risk Map)** to support risk analysis, prioritization, and decision-making.

**5. Information Technology Risk Indicators**

The Company shall establish appropriate **Information Technology Risk Indicators (IT Risk Indicators or KRIs)** to monitor significant IT risks.

Risk indicators shall be monitored on a regular basis, and the results shall be reported to the responsible management and relevant governance bodies to enable timely decision-making, effective risk mitigation, and continuous improvement of the Company's IT Risk Management processes.

primo
SERVICE SOLUTIONS
PUBLIC COMPANY LIMITED

## Chapter 2

## Information Technology Security (IT Security)

### Supplementary Guidelines on the Information Security Policy

### 1. Objective

To establish additional security requirements and user responsibilities in order to prevent violations of the Company's Information Security Policy and to ensure the secure, appropriate, and lawful use of the Company's information technology resources.

### 2. Guidelines

Users shall comply with the following requirements:

- Company information technology resources, computer systems, and network infrastructure shall not be used for any unlawful activities or activities contrary to public order or good morals, including the creation of websites or the distribution of content for illegal purposes or other inappropriate activities.
- Users shall not access the Company's computer systems or network using another person's user account, whether or not permission has been granted by the account owner.
- Users shall not gain unauthorized access to computer systems or protected information belonging to other persons for the purpose of modifying, deleting, adding, copying, or otherwise manipulating such information.
- Users shall not disclose, publish, distribute, or otherwise release information belonging to other individuals, the Company, or any organizational unit without prior authorization from the information owner.
- Users shall not interfere with, disrupt, damage, or attempt to compromise the Company's information technology resources or network infrastructure. This includes, but is not limited to, introducing malware or computer viruses, launching **Denial-of-Service (DoS)** attacks, or

performing any activity intended to disrupt the normal operation of computer systems or network services.

- Users shall not intercept, monitor, capture, or access data transmitted over the Company's network or any other computer network without proper authorization.
- Before using any removable storage media or opening e-mail attachments or files downloaded from the Internet, users shall ensure that such media or files have been scanned using approved anti-malware or antivirus software.
- Users shall keep their user accounts and passwords confidential and shall not permit any other person to use their credentials to access the Company's computer systems, network infrastructure, or information systems.

**Organization of Information Security**

**1. Objective**

To establish an information security governance framework that defines the roles, responsibilities, and management structure for protecting the Company's information systems and information assets.

**2. Guidelines**

- **Senior Management** shall be responsible for overseeing and ensuring that information security is managed in accordance with the Company's Information Security Policy and related procedures.
- The **Manager of the Information Technology Department** shall assign appropriate responsibilities to Information Technology personnel for the administration, operation, and protection of the Company's information systems. The Manager shall also supervise and monitor IT operations to ensure continued compliance with the Company's Information Security Policy and related security procedures.
- The **Manager of the Information Technology Department** shall be responsible for the overall governance, management, monitoring, and periodic review of the Company's Information Security Policy and information security management framework.

- Information Technology personnel assigned as **System Administrators** shall be responsible for maintaining the security of the information systems under their administration. They shall continuously monitor system security, promptly respond to any information security incidents or other unexpected security events, implement appropriate corrective actions, and report such incidents to their immediate supervisor without undue delay.
- All users, as well as internal and external organizations authorized to access the Company's information systems, shall comply with the Company's Information Security Policy and related procedures. They shall also comply with all applicable laws and regulations relating to information security and computer-related offences and shall refrain from any activities that may compromise the confidentiality, integrity, or availability of the Company's information systems or information assets.

**Human Resource Security**

**1. Objective**

To ensure that all users understand their roles, responsibilities, and obligations regarding the secure use of the Company's information systems and information assets throughout the employment or contractual relationship.

**2. Guidelines**

- The Company shall define, document, and communicate information security roles and responsibilities for employees, contractors, consultants, and external service providers. Such responsibilities shall be consistent with the Company's Information Security Policy and related procedures.
- All employees and external personnel engaged by the Company shall sign a **Non-Disclosure Agreement (NDA)** or be bound by equivalent confidentiality obligations before being granted access to the Company's information or information systems. Such confidentiality obligations shall remain effective throughout the period of employment or engagement and continue for **at**

**least one (1) year** after the termination of employment or contractual engagement, unless otherwise required by applicable law or contractual agreement.

- To ensure that user accounts are managed accurately and remain up to date, the **Human Resources Department** or the relevant responsible department shall promptly notify the **Manager of the Information Technology Department** whenever any of the following events occur:
    - Recruitment or appointment of personnel;
    - Changes in employment status or contractual engagement;
    - Resignation, termination of employment, or cessation of service as a director or employee of the Company; or
    - Transfer to another department or change of job responsibilities.
- All users and external personnel engaged by the Company shall acknowledge and comply with the Company's Information Security Policy and all related information security requirements before being granted access to the Company's information systems.
- Newly appointed employees shall receive information security awareness training as part of the Company's orientation or onboarding program to ensure that they understand their information security responsibilities before accessing the Company's information systems.
- Upon resignation, termination of employment, completion of a contractual engagement, or the conclusion of a project, all user access rights to the Company's information systems and information assets shall be revoked or adjusted immediately, as appropriate, in accordance with the Company's access control procedures.

**Asset Management**

**Computer and Peripheral Usage Control**

**1. Objective**

To ensure that users understand their roles and responsibilities regarding the use of the Company's computers and peripheral devices, and to promote the proper protection of the Company's information assets so that they remain secure, accurate, and available for business operations at all times.

**2. Guidelines**

- Users assigned Company computers or peripheral devices shall be responsible for the proper use, care, and protection of such assets throughout the period of assignment.
- Company computers, peripheral devices, networks, and information technology resources shall not be used for personal commercial activities, private business operations, or any other inappropriate purposes unrelated to the Company's business.
- Users shall not install, modify, remove, or configure any software on Company computers unless authorized by the System Administrator or approved by the head of the relevant department.
- Users shall not alter, modify, dismantle, or replace any hardware components or peripheral devices without prior approval from the System Administrator or the responsible department. All equipment shall be maintained in its original condition, except where authorized modifications have been approved.
- Users shall store and operate computer equipment in suitable environments and shall protect such equipment from excessive heat, humidity, dust, impact, or other conditions that may cause damage.
- Computer equipment shall not be placed or operated near liquids, strong magnetic fields, high-voltage electrical equipment, excessive vibration, or environments where the ambient temperature exceeds **37°C**.
- Users shall exercise due care when transporting computer equipment and shall avoid dropping, striking, or placing heavy objects on such equipment.
- Computer equipment shall not be moved while the hard disk drive is operating or while the device is powered on, unless the equipment is specifically designed to support such movement.
- Computer monitors and display screens shall be handled with care. Users shall avoid contact with sharp or hard objects that may scratch or damage the display and shall clean screens gently using appropriate materials and cleaning methods.

- Upon resignation, termination of employment, completion of a temporary assignment, or the expiration of a borrowing period, users shall return all Company computers, peripheral devices, and related equipment under their responsibility to the designated responsible department in good working condition, subject to normal wear and tear.
- Users who remove Company computer equipment from Company premises for business purposes shall comply with the Company's procedures governing the removal of Company property from Company premises.
- Users shall take appropriate precautions to prevent the loss, theft, or unauthorized access to Company computer equipment. Computer equipment shall not be left unattended in public places or other locations where there is a significant risk of loss or theft.

**Software License Management**

**1. Objective**

To ensure that all users understand their roles and responsibilities regarding the lawful, secure, and appropriate use of computer software, including compliance with software licensing requirements, the Company's Information Security Policy, the Computer Crime Act, and other applicable laws and regulations.

**2. Guidelines**

*Responsibilities of the System Administrator*

The System Administrator shall:

- Be responsible for managing, controlling, and administering the use of software within the Company in accordance with the applicable software licensing terms and authorized user entitlements.
- Be responsible for installing, configuring, updating, upgrading, and maintaining software for users according to approved schedules and operational requirements.

- Promptly revoke, remove, or reassign software licenses upon notification by the Company or the relevant department of the cancellation, reassignment, or termination of software usage rights.

*Responsibilities of Users*

Users shall:

- Use all software with due care and responsibility as if it were their own property, and shall not use any software for unlawful purposes or in any manner that infringes the rights of others or causes damage to the Company.
- Use only software that has been legally acquired and properly licensed by the Company. Users shall not copy, duplicate, modify, distribute, transfer, or install Company-licensed software on any unauthorized device or make such software available to any third party without prior authorization.
- Not reproduce, distribute, publish, or otherwise use pirated or unauthorized software, copyrighted software without permission, or unauthorized software code, particularly where such software may be used to facilitate unlawful activities.
- Not install or use any unauthorized software on Company-owned computers or information systems. Where users request to use software that is not provided by the Company, whether licensed software, freeware, or open-source software, such software shall not be installed or used without prior approval from the Company. Users shall be responsible for any loss, damage, security incident, or legal liability arising from the unauthorized installation or use of such software.
- Submit requests for the installation, removal, transfer, reallocation, or return of software licenses or Company computers through the Company's established approval process. The System Administrator shall implement such requests only after obtaining the required authorization from the designated approving authority.

**Information Asset and Computer System Access Control**

**1. Objective**

To protect the Company's information assets from unauthorized access, disclosure, alteration, loss, or misuse, and to ensure that computer systems and information resources are accessed only by authorized users in accordance with the Company's Information Security Policy.

**2. Guidelines**

The Company shall implement appropriate controls to ensure that information assets, including documents, storage media, computer equipment, and information, are protected from unauthorized access whenever they are unattended. Users shall also ensure that information systems are properly secured when not in active use by complying with the following requirements:

- Users shall **log out** of information systems immediately upon completion of their work or whenever access to the system is no longer required.
- Access to Company computers and information systems shall be protected through appropriate authentication mechanisms before use.
- Critical business information shall be securely stored and regularly backed up in accordance with the Company's data protection and backup procedures.

  Information may be stored only in the following approved locations:

  - Within the databases of authorized business applications hosted in the Company's Data Center. Data stored within such applications shall not be exported unless expressly authorized by the Company.
  - Within authorized shared network drives (Shared Drives) and only in folders for which the user has been granted appropriate access rights.

- Users shall shut down their computers whenever they will be unattended for more than **one (1) hour** or at the end of the working day, except for servers or other designated systems that are required to operate continuously on a 24-hour basis.
- Computers shall be configured to activate an automatic **screen lock** after no more than **10 minutes** of inactivity, requiring user authentication before access can be resumed.
- Any removal of information assets, including documents, storage media, computer equipment, or other information technology assets, from Company premises shall require prior approval from the Head of Department or a higher authorized authority and shall comply with the Company's procedures governing the removal of Company property.
- Users shall exercise due care in safeguarding all Company assets under their responsibility and shall treat such assets with the same level of care as their own property. Any loss or damage resulting from negligence may result in the user being held responsible for the associated damages in accordance with the Company's policies and applicable laws.

**Electronic Mail (E-mail) Usage**

**1. Objective**

To ensure that the Company's electronic mail (e-mail) system is used as an effective, secure, and reliable communication channel in support of business operations while complying with applicable laws, regulations, internal policies, and information security requirements.

This policy also aims to promote users' awareness of the risks associated with the use of Internet-based e-mail services. Users are required to understand and comply with the rules and security measures established by the Company and the System Administrator and shall refrain from any activities that may compromise the security, integrity, or proper operation of the Company's e-mail system.

**2. Guidelines**

- Users shall comply with the Computer Crime Act, the Electronic Transactions Act, all other applicable laws and regulations, and the Company's Information Technology and Information Security policies when using the Company's e-mail system.
- The Company's e-mail service shall be used primarily for legitimate business purposes and activities related to the Company's operations.
- E-mail accounts shall be created and managed by the System Administrator based on personnel information provided by the Human Resources Department.
- Users shall not access, read, send, or receive e-mail by using another person's e-mail account without the account owner's authorization. Each user shall remain responsible for all activities conducted through their assigned e-mail account.
- Users shall not impersonate another person, falsify the sender's identity, or otherwise misrepresent the origin of any e-mail communication.
- Official communications conducted on behalf of the Company shall be transmitted only through the Company's authorized e-mail system. The use of personal or external e-mail services for official business is prohibited unless the Company's e-mail system is unavailable and prior approval has been obtained from the user's supervisor.
- Users shall communicate professionally and courteously and shall not send messages that are offensive, defamatory, misleading, discriminatory, unlawful, or contrary to public order or good morals. Users shall not present personal opinions as official Company positions or engage in communications that may damage the Company's reputation.
- Users shall not use the Company's e-mail system to distribute or transmit information, messages, images, or other content that is illegal, inappropriate, offensive, defamatory, harmful to national security, disrespectful of the monarchy, or otherwise detrimental to the Company's operations or disruptive to other users.
- Company e-mail addresses shall not be used for personal commercial activities or for registering personal accounts on social media platforms, online services, or other non-business-related applications. Users shall be responsible for any consequences arising from unauthorized use of their Company e-mail accounts.

- Users shall not engage in activities that consume excessive system resources or disrupt normal e-mail operations, including but not limited to sending chain letters, spam e-mails, e-mail bombing attacks, or e-mails containing malware, malicious code, or computer viruses.
- Confidential Company information shall not be transmitted to unauthorized persons or organizations. Where confidential information must be transmitted by e-mail, appropriate encryption or other approved security measures shall be applied. The subject line should not disclose or indicate the confidential nature of the information.
- Where complaints, legal requests, suspected violations, or other inappropriate activities are identified, the Company reserves the right to suspend or revoke a user's e-mail access temporarily while conducting an investigation, in accordance with applicable laws and Company policies.
- Users who become aware of inappropriate conduct, suspected security incidents, or violations of this Policy shall promptly report such matters through the Company's designated whistleblowing or reporting channels.
- Users shall be solely responsible for all content that they create, publish, transmit, or distribute through the Company's e-mail system or any personal web pages under their control. The System Administrator and the Company shall not be responsible for content created or disseminated by users beyond their administrative responsibilities.

**Access Control**

**Corporate Network Usage**

**1. Objective**

To establish security measures governing access to the Company's information systems and the use of the Company's network and Internet services, ensuring that such resources are used efficiently, securely, and in accordance with applicable laws, regulations, and the Company's Information Security Policy.

This policy also aims to promote users' awareness of the risks associated with Internet usage and to ensure that access to websites and online resources is conducted responsibly and securely.

**2. Guidelines**

- The Information Technology Department shall establish secure network connectivity for Internet access through appropriate security controls, including, but not limited to, firewalls, proxy servers, secure gateways, or other approved network security solutions.
- All Company computers shall be equipped with approved anti-malware or antivirus software and shall have the latest security patches and operating system updates installed before connecting to the Company's network.
- Users shall close all web browsers and terminate Internet sessions after completing their work to prevent unauthorized access by other persons.
- Users shall access information systems, network resources, and information only to the extent authorized by their assigned roles and responsibilities, in accordance with the principle of least privilege and the Company's access control requirements.
- Users shall not disclose confidential or sensitive Company information except through officially authorized disclosure procedures and in accordance with the Company's information classification and disclosure requirements.
- Users shall exercise due care when downloading software, updates, files, or other content from the Internet. All downloads shall comply with applicable copyright laws, intellectual property rights, and the Company's software management requirements.
- Users shall verify the accuracy, integrity, and reliability of information obtained from the Internet before using or relying upon such information for business purposes.
- The Company's Internet services shall not be used for personal commercial activities or for accessing websites containing illegal, inappropriate, offensive, obscene, or harmful content, including content that violates public order, national security, religious harmony, respect for the monarchy, or other applicable laws and regulations.
- Users shall use the Company's Internet services responsibly and shall not infringe upon the rights of others, compromise the security of the Company's information systems, or engage in any activity that may cause damage to the Company. Users shall strictly comply with the Computer

Crime Act, other applicable laws and regulations, and all Company policies and procedures governing the use of Internet and network resources.

**Cryptographic Control**

**1. Objective**

To prevent unauthorized persons from accessing, obtaining, modifying, or altering information or the operation of information systems beyond their authorized duties and responsibilities.

**2. Guidelines**

• *Information Management*

- Information shall be classified according to its confidentiality level, business purpose, and importance. Appropriate management procedures shall be established for each classification, including procedures for handling confidential or critical information prior to disposal or reuse.
- **Information Classification**

  As information varies in nature and may have different levels of impact on the Company's operations, the Company classifies information into the following four levels:

  **Level 1 – Public Information**

  Information that may be disclosed and distributed to the public through the Company's official communication channels, such as the Company's website, applications, annual reports, financial statements, or other publicly available materials. Such disclosure shall be made for the benefit of the Company and/or in accordance with applicable laws, regulations, or requirements of relevant regulatory authorities.

  **Level 2 – Internal Use**

Information intended solely for internal use within the Company. Unauthorized disclosure of such information may adversely affect the Company's operations or cause damage to the Company. Examples include internal regulations, policies, operating manuals, internal announcements, and similar documents.

Access to this information shall be restricted from external parties unless disclosure is required by law, administrative order, and/or has received prior written approval from the head of the relevant department and/or the owner of the information.

**Level 3 – Confidential Information**

Information designated as confidential and accessible only to specifically authorized individuals as determined by the relevant business unit and/or information owner. Access and disclosure shall require prior written authorization from the head of the relevant department and/or the information owner.

This category includes information that may have a material impact on the Company's business and whose unauthorized disclosure could result in significant damage to the Company, including but not limited to:

- Customers' personal data;
- Personal data of employees, executives, directors, and stakeholders;
- Business plans;
- Marketing plans;
- Land acquisition plans;
- Approved sales promotion programs that have not yet been officially announced.

Such information shall be protected against unauthorized access by both internal and external parties. Where disclosure is required by law, prior written approval from the Chief Executive Officer (CEO) shall be obtained before any Level 3 information is disclosed.

**Level 4 – Top Secret Information**

Information of the highest level of confidentiality, accessible only to senior executives due to its strategic importance to the Company's operations, decision-making, and future business direction.

Unauthorized disclosure of such information may seriously impair the Company's competitive advantage or result in substantial financial losses. Examples include:

- Business expansion plans;
- Investment plans;
- Projects under development;
- Trade secrets;
- Corporate strategic plans.

Top Secret information shall receive the highest level of protection against unauthorized access by both internal and external parties. Where disclosure is required by law, prior written approval from the Chairman of the Board of Directors shall be obtained before any Level 4 information is disclosed.

- Confidential information transmitted through public networks shall be protected using internationally recognized encryption standards, such as **SSL (Secure Socket Layer)**, **VPN (Virtual Private Network)**, or equivalent encryption technologies.
- Appropriate controls shall be implemented to ensure the accuracy and integrity of information during storage, input, processing, and output. Where identical or related datasets are stored across multiple locations or distributed databases, appropriate measures shall be established to maintain data consistency, completeness, and accuracy.
- Appropriate safeguards should be implemented to protect information when computer equipment is removed from the Company's premises, such as for maintenance or repair. Where appropriate, information stored on storage media shall be securely erased or destroyed prior to such removal.

• ***User Privilege Control***

- Access to information and data processing equipment shall be controlled with due consideration to operational requirements and information security. Rules and procedures governing access authorization shall be established. User privileges shall be clearly defined to ensure that all users at every level are aware of, understand, and strictly comply with the established guidelines, and recognize the importance of information security.
- Access rights to information and information systems (e.g., application systems, internet access, and other related systems) shall be assigned based on job roles and responsibilities. Users shall be granted the minimum level of access necessary to perform their duties. Such access rights must be approved in writing by authorized personnel and shall be reviewed periodically.
- In cases where privileged user accounts are required, strict access controls shall be implemented. The assessment of adequate control for privileged users shall be based on the following considerations:
    - Approval must be obtained from authorized personnel, and the use of privileged accounts shall be strictly controlled and limited to necessary purposes only.
    - The usage period shall be defined, and access shall be immediately revoked upon expiration of the approved period.
    - Passwords shall be managed under strict controls, such as mandatory changes upon completion of use, or at least every six (6) months in cases of prolonged necessity.
- When a user is not actively operating a computer, appropriate safeguards shall be implemented to prevent unauthorized access, such as requiring users to log out of systems when leaving their workstation.
- Where it is necessary for data owners to grant other users access to or modification rights over their information (e.g., file sharing), such access shall be granted only on a case-by-case or group basis. All such permissions must be formally documented, time-bound, and revoked immediately when no longer required.
- In cases where temporary or emergency access to information systems or network resources is required, formal procedures shall be established. Such access must be approved by authorized personnel each time, with documented justification and defined usage periods. Access rights shall be revoked immediately upon expiration of the approved period.

• ***User Account and Password Control***

- A robust **Identification and Authentication** mechanism shall be implemented to verify user identity and access rights prior to system login. Passwords shall be designed to be sufficiently complex and difficult to guess. Each user shall be assigned a unique **User Account**.

  The Company shall consider the following factors in determining whether password controls are sufficiently strong and secure:

  - Passwords should have an adequate length. International standards generally recommend a minimum of **8 characters**, consisting of alphabetic and numeric characters.
  - Passwords should include a combination of uppercase letters, lowercase letters, numbers, and special characters such as : ; < > $ @ #, etc.
  - For general users, passwords shall be changed at least every **80 days**. For privileged users, such as System Administrators and default system accounts, passwords shall be changed at least every **60 days**.
  - New passwords must not be the same as any of the previous **10 passwords** used.
  - Passwords shall not follow predictable patterns or be easy to guess, such as “abcdef”, “aaaaaa”, “123456”, “password”, or “Password”, etc. Passwords shall not be related to personal information such as names, surnames, dates of birth, or addresses.
  - Passwords shall not consist of dictionary words.
  - The number of allowed failed login attempts shall generally be limited to **three (3) attempts**. If the limit is exceeded, the system shall deny access or temporarily suspend the account.
  - Passwords shall be delivered to users through secure and controlled methods, such as sealed envelopes.
  - Users receiving a default password or newly issued password shall be required to change it immediately upon first login.

  - Users shall keep their passwords strictly confidential and must not write them down or display them in visible locations. If a password is suspected of being compromised, it shall be changed immediately.
  - In cases of shared user licenses (e.g., SAP systems), system administrators shall notify responsible users via email to change passwords whenever there are changes in assigned personnel.
- Password files shall be protected using **encryption mechanisms** to prevent unauthorized disclosure, modification, or compromise.
- User accounts for critical systems shall be reviewed regularly. Accounts that are no longer authorized, such as those belonging to resigned employees or default system accounts, shall be promptly disabled or removed. Actions may include disabling the account, deleting it from the system, or resetting the password immediately upon detection.

**Physical and Environmental Security (Information Security)**

**1. Objective**

The objective of controlling access to the Data Center Room is to prevent unauthorized individuals from accessing, viewing, modifying, or causing damage to information and computer systems. In addition, damage prevention aims to protect information and computer systems from environmental risks or various disasters. This section covers access control guidelines for the Data Center Room and the environmental protection systems that the Company should implement within the Data Center.

**2. Guidelines**

• *Data Center Room Access Control*

- Critical IT equipment such as servers and network devices must be installed in the Data Center Room or other restricted areas. Access rights to the Data Center Room must be strictly limited to authorized personnel only, such as system administrators or designated IT staff.

- In cases where non-authorized personnel are required to enter the Data Center Room occasionally, strict control measures must be applied. For example, such access must be supervised at all times by system administrators and/or responsible personnel.
- An access log system must be implemented to record entry and exit of the Data Center Room, including user identity and timestamp. These logs should be reviewed regularly.
- The Data Center Room should be clearly organized into zones, such as:
    - Network Zone
    - Server Zone
    - UPS Zone
    - Battery UPS Zone

    to improve operational efficiency and enhance control over critical equipment access.

• *Damage Prevention Systems*

**Fire Protection System**

- Fire detection equipment such as smoke detectors and heat detectors must be installed to enable early detection and response.
- The main Data Center Room must be equipped with an automatic fire suppression system. The disaster recovery or backup site must at least be equipped with fire extinguishers for initial response.

**Power Failure Protection**

- Systems must be in place to protect computer equipment from electrical instability.
- An Uninterruptible Power Supply (UPS) and automatic voltage regulation system must be provided for critical systems and network infrastructure to ensure business continuity.
- Users must promptly save any ongoing work and safely shut down computers and related devices during power instability or outages.

**Temperature and Humidity Control**

- Environmental conditions must be maintained at appropriate temperature and humidity levels. Air conditioning systems must be configured according to the technical specifications of IT equipment, as improper conditions may cause system malfunction.

**Water Leak Detection System**

- Where raised flooring is used for cabling and air-conditioning systems, water leak detection systems should be installed in areas with water piping to ensure early detection and prevention of leaks.
- If the Data Center Room is located in a high-risk flood or leakage area, regular inspection for water leakage must be conducted.

**Operations Security**

**1. Objective**

To ensure that the Company's information systems are operated accurately, securely, and efficiently, preventing data loss and protecting systems from malware and other malicious software.

**2. Guidelines**

- Document operating procedures or standard operating manuals for critical information systems to minimize operational errors.
- Implement change management controls for information systems, requiring appropriate management approval before any system changes are made.
- Perform data backups prior to implementing any changes to information systems.
- Monitor information system resources, including CPU, memory, and storage capacity, to ensure adequate performance and support future capacity planning.
- For critical systems, maintain separate development, testing, and production environments to prevent unauthorized or unintended changes to live systems.

- Identify and classify information according to its criticality, define backup requirements, and establish appropriate backup frequencies.
- Critical information must be backed up more frequently and, where appropriate, copies should be stored securely at an off-site location.
- Test the availability and effectiveness of backup and recovery systems at least once annually.
- Implement measures to protect information systems from malware and malicious software, including:
    - All desktop computers and laptops must have approved antivirus software installed and operating systems and web browsers patched before connecting to the Company's network.
    - Users must regularly update operating systems and application software using official updates provided by the software vendor to address known security vulnerabilities.
    - All files transmitted via email must be scanned for malware using approved antivirus software before being opened or transmitted.
    - Users may install only software approved and provided by the Company. Any additional software installation must receive prior security review and approval from the Information Technology Department.
    - Network administrators must continuously monitor network traffic and system usage to detect abnormal traffic volumes or unusual access patterns, investigate potential causes, and implement appropriate preventive measures.

**Communications Security**

**1. Objective**

To protect information within network communication systems from unauthorized access, viruses, and malicious code that may compromise data confidentiality, integrity, or system availability.

**2. Guidelines**

**2.1 Network Security Management**

- Network access controls must be defined and implemented to ensure secure access to the Company's network systems.
- The network must be segmented to separate internal users from external parties connecting to the Company's systems, in order to reduce security risks and prevent unauthorized access.

**2.2 Information Transfer**

- Information transfer activities must be governed by formal agreements (Agreements on Information Transfer), taking into account information security requirements.
- System administrators must oversee and control such activities to ensure security in terms of:
    - **Confidentiality** (prevention of unauthorized disclosure)
    - **Integrity** (accuracy and completeness of data)
    - **Availability** (accessibility when required)
- A Non-Disclosure Agreement (NDA) must be signed between the Company and external parties prior to any exchange or transfer of confidential information, in order to ensure that company information is not disclosed without authorization.

**System Acquisition, Development and Maintenance**

**1. Objective**

To ensure that information systems developed or modified operate accurately, completely, and in accordance with user requirements, thereby reducing **integrity risk**. This covers the entire lifecycle of system changes, from request initiation through development, testing, and deployment into production.

**2. Guidelines**

**2.1 System Development and Change Management Procedures**

- A documented procedure must be established for system development and modification. At a minimum, it should cover:

  - Change request process
  - Development or modification process
  - Testing process
  - System migration / deployment process
- Emergency changes must be supported by a defined procedure, including documented justification and prior approval from authorized personnel.
- Procedures must be communicated to all relevant users and enforced consistently.

**2.2 System Change Control**

*Change Request*

- All requests for system development or modification must be documented (including electronic formats such as email) and approved by authorized personnel (e.g., department head or IT system owner).
- Impact assessments must be conducted and documented, covering:
  - Operations impact
  - Security impact
  - System functionality impact
- Regulatory and compliance implications must also be reviewed before implementing changes.

*Development Environment Control*

- Development environment must be strictly separated from the production environment.
- Access to each environment must be restricted to authorized personnel only.
- The separation may be implemented using either:
  - Different physical machines, or
  - Segmented environments within the same system.
- Requesters and relevant users should participate in development to ensure alignment with business requirements.
- Security and system availability must be considered from the initial design phase.

*Testing Process*

- Testing must involve requesters, IT personnel, and relevant users to ensure that the system functions correctly, completely, and meets requirements before production deployment.

*System Migration / Deployment*

- System deployment to production must be verified to ensure completeness and accuracy.

*Documentation and Version Control*

- Documentation of system development history must be maintained, including details of all modifications and versions.
- All system documentation must be updated after any change, including:
    - System architecture documents
    - User manuals
    - Data structure documentation
    - Access control lists
    - Program specifications
- Documentation must be securely stored and easily accessible when needed.
- Previous software versions must be retained for rollback in case of failure.

*Post-Implementation Testing*

- Post-implementation testing should be conducted after the system has been in use for a period of time to ensure continued performance, accuracy, and compliance with user requirements.

*Change Communication*

- All system changes must be communicated to relevant users to ensure proper understanding and correct usage of the updated system.

**IT Outsourcing (Use of Information Systems Services from Service Providers)**

**1. Objective**

To protect the Company's assets accessed by IT outsourcing providers and to ensure that the required level of information security and service quality is maintained in accordance with agreed service level agreements (SLAs).

**2. Guidelines**

- Security requirements for Company data must be clearly defined when IT outsourcing providers are granted access to Company information or assets. These requirements must align with the Company's confidentiality policies.
- Security requirements must be communicated, enforced, and acknowledged by the outsourcing provider before access to systems or data is granted.
- Service agreements must include provisions for regular monitoring, review, and audit of outsourced services to ensure compliance with agreed standards.
- Any changes to service agreements related to critical systems must undergo a formal information security risk assessment prior to implementation.

**Information Security Incident Management**

**1. Objective**

To establish a consistent and effective approach for managing information security incidents, including reporting security events and identifying information system vulnerabilities in a timely manner.

**2. Guidelines**

- Responsibilities and procedures must be clearly defined for responding to information security incidents affecting the Company's systems and operations.

- Communication channels must be clearly established for reporting information security events and incidents.
- Users who detect any event that may impact information security must immediately report it to the Information Technology Department.
- Incident reporting must be categorized according to severity levels. In cases where incidents have a significant impact on a large number of users, immediate notification or announcement must be made.
- All information security incidents must be properly recorded, including at minimum:
    - Type of incident
    - Frequency or scale of occurrence
    - Associated costs or damages

      This is to support analysis, lessons learned, and preventive improvements.
- Evidence related to security incidents must be collected and securely stored in accordance with applicable legal and regulatory requirements to support potential legal proceedings.

**Information Security Aspects of Business Continuity Management**

**1. Objective**

To prevent disruption of the Company's operations caused by crises or disasters, and to ensure the availability and readiness of the Company's information systems and supporting IT infrastructure.

**2. Guidelines**

- The Information Technology Department must establish a contingency plan to address uncertainty, crises, and disasters that may affect information systems, in alignment with the Company's Crisis Management Plan.
- Information system risks must be assessed and reviewed at least once per year.
- The Business Continuity and emergency preparedness plans must be reviewed at least once per year to ensure their effectiveness and relevance.

- The readiness and availability of backup systems must be tested at least once per year to ensure continuity of critical operations.

**Effective Date:** This policy shall be effective from 26 July 2022 onwards.

| | |
|---|---|
| Ms. Jatuporn Vilaikaew<br>Chief Executive Officer<br>Primo Service Solutions Public Company Limited | Mr. Maroj Wananan<br>Chairman of the Audit Committee<br>Primo Service Solutions Public Company Limited |

**PRIMO SERVICE SOLUTIONS PUBLIC COMPANY LIMITED**
496 Moo 9 Sukhumvit 107 Road, Samrong Nuea,
Muang Samut Prakarn District, Samut Prakarn 10270
**T** 02 081 0000 **E** info@primo.co.th
WWW.PRIMO.CO.TH