PRTR

PRTR Group Public Company Limited and its subsidiaries.

Policy used of Information Technology.

This Information Technology (IT) Usage Policy is the copyright of PRTR Group Public Company Limited (the 'Company'). It is established with a commitment to developing a corporate governance system that aligns with the principles of good corporate governance, best practices, as well as the laws, regulations, and requirements prescribed by official authorities and regulatory bodies.

The Board of Directors approved this Information Technology (IT) Usage Policy at Meeting No. 2/2024 on February 27, 2024, to serve as the fundamental principle and operational guideline for executives, employees, and relevant parties of the Company and its subsidiaries, effective from March 1, 2024, onwards.

To ensure that the Information Technology (IT) Usage Policy remains current and appropriate to prevailing situations and changes, a mandatory review of this Policy shall be conducted at least once a year. Any subsequent amendments or modifications must be strictly approved by the Board of Directors only.

(Mr. Niphon Bundechanan)

Acting Chairman of the Board of Directors.

Table of Contents

1. Introduction

PRTR Group Public Company Limited (the 'Company') prioritizes and exercises extreme caution regarding the utilization of the Company's information technology systems, which are vital resources and databases for its business operations. The Company is fully aware that any lack of due care or unauthorized use of these systems could result in significant damage to the Company and its relevant stakeholders. Consequently, the Company has established this Information Technology (IT) Usage Policy for executives, employees, and relevant parties to strictly adhere to.

2. Objectives

2.1 To establish a unified Information Technology (IT) Usage Policy for the Company, its subsidiaries, and its associates, ensuring consistent adherence across the entire organization.

2.2 To serve as a formal communication tool by providing a written Information Technology (IT) Usage Policy for the personnel of the Company, its subsidiaries, and its associates, fostering a clear and mutual understanding of established standards.

3. Scope

This policy applies to PRTR Group Public Company Limited, its subsidiaries, and its associates, encompassing the core principles, policies, and operational guidelines.

4. Policy on the use of information technology systems in the company

These corporate regulations are established to provide operational guidelines for the employees of PRTR Group Public Company Limited and its subsidiaries. The primary objective is to ensure that information within the IT systems remains secure and stable, adhering to the fundamental pillars of information security: Confidentiality, Integrity, and

Availability (CIA). Employees at all levels are required to prioritize and strictly comply with this Information Technology (IT) Usage Policy, as well as all other relevant corporate regulations.

Objectives

1. To mitigate potential risks arising from information system operations.
2. To ensure information systems remain secure and protected against inappropriate or incorrect utilization of information technology.
3. To serve as the formalized information technology operational framework for the Company.
4. To ensure full compliance with all laws, regulations, and statutory requirements pertaining to information technology.
5. To foster employee awareness regarding cyber threats and the importance of information technology security.
6. To ensure that all employees strictly adhere to corporate regulations and the Information Technology Department's policies.

Furthermore, all employees who utilize information systems must undergo mandatory training regarding this Information Technology (IT) Usage Policy, corporate regulations, and/or other relevant official announcements. All personnel are required to strictly comply with these established standards.

Penalties

Any employee found to be in violation of, or failing to comply with, the Information Technology Security Policy, including operational regulations pertaining to the use of Artificial Intelligence (AI) and the Company's intellectual property, shall be deemed to have committed a disciplinary offense in accordance with the Company's Work Rules and Regulations.

Furthermore, the Company reserves the right to determine disciplinary actions based on the severity of the circumstances, intent, and the magnitude of the resulting damages, without the necessity of following a progressive disciplinary sequence (from minor to major

penalties). Additionally, the Company shall pursue legal proceedings to the fullest extent of the law encompassing civil, criminal, and other relevant statutes (such as the Computer-Related Crime Act and the Personal Data Protection Act - PDPA) against any offending employee until the matter reaches its final legal conclusion.

Chapter 1: Compliance with Corporate Regulations, Laws/Statutes, and Operational Guidelines

1.1 IT Personnel shall:

1) Prioritize information system threats and undergo mandatory training regarding the Company's Information Technology (IT) Usage Policy.
2) Strictly adhere to IT policies, various corporate regulations, and other security measures established by the Company, as well as all applicable domestic laws and statutory requirements.
3) Maintain and safeguard information within the Company's IT systems to ensure continuous availability and operational readiness at all times.
4) Educate employees and foster a strong culture of Cybersecurity awareness throughout the organization.

1.2 All employees, including employees of the Information Technology Department, musAll employees, including IT personnel, shall adhere to the following:

1) Prioritize the security of information systems and undergo mandatory training regarding the Company's IT Usage Policy, corporate regulations, and other relevant official announcements.
2) Regularly monitor announcements from the IT Department and strictly comply with all recommendations and the Company's IT Usage Policy.

3) Refrain from utilizing the Company's data and information systems in any manner that is inappropriate, defamatory, illegal, or inconsistent with corporate policies, IT regulations, and the Personal Data Protection Policy.
4) Employees are prohibited from storing personal data on the Company's information systems or electronic devices.
5) Employees must not disclose or disseminate information regarding system vulnerabilities or sensitive data to unauthorized persons without prior approval.
6) The Company reserves the right to record Log Files or computer traffic data in accordance with the Computer-Related Crime Act B.E. 2560 (2017).
7) Any employee failing to comply with corporate policies and regulations may face suspension of access or appropriate disciplinary actions.
8) Utilization of the Company's computer equipment, electronic devices, or information systems for non-work-related activities—such as gaming, gambling, social media, online shopping, or any actions that are illegal, immoral, or unethical is strictly prohibited.
9) Employees must not leave the Company's electronic devices, information, or documents unattended in public areas.
10) Maintain responsibility for Company assets as if they were one's own. In the event of loss or damage, employees must immediately notify their supervisor and the IT Department.
11) Employees shall not utilize Company information systems to commit, or support the commission of, any offense under the Computer-Related Crime Act B.E. 2560 (2017).
12) The Company does not support or permit any employee or relevant party to use its systems for illegal acts. Any violation is deemed a personal act, for which

the individual shall be held solely liable under the penalties prescribed by the Computer-Related Crime Act.

13) Employees must promptly report any system malfunctions or downtime to the IT Department.
14) Fully cooperate with the Company's IT personnel or auditors in the examination and monitoring of information system usage.
15) Employees, contractors, or authorized users must execute a Non-Disclosure Agreement (NDA) with the Company prior to accessing or receiving sensitive information.

Chapter 2: Responsibility Towards the Company's Information Assets

1) Employees utilizing information systems must not disclose any confidential or sensitive information of the Company to external parties or the public, except with explicit authorization from an authorized person.
2) Employees are prohibited from accessing, editing, or modifying information systems for which they have no access rights, authorization, or relevant job responsibilities.
3) All information systems and data used within the Company are considered Company property. Employees are strictly prohibited from utilizing such assets for personal gain.
4) Employees, contractors, or authorized users must execute a Non-Disclosure Agreement (NDA) or confidentiality statement with Executive Management and the IT Department prior to the delivery or receipt of sensitive information that could potentially damage the Company.
5) Employees are responsible for performing regular backups of essential Company data.
6) Employees must exercise due care and caution when handling all types of information documents and data.
7) Public dissemination of Company information must receive prior approval from the relevant data owner, authorized person, or Executive Management.
8) Employees are prohibited from storing personal data on the Company's information systems or electronic devices.

9) Disseminating information regarding system vulnerabilities or sensitive/confidential data to the public without authorization is strictly prohibited.
10) Employees must not leave the Company's electronic devices, information, or documents unattended in public areas.
11) Prior to reusing or disposing of storage media, employees must inspect the devices for sensitive Company data (e.g., confidential information or licensed software). All data must be erased or the media destroyed using proper methods before disposal.
12) Employees must not remove IT assets, including information or software, from the Company's premises without prior authorization from their supervisor or the system owner.
13) Employees must not disseminate information for personal benefit, or content that is immoral, infringes upon the rights of others, or could potentially damage the Company's reputation.
14) IT personnel or employees responsible for publishing Company information via the website or other channels must verify the accuracy of the content. The individual publisher shall be held liable for any errors, and such publishing must be performed only by authorized Company personnel.

Chapter 3: Connection of Computer Equipment and Electronic Devices to the Internal Network

1) Only computer equipment and electronic devices belonging to the Company are permitted to connect to its information systems. In cases where employees provide their own devices (BYOD), prior authorization from their respective department is mandatory, and such devices must strictly comply with all corporate regulations and the Information Technology (IT) Usage Policy.
2) All computer equipment and electronic devices connected to the internal network, whether personally owned or Company-provided, must have essential threat prevention software installed, such as anti-virus, anti-malware, personal firewalls, and personal intrusion prevention systems. Furthermore, such software must be consistently updated (signature and patch updates) to remain current.

3) Access to the Company's information systems must be validated through official employee authentication systems or protocols capable of verifying authorized users and their respective access rights.
4) The installation of malicious programs or the use of illegal software/application suites on any computer equipment or electronic devices connected to the Company's network is strictly prohibited.

Chapter 4: Copyright and Intellectual Property Infringement

1) All employees utilizing the Company's information resources must not infringe upon the privacy rights or the intellectual property of others.
2) The Company prioritizes copyright and intellectual property. Consequently, employees are permitted to use only licensed software provided by the Company. All employees are strictly prohibited from installing or utilizing any unauthorized or unlicensed software. Should any violation be detected, it shall be deemed the individual's personal offense, for which the employee shall be solely liable.
3) Software provided by the Company is considered an essential business tool. Employees are prohibited from uninstalling, modifying, or duplicating such software for external use without prior authorization. Any necessary actions regarding software or related components must receive prior approval from the IT Department or the respective department head.
4) Software licenses provided by the Company are restricted for use only on computer equipment and electronic devices issued by the Company. Exceptions are permitted only with the approval of the respective department head and prior notification to the IT Department. In such cases, the authorizing department shall remain responsible for the utilization of the software.
5) Employees must exercise due care when utilizing documents or data in any format. Where specific usage terms and conditions are defined, employees must strictly adhere to such requirements to avoid infringing upon the intellectual property of third parties.

Chapter 5: Password Responsibility

1) Passwords and electronic keys are considered Company property. It is the mandatory responsibility of every employee to safeguard these credentials.
2) Employees must maintain the strict confidentiality of their passwords and related security credentials. Disclosure of passwords to any third party is prohibited, and the sharing of passwords among employees is strictly forbidden without exception.
3) Employees must log off or activate an automatic screen lock (set to a duration not exceeding 5 minutes) whenever they are away from their computer workstation.
4) Passwords utilized for system communication over untrusted or unsecured networks must be encrypted at all times.

Chapter 6: Access Control for the Data Center and Utilization of IT Equipment

1) Entry and exit to the Data Center must be formally recorded, clearly specifying the time of access, full name, department, and the specific purpose of entry.
2) The utilization of information systems and relevant electronic devices shall be strictly limited to the Company's business operations. Utilizing Company assets for personal use is prohibited. It is the mandatory duty of every employee to safeguard information systems, related equipment, and other resources including data stored within those systems—against damage or unauthorized access by irrelevant parties.
3) Employees are prohibited from installing any unauthorized software onto the Company's computer equipment or electronic devices. Furthermore, employees should refrain from modifying software or operating system configurations. Should any such actions be necessary, prior notification and approval from the IT Department or the respective department head are required.
4) The integration of external devices, software suites, or data with the Company's network or information systems must receive prior approval from the respective department head and be reported to the IT Department. Individuals introducing such equipment must strictly adhere to all corporate regulations and the Company's Information Technology (IT) Usage Policy.

Chapter 7: Testing of Developed or Modified Systems

1) Any system modifications or developments initiated with the approval of the System Owner require the active participation of the System Owner in the testing and development process. Furthermore, a formal certification of the test results must be signed jointly by the relevant personnel and the system audit committee appointed by Executive Management.
2) Prior to the deployment of any internally developed systems including those acquired through procurement or outsourced development for corporate use a comprehensive vulnerability assessment must be conducted. This assessment shall encompass the operating system, database, applications, and software programs before official commencement of operations.

Chapter 8: Protection Against Malicious Software (Malware, Viruses, Worms, etc.)

1) All computer equipment and electronic devices provided by the Company are equipped with anti-malware software. Employees are strictly prohibited from disabling or terminating the operation of such software, except with explicit authorization from an authorized person.
2) Employees are responsible for ensuring that virus signatures and other malware detection databases are regularly updated. Furthermore, software vulnerabilities must be addressed through consistent patching of operating systems and other application suites, such as web browsers, to prevent potential security breaches and damages.
3) Employees must maintain continuous vigilance against malicious software. Any identified irregularities or suspicious activities must be reported to the IT Department or System Administrator immediately.
4) Upon discovering system malfunctions or suspecting a malware infection, employees must immediately cease all computer and network-related activities. The IT Department or System Administrator must be notified urgently to initiate proper mitigation procedures.

Chapter 9: Electronic Mail (E-mail) Usage

1) Electronic mail is the property of the Company, intended solely to enhance operational efficiency. Employees are prohibited from utilizing Company e-mail for personal matters or purposes beyond the Company's scope, including any fraudulent representation that may cause damage to the Company.
2) Employees must not disclose Company e-mail accounts to the public, such as posting on web forums, threads, or inappropriate websites.
3) The use of free e-mail services (e.g., Gmail, Hotmail, Yahoo) for transmitting Company information is strictly prohibited.
4) Electronic mail containing sensitive information must be transmitted in an encrypted format. Confidential files sent to external parties must be encrypted, and the file must be sent through a separate channel from its password.
5) Sending letters to related parties such as customers, contractual companies, company employees, etc. In case it is necessary to use information with personal content, use free e-mail services such as Gmail, Hotmail, Yahoo, etc.
6) The E-mail System Administrator (IT Department) reserves the right to block or remove inappropriate attachments or messages. This includes setting maximum file size limits for transmissions and restricting specific senders/recipients or attributes that may jeopardize the Company.
7) Employees must not forward chain e-mails, spam, or any correspondence intended for harassment or disruption.
8) Communication with stakeholders must clearly and accurately identify the sender. The use of aliases, anonymous identities, or mechanisms to hide/mask the sender's name in replies or originations is prohibited.
9) All data transmitted or received via e-mail systems to the Company's computers or storage media must be scanned for viruses or malicious software prior to access.
10) Accessing the e-mail system requires Multi-Factor Authentication (MFA) to enhance security measures.

Chapter 10: Remote Access Control to Information Systems

1) Employees requiring remote access to information systems must obtain prior authorization from their respective department and the IT Department. Access rights shall be granted strictly on a 'need-to-know' basis, limited only to the sections necessary for their specific job functions.
2) Remote access to information systems must be conducted through the Company's official authentication system via secure communication channels, such as Virtual Private Network (VPN) or Remote Desktop software that requires end-user acceptance. The IT Department reserves the right to monitor Log Files or computer traffic data of such access to track and investigate any irregularities.
3) Employees are prohibited from connecting information systems to external networks without the prior approval of the IT Department. In instances where an external connection is established without bypassing the Company's internal network, the employee must notify the IT Department or their direct supervisor.
4) Any interconnection between the internal corporate network and untrusted external networks must be executed through secure channels, such as VPN or secure protocols like SSL VPN, to ensure data integrity and security.

Chapter 11: Internet and Intranet Usage

1) The Internet and Intranet networks are the property of the Company and are permitted for use strictly for business purposes or activities relevant to the Company's operations.
2) The use of online streaming applications for movies, music, or multimedia content, as well as any other high-bandwidth applications that may cause network disruption or system failure, is strictly prohibited.
3) Employees are prohibited from utilizing Peer-to-Peer (P2 P) file-sharing software or similar high-risk applications (e.g., eMule or BitTorrent), except with explicit authorization from their respective department.
4) Employees must not utilize the Company's internet network for personal business gain or to access inappropriate websites, including those that are immoral, contain content contrary to the Nation, Religion, or the Monarchy, or are deemed socially harmful.

5) Internet access for external parties shall be provided via a one-time password (OTP) or guest credentials with a specified expiration period. All external users must undergo registration to ensure full auditability and traceability.

Chapter 12: Incident Response

1) Every employee is responsible for reporting identified threats and irregularities—such as security vulnerabilities, software weaknesses, malware propagation, or the unauthorized and improper use of information assets—to the IT Department or relevant authorities as expeditiously as possible to facilitate timely remediation.
2) Any employee who acquires or possesses information regarding information system vulnerabilities must immediately transmit such details to the IT Department or relevant parties for appropriate assessment and remedial action.

I f the event of malfunctions or downtime affecting systems, computer equipment, or peripheral devices, employees must promptly notify the IT Department. This ensures that the IT Department can initiate repairs and restore operational status as swiftly as possible.

Chapter 13: Generative AI Enforcement Policy

1) The input of confidential corporate information, financial data, customer information, passwords, source code, or Personally Identifiable Information (PII) into Generative AI systems is strictly prohibited. This measure is established to prevent unauthorized data processing or leakage to the public.
2) Infringement of copyrights and intellectual property is strictly forbidden. Employees must not use AI to generate content that copies or modifies the copyrighted works of others (e.g., articles, images, music) without authorization. Furthermore, utilizing personal data for model training without the explicit consent of the data subject is prohibited.
3) Prior to utilization, employees must ensure that AI system privacy settings are configured to the maximum level at all times. Mandatory configurations include: disabling commands that allow the system to learn from user data (Turn off Model

Training), utilizing temporary chat modes (Temporary Chat), and disabling memory storage systems (Turn off Memory).

4) Employees are responsible for verifying the accuracy of AI-generated information before practical application and shall be held liable for the outcomes as if they were the sole authors. The use of AI to generate false information or content that causes damage to the Company is strictly prohibited.
5) The utilization of AI must remain within the framework of Personal Data Protection laws (PDPA/GDPR) and international standards prescribed by the Company (e.g., ISO/IEC 23894). Employees are required to undergo mandatory AI security training as scheduled by the Company. Any data leaks or irregularities arising from AI usage must be reported immediately to a supervisor in accordance with the Incident Response procedures.

Chapter 14: Remote Technical Support and Screen Recording

1) The IT Department is authorized to access user workstations via designated remote support software (e.g., AnyDesk) for troubleshooting or system inspection purposes. Users must verify the request and explicitly click 'Accept' to authorize each connection session.
2) Remote connection sessions shall be recorded in video format to serve as operational evidence, prevent misconduct, and safeguard against unauthorized data access.
3) By accepting the remote connection, the user acknowledges and provides explicit consent for the recording of their screen and all associated activities, in full compliance with the Personal Data Protection Act (PDPA).
4) Recorded files shall be maintained in a secure, encrypted storage environment. Access to these recordings is strictly restricted to authorized personnel for auditing and investigative purposes only.
5) Employees are strictly prohibited from installing or utilizing any remote desktop software not officially approved by the Company. This measure is established to prevent potential security vulnerabilities and unauthorized breaches.

Chapter 15: Microsoft 365 Usage and Access Controls

1) Access to the Company's Microsoft 365 ecosystem (including E-mail, OneDrive, Teams, etc.) is strictly restricted to users within Thailand. This measure is established as a proactive defense against cross-border cyberattacks and unauthorized external access.
2) The system shall automatically block all connection attempts originating from international locations. Access will be denied by default unless a prior authorization request has been formally submitted and approved.
3) Employees required to perform duties abroad must submit an Exception Request to the IT Department in advance for temporary access approval. Such requests shall be evaluated on a case-by-case basis.

Employees granted temporary overseas access are mandated to utilize Multi-Factor Authentication (MFA) and may be required to connect via designated secure channels as specified by the Company to ensure maximum security integrity.

5. Revision History

No.	Operator	Review Date	Effective Date	Revision Details
0	Paphop Plapiriyakit	15 Feb 2024	1 Mar 2024	Documentation for the first time
1	Paphop Plapiriyakit	17 Apr 2025	15 May 2025	Review and update policies
2	Paphop Plapiriyakit	10 Feb 2026	26 Feb 2026	Review and update policies

Appendix: List of Companies Subject to This Policy

This policy applies to **PRTR Group Public Company Limited**, as well as its subsidiaries under its direct or indirect control.

The companies within the scope of this policy include the following:

1. PRTR Recruitment Company Limited
2. PRTR Recruitment and Outsourcing (Eastern Seaboard) Company Limited
3. Nexmove Platform Recruitment Company Limited
4. The Blacksmith Company Limited
5. Pinno Solutions Company Limited
6. PRTR Global Recruitment Company Limited
7. Biz Resource Company Limited

Remarks:

- Newly established subsidiaries or subsequent investments shall automatically fall within the scope of this policy, unless otherwise specified.
- For companies not under the Company's control, this policy may be adopted and applied as appropriate.

Additional Note: This appendix shall be deemed an integral part of this policy and shall have the same full force and effect as the main policy in all respects.