PRTR Group Public Company Limited and its subsidiaries.

IT Security Policy.

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

(Niphon Bundechanan)

Acting Chairman of the Board of Directors

Table of Contents

1. Introduction

To ensure that the information technology, network, and computer systems of PRTR Group Public Company Limited and its subsidiaries which utilize shared information systems and network infrastructures are operated appropriately, securely, and capable of supporting the Company's business operations continuously; to ensure that system utilization is correct and fully compliant with the Computer-Related Crime Act and other relevant laws; and to prevent threats that may result in damage to the Company, the Company hereby establishes this Information Technology (IT) Security Policy as follows:

2. Objectives

2.1 To establish an Information Security Policy that fosters confidence and ensures the security of the Company's information technology systems and computer networks, enabling operations to be conducted with maximum efficiency and effectiveness.

2.2 To define the scope of information technology security management and ensure continuous improvement and updates to the security framework.

2.3 To establish standards, operational guidelines, and procedures that ensure executives, employees, system administrators, and third-party contractors are aware of the critical importance of information security in business operations and strictly adhere to established protocols.

2.4 This Policy shall undergo a mandatory formal review, audit, and evaluation at least once (1) per year to ensure its ongoing relevance and adequacy.

2.5 To serve as a formal communication tool by providing a written Computer and Information Technology Usage Policy for the personnel of the Company, its subsidiaries, and its associates, thereby fostering a clear and mutual understanding across the organization.

3. Scope

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

4. Definition

This section provides the definitions for terms used within this Information Technology (IT) Security Policy and its operational guidelines to ensure clarity and a mutual understanding of their meanings.

1. **"The Company"** means PRTR Group Public Company Limited, its subsidiaries, and affiliates that utilize shared information systems, networks, and computer infrastructures.
2. **"Human Resources Department"** means the Human Resources Department of PRTR Group Public Company Limited.
3. **"Information Technology Section"** means the Information Technology Section of PRTR Group Public Company Limited.
4. **"Users"** means Board Directors, executives, officers, employees, relevant users, and external users who are authorized to access the Company's network systems.
5. **"External Users"** means persons or legal entities other than the Company's officers and relevant internal users.
6. **"System Administrator"** means the IT Section Manager or other officers assigned by a supervisor at the Director level or above, responsible for the development, modification, improvement, and maintenance of the Company's information and network systems, or the department directly responsible for such oversight.
7. **"Information System"** means the Company's operational systems used for data storage, processing, and dissemination of information through the coordination of hardware, software, data, users, and processing procedures to produce information beneficial for planning, administration, and supporting the Company's operational mechanisms.

8. **"Network System"** means a system used for communication or the transmission of data and information between various IT systems of the Company, such as LAN, Wireless, Intranet, Internet, and other communication systems.
9. **"Assets"** means any tangible or intangible property or item of value to the Company, including data, information systems, and IT/Communication assets such as personnel, hardware, software, computers, servers, networks, network equipment, IP addresses, licensed software, or anything of value to the Company.
10. **"Information Technology (IT) Security"** means the stability and security of the Company's IT and network systems by maintaining the Confidentiality, Integrity, and Availability of information, including other attributes such as Authenticity, Accountability, Non-Repudiation, and Reliability.
11. **"User Rights"** means the classification of access levels to information for officers and relevant users, including general rights, privileged rights, and any other rights pertaining to the Company's information and network systems.
12. **"Access and Information Usage Control"** means the granting of permission, rights, or authorization for users to access or utilize network or information systems, both electronically and physically, as well as the establishment of protocols regarding unauthorized access.
13. **"User Account"** means employee ID, E-mail, Username, and Password for officers, relevant users, and external users.
14. **"Security Event"** means a case identifying an occurrence or a state of a service or network indicating a possible breach of security policies, a failure of protective measures, or an event that may potentially involve security risks.
15. **"Encryption"** means the process of encoding data to prevent unauthorized access. Only those with the appropriate decryption program can restore the encrypted data to its original usable state.
16. "Authentication" means the security procedure for system access, used to verify the identity of a user, typically through a username and password.

17. **"SSL (Secure Socket Layer)"** means a data encryption technology used to enhance the security of communication or data transmission over the internet between a server and a web browser or application.
18. **"VPN (Virtual Private Network)"** means a private, virtual computer network that utilizes actual data transmission channels through a specialized encryption process over the internet, ensuring that data remains unreadable and invisible to others until it reaches its destination.

5. Information Security

5.1 Information Security

Objectives : To ensure that the operations of employees handling data, including the management of relevant information systems, are conducted with adequate information security measures to support business operations. This is to ensure the security, confidentiality, integrity, and availability of the Company's data, thereby mitigating potential impacts on the Company's finances, credibility, and reputation.

Scope: This Policy encompasses the protection of the Company's data, with a primary focus on data in electronic format. It is applicable to all personnel across all levels of the organization, including executives, employees, and relevant third parties involved in the utilization of the Company's data.

5.2 Communication of the Regulations

The Company mandates that all employees must undergo mandatory training regarding the secure utilization of information systems. Furthermore, every employee is required to formally sign an acknowledgment of the terms and conditions governing the use of the Company's information systems.

5.3 Review of the Regulations

The Information Technology (IT) Manager shall review this Policy at least once (1) per year to ensure its alignment with organizational changes and future risk trends that may impact the Company's information security. Such reviews are mandatory during significant transitions, including shifts in IT strategy and direction, or major structural changes within the Company or its technology infrastructure. The reviewed Policy shall be submitted to the

Deputy Managing Director for review and signature as the 'Prepared By' authority, and subsequently presented to the Chief Executive Officer (CEO) for final review and formal approval signature.

5.4 Penalties

Any individual found in violation of this Policy shall be deemed to have committed a severe disciplinary offense. Such violations are subject to maximum disciplinary actions in accordance with the Company's Work Rules and Regulations.

6. Organization of Information Security

6.1 Internal organization

Objectives: To establish appropriate and secure information security management roles and responsibilities within the organization, Executive Management shall appoint an Information Security Working Group or Committee. This group is officially delegated with the duties and responsibilities for overseeing the Company's information security framework. Segregation of Duties:

1) The Information Technology (IT) Manager is responsible for defining appropriate information security roles and responsibilities. Furthermore, the IT Manager shall oversee and control operational activities to ensure continuous compliance with the Company's information security policies and operational guidelines.

2) The Information Technology (IT) Manager is accountable for the overall management, governance, monitoring, and formal review of the Company's information security policy framework.

3) Executive Management is responsible for the oversight of information security to ensure that all activities align with the Company's information security policies and operational guidelines.

4) All employees and third-party service providers must strictly adhere to the Company's information security policies and operational guidelines.

Contact with authorities:

1) The Company shall maintain a comprehensive registry of contact information for relevant authorities and organizations, such as the Royal Thai Police, Internet Service Providers (ISPs), and the Thailand Computer Emergency Response Team

(ThaiCERT). This registry is established to facilitate effective coordination and timely response regarding information security incidents and regulatory compliance.

Contact with special interest groups:

1) The Company shall maintain a formal registry of contact information for special interest groups and professional organizations dedicated to information security. This is to facilitate continuous engagement, knowledge sharing, and staying informed regarding the latest security trends, emerging threats, and industry best practices.

Information Security in Project Management:

1) Comprehensive regulations, rules, and criteria regarding operational processes and data access must be established to ensure project security. This includes, but is not limited to, the formal definition of User Access Rights to project-related information.

In cases where projects involve third-party service providers, all operations must strictly adhere to the Company's Information Technology (IT) operational procedures. This requirement is established to ensure secure project management and to mitigate potential risks or adverse impacts.

7. Asset Management

7.1 Responsibility for Assets

Objective: To ensure that all corporate assets are identified and appropriate responsibilities for their protection are assigned, the following principles apply:

Assets refer to data, software, and all related information processing equipment. The Company mandates the appointment of Asset Owners to be responsible for such assets. While an Asset Owner may delegate the daily maintenance and control of an asset to another individual, the Asset Owner remains ultimately accountable for the security and protection of said asset.

7.1.1 The Accounting Department is mandated to maintain a comprehensive asset register for hardware and software. This register must include all pertinent details. Physical asset verification shall be conducted in coordination with asset custodians to ensure the asset register is updated at least once (1) per year.

7.1.2 The asset register must clearly identify the custodian or person responsible for each asset. It is required to review the accuracy of asset details within the register and formally notify the Accounting Department of any asset transfers across affiliated companies within the Group.

7.1.3 For new employees, the Human Resources Department shall provide an 'Add/Change/Terminate User Rights' form. The relevant department head must define appropriate access levels for data systems, network usage, and peripheral devices. These user access rights must be formally reviewed at least once (1) per year.

7.1.4 Upon termination of employment, expiration of contract, completion of engagement, or resignation, employees must return all Company assets in their possession. The Human Resources Department will issue an 'Asset Checklist' to the direct supervisor to monitor the handover and inspect the condition of the assets. Employees shall be held liable for any damages or missing data identified during the inspection process.

7.1.5 The Accounting Department shall maintain a Software License Register to control software copyrights and the Company's intellectual property rights. The IT Department is responsible for the secure storage of legal documentation proving ownership. The Accounting Department is required to perform a random audit of these ownership documents at least once (1) per year.

7.2 Information classification

Objectives : The Company has established criteria for Data Classification to ensure that all information is categorized and protected appropriately, in accordance with the management guidelines for each classification level. Furthermore, it is mandated that Data Owners and relevant Data Custodians are responsible for classifying information to ensure it receives a level of protection commensurate with its significance and value to the Company.

7.2.1 Information must be classified based on legal requirements, business value, criticality, and the degree of sensitivity regarding unauthorized disclosure or modification. The classification categories are defined as follows:

1) Tier 1 : Information that can be disclosed to the general public without restriction, or information that is required by law to be made publicly available.

2) Tier 2 : Information designated by the Data Owner for internal circulation among all employees within the Company. Disclosure to external parties is strictly prohibited, as it may cause potential damage or adverse impacts to the Company.

3) Tier 3: Internal information designated by the Data Owner that must not be disclosed to all employees. Access to this information is strictly restricted to authorized personnel who require it for specific operational purposes. Access is granted based on the 'Need-to-Know' principle, ensuring only the minimum necessary information is available for the performance of duties.

7.3 Media Handling

Objectives : To prevent the unauthorized disclosure, modification, removal, deletion, or destruction of information stored on storage media.

7.3.1 Operational procedures for the management of storage media must be formally established and strictly adhered to. These procedures must align with the Company's information classification standards and guidelines.

1) All storage media must follow the prescribed naming conventions and be maintained within a formal usage control register.

2) The requisition or withdrawal of storage media must receive formal approval from the authorized person within the requesting department.

3) All storage media must undergo a formal physical count and inventory verification at least once (1) per year.

7.3.2 The disposal or destruction of data and storage media must be conducted in strict accordance with the Company's established destruction procedures. For confidential information, formal approval from an authorized person is required, and

each instance of destruction must be documented as an official record for future auditing purposes.

1) Physical Documents: Document destruction must be carried out via paper shredding, incineration, or other methods that ensure the information is rendered permanently irrecoverable.

2) Storage Media: Electronic media must be destroyed using methods that guarantee all data contained within the media is non-recoverable and cannot be reused.

7.3.3 Physical Media Transfer: Measures must be implemented to protect information from unauthorized access, misuse, or damage during the transit and physical transfer of storage media.

7.3.4 The use of removable media—including but not limited to USB Drives, Flash Drives, External Hard Disks, and Memory Cards—is strictly subject to formal authorization and usage controls. Furthermore, it is mandatory that all data stored on such removable media be encrypted to ensure its security.

8. Access Control

8.1 Business Requirements of Access Control

Objective: To restrict access to information and information processing facilities, and to mitigate the risks associated with unauthorized or inappropriate usage.

8.1.1 Access Control: The Information Technology (IT) Department shall maintain an Inventory of Authorized Access to Information Systems. This inventory must be formally reviewed in accordance with both business requirements and information security standards.

8.2 System and Application Access Control

Objectives : To prevent unauthorized access to the operating system (OS) by unprivileged users, the Information Technology (IT) Department must implement mandatory system use notification (Log-on warning banners), robust user authentication protocols, and

comprehensive password management for all users. Furthermore, controls regarding session time limits and connection duration to the information systems must be strictly enforced.

8.2.1 Information Access Restriction: Access to information and application functions must be restricted in accordance with the established access control policy. System Administrators are required to implement a system notification displaying a 'Log-on Warning Banner' stating: 'Authorized Personnel Only' prior to establishing a connection to the Company's computing resources. Furthermore, the system must provide users with an explicit option to terminate the connection should they determine that the system is irrelevant to their authorized duties.

1) Every user must be assigned a unique Personal User ID to ensure individual identification and the traceability of all system activities.
2) Users are required to log off from the network immediately upon completion of their tasks or when system access is no longer necessary.
3) All computers must be configured with a password-protected screen saver. This security feature shall be automatically activated after a predetermined period of inactivity.
4) In the event of extended periods of inactivity, users must properly shut down their computers or terminal devices.
5) The use of Administrator Accounts must be strictly controlled and restricted. Administrative privileges shall be granted based on specific job responsibilities and necessity, adhering to the 'Principle of Least Privilege.
6) A formal review and audit of system access rights must be conducted at least once (1) per year, or immediately upon any significant organizational or system changes.

8.3 User Access Management

Objectives : To restrict information system and service access to authorized users only, and to prevent unauthorized access through robust entitlement controls. This framework governs the entire user lifecycle management process including the requisition, modification, and

termination of access rights—as well as the stringent oversight of privileged accounts with the authority to modify system configurations or access permissions.

8.3.1 Requisition, Modification, and Termination of User Access Rights:

1) Every employee authorized to access information systems must be assigned a unique personal User ID for system authentication.
2) User IDs are strictly personal; the use of Shared User IDs is prohibited. Upon an employee's resignation or termination, their specific User ID must be deactivated and shall not be reassigned to any other individual.
3) All requests for system access must undergo formal review and receive written endorsement from the relevant department head or direct supervisor.
4) Department supervisors and the Information Technology (IT) Department must coordinate to ensure the immediate termination of access rights for any user who no longer requires system access.

8.3.2 Review of User Access Rights: Departmental supervisors are required to conduct a formal review of user access rights at least once (1) per year. This review process is mandatory to ensure that access permissions remain aligned with current job responsibilities and the 'Principle of Least Privilege.

8.4 User Responsibilities

Objective: To ensure that all system users maintain high levels of information security awareness, users are required to strictly cooperate in the management of their passwords and must be fully informed of the proper security procedures to be followed upon the completion of their computer-related tasks.

8.4.1 All users must adhere to the following authentication standards:

1) System passwords must be treated as strictly confidential. Users are prohibited from sharing or disclosing their User ID and password to any other individual.

2) Passwords must be a minimum of eight (8) characters in length and must consist of a combination of numeric digits, special characters, and both uppercase and lowercase letters.

3) Users must change their passwords every ninety (90) days, regardless of whether the system enforces a change. The new password must not be identical to previous passwords, and simple sequential numeric suffixes are strictly prohibited.

4) Users are responsible for verifying that their granted access levels are appropriate for their current job responsibilities. Any discrepancies must be immediately reported to their supervisor for formal review and adjustment.

5) In cases where software limitations prevent the application of the standard password policy, configuration shall follow the maximum security capabilities of said software.

6) Users must change their passwords according to Company schedules or immediately upon suspicion that their credentials have been compromised.

7) Users are prohibited from reusing any of their four (4) most recent passwords.

8) Following three (3) consecutive failed login attempts, the user account shall be 'Suspended' or 'Locked' permanently. The account cannot be automatically unlocked; the user must contact the Information Technology (IT) Department to initiate a formal unlock procedure.

9) In instances where specific user accounts cannot comply with the Company's mandatory password standards due to software technical limitations or essential system integrations, the following exception guidelines shall apply:

   - Maximum Password Age: For System Accounts, Service Accounts, or Database Accounts used for reporting systems and application integrations—where password expiration would result in business

continuity disruptions an exemption is granted to configure these accounts with non-expiring passwords ('Password Never Expires').

- Complexity and Lockout Policies: If a system does not support mandatory complexity, password history, account lockout thresholds, or lockout durations, compensating controls must be implemented. In such cases, a complex password with a minimum length of 14 – 16 characters, or the maximum length supported by the system, must be utilized to mitigate the absence of standard security features.
- Documentation and Review of Exceptions: The Information Technology (IT) Department is mandated to maintain a formal 'Exception List.' This document must detail the specific technical limitations and the corresponding compensating controls implemented. A formal review of these exceptions must be conducted with departmental supervisors at least once (1) per year, or upon any significant system upgrades.

9 Cryptography

9.1 Cryptographic Controls

Objectives : To ensure the appropriate and effective use of cryptography for protecting the confidentiality, authenticity, and integrity of information. To safeguard data security across both confidentiality and integrity dimensions, it is mandatory to evaluate and implement cryptographic software and techniques. This is particularly essential for information identified as high-risk, to prevent unauthorized disclosure, tampering, or any compromise of data accuracy.

9.1.1. Standards and Operational Procedures for Third-Party Service Provider Management:

1) Database Password Encryption: All passwords stored within database systems must be encrypted. Access to and knowledge of these

passwords shall be restricted exclusively to the credential owner and the designated data-owning software.

2) Email Encryption Protocols: All email communications must utilize encryption. Specifically, data protection must be implemented at the 'Field-Level' for sensitive information within the email infrastructure.
3) Secure Transmission of Confidential Data: Emails containing sensitive information must be transmitted in an encrypted format. Furthermore, confidential files sent to external parties must be encrypted. To ensure maximum security, the encrypted file and its corresponding password (decryption key) must be transmitted via separate communication channels and must never be included within the same email.

10 Physical and Environmental Security

10.1 Secure Areas

Objective: To define secure areas within the Company and establish appropriate protective measures based on the risk levels of each specific location. These controls are designed to provide fundamental protection for the Company's information and information processing facilities against unauthorized access, potential damage from threats, and disruptions caused by either intentional acts or natural disasters.

10.1.1 The Department has designated the Server Room in a secure location, effectively shielded from external threats. The facility is situated in an area with restricted public access and is located on a high-floor level of the building to prevent flood-related damage. The surrounding perimeter is designed to be open and transparent, ensuring clear visibility of any individual attempting to access the Server Room.

10.1.2 Access to the Server Room is strictly restricted to authorized Information Technology (IT) personnel and designated stakeholders. Should it be necessary for unauthorized external parties to enter for service or maintenance, formal prior approval is mandatory. Every instance of external access must be officially documented in the 'Server Room Access Log.' Furthermore, the following security measures must be implemented:

1) CCTV Surveillance: High-definition CCTV cameras must be installed to provide continuous (24/7) monitoring of the Server Room interior. The system must maintain a minimum of thirty (30) days of historical video footage for retrospective review.

10.1.3 Protection Against External and Environmental Threats:

1) The Data Center must be equipped with a comprehensive Fire Suppression System, a specialized Climate Control System (HVAC), and a robust Power Supply Management System.

2) The facility shall utilize dual (2) air conditioning units operating in an alternating (Redundant) configuration. The internal temperature must be strictly maintained between 20°C and 25°C, with relative humidity levels not exceeding 50%.

10.2 Equipment Management

Purpose : To prevent the loss, damage, theft, or compromise of computing and network equipment, and to safeguard the Company's operations against any unauthorized disruptions.

10.2.1 Server Monitor: Comprehensive server status reports, encompassing all critical servers and essential peripheral devices, must be generated on a daily basis. Responsible personnel are required to document all operational conditions within the 'Server Operational Status Log.' Furthermore, a performance summary report for all servers must be formally presented to Management for review on a quarterly basis.

10.2.2 Supporting Utilities: All critical equipment must be protected against power failures and other potential disruptions caused by the failure of supporting utilities or infrastructure systems. This includes implementing measures to ensure continuous operation and system stability.

1) Critical computing and network equipment must be supported by an Uninterruptible Power Supply (UPS) system. This requirement ensures continuous operational stability or facilitates a controlled and graceful system shutdown in the event of a primary power failure.

Uninterruptible Power Supply (UPS) equipment must undergo regular inspections and testing in strict accordance with the manufacturer's specified procedures. This is to ensure that the units maintain full operational capacity and reliability to support critical systems during a power failure or electrical disruption.

11 Operations Security

11.1 Operational Procedures and Responsibilities

Objective: To ensure the security and integrity of information processing operations, with careful consideration for the appropriate Segregation of Duties (SoD).

Regarding Capacity Management, system resource utilization must be continuously monitored, optimized, and projected for future requirements to ensure that system performance meets established standards. To achieve this, the Information Technology (IT) Department has developed an 'IT Master Plan.' This plan ensures that the Company's information assets remain secure, while remaining easily accessible and usable by authorized personnel. Furthermore, the plan encompasses the strategic provisioning of software, hardware, and essential supporting equipment to align with the Company's overall strategic objectives.

11.2 Protection from Malware

Purpose: To control and protect software and information assets from malicious programs and harmful software, ensuring the integrity and availability of the Company's information systems.

11.2.1 Comprehensive measures for the detection, prevention, and recovery from malicious software must be implemented in conjunction with appropriate user security awareness programs.

1) The Information Technology (IT) Department must ensure the installation of the latest version of Antivirus/Antimalware software on all workstations and servers. These systems must be continuously updated with the most recent virus definitions.

2) The Information Technology (IT) Department must configure antivirus scanning to initiate automatically upon system startup. Such protection

must remain active and operate in real-time throughout the duration of system usage.

3) All email attachments and files downloaded from the internet must undergo mandatory virus scanning prior to being opened or executed.
4) Employees are strictly prohibited from engaging in the development, possession, or distribution of computer viruses or any form of malicious software.
5) In cases where authorized external storage media is utilized, users are required to perform a comprehensive virus scan every time before accessing or transferring data from such media.

11.3 Backup

Objective : To prevent data loss and to ensure that information processing facilities maintain their integrity, accuracy, and continuous availability at all times.

11.3.1 Backups of information, software, and system images must be maintained and regularly tested for availability and readiness.

1) A formal Backup and Disaster Recovery (DR) Plan must be established, including procedures for system and data recovery testing. This plan must be reviewed and updated annually.

2) Detailed operational manuals for the backup and recovery of all critical systems must be developed and maintained within the 'Backup and Data Recovery Manual.
3) The Information Technology (IT) Department is required to monitor the status of all system backups daily. All backup outcomes and operational statuses must be formally recorded in the 'Daily Backup Status Log.
4) The IT Department must conduct restoration tests for all system backups. Critical systems must undergo recovery testing in accordance with the established plan. A summary report of these test results must be presented to the Information Security Committee at least once (1) per year.

5) Users are individually responsible for the backup of critical files and data stored locally on their personal computers or workstations.

11.4 Logging and Monitoring

Objective: To ensure the systematic recording of events and the generation of verifiable evidence.

11.4.1 Event logs encompassing user activities, system anomalies (deviations from standard operating procedures), operational errors, and information security incidents must be systematically recorded, securely stored, and regularly reviewed. Furthermore, logging facilities and the recorded log data must be protected against unauthorized access and any form of tampering or modification.

11.5 Control of Operational Software

Objective: To ensure the correct and secure operation of operational systems.

11.5.1 Installation of Software on Operational Systems:

The installation of software on all Company computing devices must be performed exclusively by the Information Technology (IT) Department. All installations must be verified and conducted in strict accordance with the established Asset Management policy and procedures.

11.6 Technical Vulnerability Management

Objectives : To prevent the exploitation of technical vulnerabilities.

11.6.1 Management of Technical Vulnerabilities: Information regarding technical vulnerabilities and the Company's exposure to such weaknesses must be systematically collected and evaluated. Appropriate countermeasures must be implemented to mitigate associated risks. All identified vulnerabilities must be documented in the 'Technical Vulnerability Log,' and a comprehensive vulnerability report must be presented to Senior Management at least once (1) per year.

11.6.2 A formal vulnerability assessment must be conducted at least once (1) per year. This assessment shall encompass all information systems, including servers, database systems, applications, network infrastructure, and related hardware components.

11.6.3 All detected vulnerabilities must undergo a formal risk assessment and be categorized into four severity levels: Low, Medium, High, and Critical. Based on these levels, specific remediation timelines must be established to ensure timely and effective resolution.

Critical: Within seven (7) days

High: Within fourteen (14) days

Medium: Within thirty (30) days

Low: As appropriate.

11.6.4 Penetration Testing: Formal Penetration Testing must be conducted on all critical systems at least once (1) per year. Furthermore, additional testing is mandatory following any significant system upgrades or major architectural changes to ensure that no new security vulnerabilities have been introduced.

11.7 Information System Audit Considerations

Objective: To minimize the operational impact of audit activities on production and operational systems.

11.7.1 Information Systems Audit Controls:

Audit requirements and evaluation activities involving operational systems must be carefully planned and mutually agreed upon. This is to minimize the potential for operational disruptions to business processes. The Information Technology (IT) Department is responsible for establishing a formal assessment schedule for all critical systems within the 'Systems Audit Register.' The resulting assessment reports must be formally presented to Senior Management in accordance with the established reporting schedule.

12 Communications Security

12.1 Network Security Management

Objective: To ensure the security and efficiency of the network infrastructure as a reliable medium for data transmission.

12.1.1 Network Controls: Networks must be managed and controlled to protect information within various systems. The Information Technology (IT) Department is responsible for network operational controls, as follows:

1) Establish and maintain comprehensive 'Network Configuration Diagrams' detailing all communication equipment and circuits. This includes the regular update of network topologies, server locations, and server service/port tables to ensure they remain current.
2) Control and oversee the installation of all communication hardware to ensure strict alignment with the approved network configuration diagrams.
3) Implement measures to monitor the condition and evaluate the performance of communication lines, circuits, and network equipment to ensure continuous availability.
4) Conduct regular and systematic maintenance of all network hardware and associated equipment.
5) Conduct a formal network performance assessment at least once (1) per year. Develop strategic plans for network enhancements to accommodate future business expansion and workload growth.

12.1.2 Security of Network Services: Security mechanisms, service levels, and management requirements for all network services must be formally identified and incorporated into network service agreements, whether these services are managed in-house or outsourced to external providers. Network service providers must undergo regular audits and performance analysis. This evaluation shall encompass service level compliance, network security architecture, operational management, and overall alignment with the Company’s requirements.

12.1.3 Network Segregation and Segmentation: The Company shall establish a network architecture that clearly segregates operational environments between the Internal Network and the External Network. Furthermore, the network must be segmented into sub-networks based on data sensitivity and criticality. This is to

prevent unauthorized access and to contain the scope of potential impact in the event of a security breach. The following operational guidelines apply:

1) Network Controls: Deploy security and access control devices (e.g., Firewalls or Gateways) to filter and monitor all traffic between internal and external networks, in strict accordance with the Information Security Policy.

2) Access Restriction: Define and enforce access rights ensuring that users or systems can only access specific network segments necessary for their designated job functions.

12.2 Information Transfer

Objective : To ensure the security of information during transfer, both internally within the Company and externally with third-party organizations.

12.2.1 Electronic Messaging: All information transmitted via electronic messaging systems must be protected with appropriate security measures to ensure confidentiality and integrity.

12.2.2 Network Monitoring: The Information Technology (IT) Department is responsible for monitoring network utilization across all departments. Comprehensive network usage reports must be generated and formally presented to Senior Management on a regular basis.

12.3 Remote Access Policy

Purpose : To ensure the security and efficiency of Remote Access to internal systems, and to safeguard against cyber threats.

12.3.1 Remote Access Controls:

12.3.1.1 Access Rights and Authentication:

1. Identification and Role-Based Access: All individuals granted remote access must be clearly identified. Access privileges shall be defined based on specific job functions (Role-Based Access Control - RBAC) to restrict access solely to necessary system components.

2. Users are strictly prohibited from sharing user accounts (Shared Accounts) or disclosing passwords to any other individual under any circumstances.
3. Access by external organizations or third parties must utilize dedicated external user accounts, following the Principle of Least Privilege. Passwords for these accounts must be changed immediately upon completion of the task, or the accounts must be configured with a pre-defined expiration date (Expired Account). Furthermore, all external access sessions must be actively monitored and logged.

12.3.1.2 Geographic Access Control - O365:

1. The Microsoft 365 (O365) environment shall be configured to permit access exclusively from within Thailand. Access attempts from all international locations must be strictly blocked to mitigate the risk of cross-border cyberattacks.
2. In the event that access is required from abroad, users must formally notify the Information Technology (IT) Department in advance. Such requests will be evaluated on a case-by-case basis for temporary exemption (Temporary Whitelisting) within a specified timeframe.
3. Users granted temporary overseas access are required to perform Multi-Factor Authentication (MFA) and must connect solely through the organization’s designated secure communication channels.

12.3.1.3 Device Security:

1. All portable computing devices must implement full-disk encryption (Disk Encryption) and be equipped with the latest version of Antivirus or Endpoint Protection software.
2. Access to internal systems from remote locations must be established exclusively through the organization's designated Virtual Private Network (VPN).
3. Automatic Session Timeouts must be configured for all remote connections. If no user activity is detected within the specified timeframe, the system must automatically lock the screen or terminate the connection.

13 System Acquisition, Development and Maintenance

13.1 Security Requirements of Information Systems

Objective : To ensure that system development incorporates adequate security measures and internal controls, the Company requires a formal assessment of security requirements prior to any development activities.

13.1.1 Information Security Requirements Analysis and Specification:

Information security requirements must be integrated into the specifications for all new systems or enhancements to existing systems.

1) Business System Owners are required to define specific information security requirements before the development or procurement of any application. These requirements must be formally documented in the 'Program Development Request Form,' which constitutes an integral part of the system development or procurement specifications.
2) Defined requirements must receive formal approval from authorized personnel before being submitted to the Information Technology (IT) Department for technical feasibility assessment and development.

13.2 Security in Development and Support

Objective: To ensure that information security is designed and implemented throughout the entire System Development Life Cycle.

13.2.1 System Change Control Procedures: All system changes within the development life cycle must be governed by formal 'System Change Control Procedures.' The Information Technology (IT) Department is responsible for maintaining and updating the official 'System Version Control' documentation.

13.2.2 System Acceptance Testing: Comprehensive testing plans and acceptance criteria must be established for all new systems, system enhancements, and new version releases.

1) Procedures must be established to verify the accuracy of all computer-generated output, ensuring that data maintains its integrity and completeness.
2) The original requester (Business Owner) is responsible for performing the system testing and providing a formal sign-off in the 'Program Development Request Form' to signify system acceptance.

13.3 Test Data

Objective: To ensure the protection and integrity of data utilized during the testing process.

13.1.1 The environments for development, testing, and production (live operations) must be strictly segregated. This is to mitigate the risk of unauthorized access or unintended modifications to the production environment.

1) In the process of system development, a clear separation must be maintained between the Development System and the Production System.
2) Formal and documented procedures must be established for the secure migration and deployment of completed software from the development environment to the production environment.

14 Supplier Relationships

14.1 Information Security in Supplier Relationship

Objective: To ensure the protection of the Company's information assets that are accessed or managed by external service providers.

14.1.1 Information Security Policy for Supplier Relationships: To mitigate risks associated with third-party access to the Company's assets, formal written agreements must be established with all external service providers. The Information Technology (IT) Department is responsible for maintaining all Service Level Agreements (SLAs) and contracts as formal evidence of compliance.

14.2 Supplier Service Delivery Management

Objective : To maintain the security standards of operations performed by external parties in accordance with established agreements.

14.2.1 Monitoring and Review of Supplier Services: The Information Technology (IT) Department must systematically monitor, review, and audit the services provided by external suppliers on a regular basis.

1) Service audits of external organizations must be conducted by personnel possessing adequate knowledge of information security, as well as a thorough understanding of relevant contractual terms and conditions.

2) In the event of a security incident caused by a third party, appropriate measures must be taken to preserve the integrity of evidence and to initiate legal action where necessary.

A formal assessment of external service providers must be conducted annually, in accordance with the terms specified in the contract. A summary report of these supplier evaluations must be prepared and presented to Senior Management for acknowledgment.

15 Third-party management

Objective : To ensure that the management of Information Technology (IT) service providers and business partners—who connect to the Company's IT systems or have access to critical information and customer data—is conducted appropriately, efficiently, and securely.

The following standards and operational procedures for third-party management are established to safeguard the Company's assets, encompassing at least the following areas:

1) Prior to engaging any services, the Company shall identify and assess potential risks to information and IT systems accessible by the third party. This assessment must consider the scope, rationale, duration, and necessity of access, as well as constraints or agreements regarding provider transitions and contract termination or expiration.

2) Security obligations must be imposed on all external organizations, including their sub-contractors, ensuring strict alignment with the Company's Information Security Policy.

3) Execution of a formal Non-Disclosure Agreement (NDA) is mandatory for all partnerships.

4) Service contracts and agreements must comply with the Company's Security Policy. This includes, but is not limited to, the certified destruction of all Company or customer data upon service termination and clear liability for data breaches resulting from unauthorized data use beyond the scope of the agreement.

5) A formal process must be maintained for the ongoing monitoring, evaluation, review, and reporting of third-party performance and security compliance.

16 Information Security Incident Management

16.1 Management of Information Security Incidents and Improvements

Objective : To ensure a consistent and effective approach to the management of information security incidents.

16.1.1 Responsibilities and Procedures: Management responsibilities and operational procedures must be established to ensure a rapid, effective, and orderly response to information security incidents. All reported issues and incidents must be formally documented using the 'Incident Reporting Form.

16.1.2 Reporting Information Security Events:

All reported security issues that have been resolved within the specified timeframe shall undergo data processing and analysis. This analysis aims to identify the most prevalent issues, determine their root causes, and develop preventive measures to mitigate future occurrences. The Information Technology (IT) Department is responsible for preparing a summary report to be presented to the Information Security Committee every three (3) months. This report serves as a basis for collective review and the establishment of long-term preventive strategies.

17 Information Security Aspects of Business Continuity Management

17.1 Information Security Continuity

Objectives : To prevent and mitigate the impact of business disruptions caused by system threats, ensuring that operational risks remain within acceptable levels and that the Company's core business functions can be sustained.

17.1.1 Planning Information Security Continuity: The Company must define information security requirements and continuity standards for disaster or crisis scenarios. Management and relevant departments are responsible for managing processes to develop and maintain business continuity. This management framework must incorporate the following key elements:

1) Conduct comprehensive analysis and assessment of risks that could impact the Company's business operations.

2) Develop formal business continuity strategies and documentation that strictly align with the Company's business objectives.
3) Provide training to ensure employees are security-aware, understand the continuity plans, and are capable of executing their designated roles within those plans.
4) Formally define responsibilities for the coordination, development, review, and continuous improvement of the continuity plans.

17.1.2 Implementing Information Security Continuity: The Company shall establish, document, and maintain information management processes to ensure business continuity. This includes the continuous improvement of processes, procedures, and controls to achieve the required level of information security continuity during a disruptive incident.

1) Ensure that the emergency response and continuity plans are effectively communicated to all employees, ensuring organizational awareness and preparedness.

2) All business continuity plans (BCP) must be tested and exercised at defined intervals to validate their effectiveness and operational readiness.
3) Plan Owners are responsible for the ongoing maintenance, testing, and development of requirements and conditions necessary for the successful activation and execution of the plans.

17.1.3 Verify, Review and Evaluate Information Security Continuity The Company is required to perform periodic audits and reviews of established continuity measures at defined intervals. This ensures that such measures remain accurate, relevant, and effective in the event of a disruptive incident. The foundation of effective Business Continuity Management (BCM) lies in a comprehensive understanding of business processes and the events that may cause operational disruptions. Consequently, Business Process Owners and Application Owners who support these functions must actively participate in identifying potential threats and conducting risk assessments. This collaborative approach ensures the accuracy and completeness of the data required to develop and maintain a robust and effective Business Continuity Plan (BCP)

17.2 Redundancies

Objectives : To ensure the operational availability of information processing facilities.

17.2.1 Availability of Information Processing Facilities: Information processing facilities and computing equipment must be maintained with adequate redundancy and backup

provisions. This is to ensure that all operational systems consistently meet the defined availability and service level requirements.

18 Cloud services policy

Objective : To establish security measures for cloud service utilization and to ensure the protection of information systems and applications hosted within the cloud environment, safeguarding them against unauthorized access.

18.1 Cloud services must be managed and operated in a secure and resilient manner.

18.2 Access rights to information systems and applications must be strictly restricted to authorized personnel only. Access configurations should be granular and role-specific, such as 'Editor' (Read/Write), 'Viewer' (Read-only), and 'No Access.

18.3 The selection of Cloud Service Providers must be based on their ability to maintain robust security measures across their IT infrastructure, as follows:

18.3.1 The Cloud Service Provider (CSP) must provide secure and robust authentication mechanisms for system access.

18.3.2 The Cloud Service Provider (CSP) must have clear guidelines and practices for maintaining the security of their cloud infrastructure.

18.3.3 The Cloud Service Provider (CSP) must implement proactive procedures for identifying and remediating vulnerabilities within their IT infrastructure to ensure ongoing security.

18.3.4 The Cloud Service Provider (CSP) must maintain formal change management processes for infrastructure modifications and must provide advance notification to the Company for any changes that may impact operational services.

18.3.5 The Cloud Service Provider (CSP) must provide accessible and responsive contact channels for incident reporting and technical coordination.

18.3.6 The Cloud Service Provider (CSP) must maintain a dedicated security operations structure and team for continuous

monitoring and incident management, with a requirement to notify the Company as necessary.

18.3.7 In the event that digital evidence or forensic data residing within The Cloud Service Provider (CSP) environment is required, the CSP must provide the necessary assistance and cooperation in delivering such information.

18.4 The Company shall formally define all roles and responsibilities associated with the utilization and management of cloud services to ensure clear accountability.

18.5 The Company must maintain oversight and ensure the effectiveness of information security controls implemented by the Cloud Service Provider (CSP).

18.6 In scenarios where the Company utilizes multiple cloud services (Multi-Cloud), procedures must be established to manage service interfaces and coordinate all associated system changes securely.

18.7 Formal incident management procedures must be established specifically for identifying, responding to, and recovering from information security incidents related to cloud service usage.

18.8 The Company shall establish a framework for the continuous monitoring, review, and evaluation of cloud service utilization. This is to ensure proactive management of information security risks on an ongoing basis.

19 Compliance Review

Objective: To ensure that the Company's information security operations strictly align with established policies and security standards, relevant management personnel are required to review the compliance of operational procedures under their responsibility. This includes, but is not limited to, the formal review of system access rights and the evaluation of business continuity and emergency backup plans. Such reviews must be conducted at least once (1) per year.

20 Media disposal

Purpose: To ensure that obsolete or unnecessary data storage media are securely destroyed or erased, preventing unauthorized access and mitigating the risk of sensitive information leakage or misuse.

20.1 All Company-owned electronic storage media must be returned to the Information Technology (IT) Department when they are no longer required for business purposes or if the media becomes defective or non-functional.

20.2 Electronic storage media must be destroyed in a manner that ensures data is rendered permanently irrecoverable by any technical means or recovery methods.

20.3 Paper-based media and documents must be destroyed when they are no longer necessary for retention or operational use. The destruction process must strictly adhere to the defined data classification levels and established disposal procedures.

21 Mobile Device and BYOD Management

Objective: To establish guidelines and security measures for the utilization of Mobile Devices and personal equipment (Bring Your Own Device - BYOD) in accessing corporate resources and data, thereby mitigating the risk of data leakage and preventing unauthorized access.

21.1 Personal mobile devices (BYOD) intended for work purposes must be formally registered and approved by the respective supervisor. Such devices shall not be permitted to connect directly to the Company's core internal systems or databases.

21.2 All mobile devices and BYOD must have Anti-Virus software installed. A formal verification of the Anti-Virus update status must be conducted every six (6) months.

21.3 Approved BYOD must be kept in a secure location and must not be left unattended in areas where there is a risk of loss or theft.

21.4 The Company strictly prohibits the use of BYOD for downloading, storing, or archiving software, corporate data, customer information, or non-essential personal data from the Company's systems.

21.5 All Company-owned mobile devices and approved BYOD must adhere to the following security protocols:

1) Employees are responsible for maintaining high security awareness, ensuring device readiness, and taking proactive measures to prevent theft or loss.

2) All devices must receive formal authorization prior to connecting to any Company-related network or system.

3) Devices that have bypassed security controls, such as through Jailbreaking or Rooting, are strictly prohibited from connecting to the Company's systems.

4) Only applications listed in the Company's approved catalog may be installed. Downloads must be performed exclusively through authorized application stores.

5) Installing applications from unauthorized sources or third-party stores outside of the Company's approved list is strictly forbidden.

6) Employees must grant the Company the right to audit and inspect mobile devices and BYOD utilized for work purposes.

7) All devices must implement screen lock settings in strict accordance with the Company's defined security standards.

8) Employees must protect information from unauthorized disclosure by implementing full-disk or data-level encryption, based on the relevant data classification levels.

9) Remote Geo-location capabilities must be enabled on all mobile devices to facilitate tracking and recovery.

21.6 Employees are required to perform backups of essential work-related data on Mobile Devices and approved BYOD. Such backups must be stored exclusively within the Company's designated secure storage locations.

21.7 In the event of an information security incident, employees must grant the Company the right to remotely wipe or erase all data from the Mobile Device or BYOD utilized for work. This consent applies even if the device contains the employee's personal information.

21.8 The Company reserves the right to deny or terminate access from any personal device to corporate information and systems if the device is deemed to pose a potential risk to the Company's data, systems, employees, or customers.

21.9 The Company reserves the right to execute remote data destruction (Remote Wipe) on personal devices used for work. This action may be taken in response to incidents involving data leakage or any security compromise.

21.10 The Company reserves the right to audit and inspect the utilization of any personal device used for work purposes, whenever such inspection is deemed necessary or as part of a scheduled compliance audit.

22 Information Security and Personal Data Protection in Human Resources

Objectives: To establish guidelines for managing information security and personal data protection concerning personnel throughout the pre-employment, employment, and post-employment phases. The objective is to mitigate risks arising from either accidental or intentional actions that impact information system security, and to ensure full compliance with relevant laws and regulations, such as the Personal Data Protection Act B.E. 2562 (PDPA).

22.1 Background checks must be conducted for all job applicants, with the scope of verification appropriately scaled to the requirements and sensitivity of the respective position.

22.2 All employees and relevant stakeholders must execute a formal Non-Disclosure Agreement (NDA) or confidentiality agreement as deemed appropriate for their role.

22.3 Employees must be formally notified of their specific duties and accountabilities regarding information security.

22.4 Information technology and personal data protection training, including potential impact assessments, must be conducted to foster employee awareness at least once (1) per year.

22.5 Access to information must be strictly restricted on a 'Need-to-Know' basis, ensuring employees access only the data necessary for their specific functions.

22.6 Upon termination of employment, all access rights to corporate systems and data must be revoked immediately.

23 System development and maintenance

Objective : To establish guidelines for the secure development, modification, and maintenance of the Company's information systems throughout the planning, development, testing, and deployment phases. The objective is to mitigate risks associated with system vulnerabilities and potential cyberattacks.

23.1 The application development environment must be strictly segregated from the live production environment.

23.2 When engaging external service providers for application development, information security requirements and obligations must be formally incorporated into the service contracts.

23.3 All system developments must undergo rigorous security controls and comprehensive testing prior to being promoted to the production environment.

23.4 The use or development of Application Programming Interfaces (APIs) must adhere to international standards. Compatibility and security testing must be conducted and verified before implementation into actual business operations.

24 Risk Management Policy

Objective: To establish guidelines and criteria for the identification, assessment, management, and monitoring of organizational risks, particularly those concerning information assets, information systems, human resources, and business processes. This is to ensure operational continuity, security, and full compliance with relevant laws and regulatory requirements.

24.1 An information security risk management framework must be established. Formal risk assessment reviews must be conducted at least once (1) per year, or whenever there are significant changes to the Information Asset Inventory (additions, removals, or material modifications), or changes that potentially impact existing security controls and personal data protection measures.

24.2 The Risk Assessment Report and the Risk Treatment Plan must be formally presented to Senior Management for acknowledgment and approval of the proposed risk response and mitigation strategies.

25 Generative AI Security Policy

Objective: To ensure the appropriate and compliant use of Generative AI by employees and relevant personnel, in accordance with applicable laws and regulations, and to prevent potential adverse impacts on individuals, the organization, and society.

25.1 Guidelines for Generative AI Usage:

1) The use of Generative AI must be strictly for the benefit of the Company and must align with the Company's official missions and objectives.

2) Generative AI must not be used to create content that violates laws, regulations, or is harmful, defamatory, offensive, or inappropriate.

3) Users must not utilize Generative AI to create or distribute content intended to distort facts, provide inaccurate information, or mislead others.

4) Internal organizational data and classified information (e.g., passwords, contractual agreements, confidential documents, internal project details, etc.) must not be inputted into or processed by Generative AI platforms.

5) Personal Data (e.g., full names, national ID numbers, addresses, phone numbers) and Sensitive Personal Data must not be shared with or used in conjunction with Generative AI.

6) Information that impacts system security (e.g., API keys, system configurations) must not be utilized within AI systems.

7) In the event of a security breach or violation arising from AI usage, users must immediately notify their supervisors and follow the established Incident Response procedures.

8) Content generated by AI must be thoroughly reviewed and verified before use or publication to avoid bias or unfair discrimination.

9) Users must ensure that AI usage does not lead to the infringement of copyrights, trademarks, or the intellectual property rights of third parties.

10) If errors or negative consequences arise from AI usage, the user must report the incident to their line management immediately.

26 Change Management Policy

Objective : To ensure that all information system changes are implemented systematically, minimizing the risk of errors and preventing adverse impacts on information security and business continuity.

26.1 Change Categories

1) Standard Change: Routine tasks with clearly defined standard operating procedures (e.g., monthly security patching). A formal Backup Verification must be performed prior to every execution.

2) Normal Change: Modifications to system functions or infrastructure that require a formal request and impact assessment before implementation. These are subdivided into:

- Minor Change: Small-scale modifications that result in no system downtime.
- Major Change: Significant updates that require Planned Downtime.

All Normal Changes must be submitted via a formal request for impact assessment and obtain authorized approval before commencement.

3) Bug Fix: Non-urgent software error remediation. The reported symptoms and Root Cause must be identified, and the fix must successfully pass User Acceptance Testing (UAT) in a staging environment before deployment to the production system to prevent regression or impact on other functions.

4) Emergency Change: Critical incident remediation or patching of high-severity security vulnerabilities. Approval must be obtained from authorized personnel as rapidly as possible (verbal or urgent communication channel approvals are permitted). A Backup Plan must be in place to mitigate risks, and full retrospective documentation must be completed within 24 hours of the change.

26.2 Implementation Rules

1) Approval: All system changes—with the exception of predefined Standard Changes—must undergo formal review and receive explicit approval from authorized personnel prior to execution.

2) Roll-back Plan: A documented recovery plan must be established for every change. This plan is required to ensure that the system can be promptly

restored to its original stable state in the event of failure or if the implementation does not proceed as intended.

3) Isolation: Direct modification or testing within the Production Environment is strictly prohibited. All changes must be fully executed and verified in a dedicated Test or Staging Environment, with successful results confirmed before promotion to the live system.

4) Logging: Comprehensive records of all change activities must be maintained, including details of the requester, the approver, the date of implementation, and a description of the modifications. This documentation is mandatory to facilitate retrospective Audit and compliance reviews.

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.