PERSONAL DATA PROTECTION POLICY

Version 1/2025 VNG-GOV-PDP-PL-01
Effective Date: 11 November 2025

VANACHAI GROUP

Personal Data Protection Policy
Vanachai Group Public Company Limited and Subsidiaries

Vanachai Group Public Company Limited and its subsidiaries ("the Company") recognize the importance of protecting the personal data of all stakeholders, including employees, customers, business partners, shareholders, and any individuals involved in the Company's operations. The collection, use, disclosure, or processing of personal data must be conducted transparently, lawfully, and with due respect for the privacy rights of data subjects.

The Company is committed to conducting its business with integrity, transparency, and social responsibility, in compliance with the Personal Data Protection Act B.E. 2562 (2019) and applicable international standards, including FTSE Russell's Social Pillar (SHR07: Data Privacy). The Company ensures that personal data is managed appropriately, with robust security measures to mitigate data protection risks and minimize the likelihood of data breaches.

This policy has been established to define the Company's approach to personal data management in alignment with global data privacy principles. It serves as a governance framework for employees and relevant parties, aiming to provide assurance to stakeholders that their personal data will be collected, used, and disclosed only for the specified purposes, and protected against unauthorized access, use, or disclosure.

The Company fosters a data privacy-oriented culture, emphasizing the importance of information security and personal data protection. It assigns clear roles and responsibilities across all organizational levels and has appointed a Data Protection Officer (DPO) to oversee and monitor compliance with data protection laws. Moreover, this Personal Data Protection Policy is integrated with the Company's Information Confidentiality Policy and Information Security Policy, ensuring a comprehensive data governance system encompassing security, accuracy, and privacy.

1) Objectives

- This Personal Data Protection Policy is established to define the framework for the Company's personal data management in accordance with the Personal Data Protection Act B.E. 2562 (PDPA) and relevant international standards. The objective is to ensure that the collection, use, disclosure, and storage of personal data is conducted lawfully, transparently, and responsibly for all stakeholders.
- The policy also ensures consistency and integration with the Confidentiality Policy and IT Security Policy. The Company has set the following key objectives:
- To ensure personal data management complies with applicable laws and international standards;

- To establish effective control systems and risk mitigation measures for personal data protection;
- To clearly define the rights and responsibilities of data subjects;
- To assign roles and responsibilities to personnel at all organizational levels;
- To promote an organizational culture that prioritizes data security and privacy.

2) Policy Alignment and International Standards

This policy aligns with the principles of Good Corporate Governance and internationally recognized standards on human rights, privacy, and information security. It aims to ensure that the Company manages personal data in a transparent, auditable manner that respects the rights of all stakeholders; thereby building long-term trust and confidence in the organization.

The policy references the following key frameworks and standards:

- **Global Reporting Initiative GRI 207 Tax 2019:**
  - **GRI 418:** Customer Privacy – Governs customer and stakeholder data protection, data breach response, and disclosure of data privacy performance.
  - **GRI 102-43 & 102-44 –** Stakeholder engagement and the handling of privacy-related complaints.
- **Thailand's Personal Data Protection Act B.E. 2562 (PDPA):** Provides legal requirements for the lawful collection, use, disclosure, and retention of personal data, while defining data subject rights and penalties for non-compliance.
- **ISO/IEC 27701:** Privacy Information Management System (PIMS): An extension of ISO/IEC 27001 focusing on privacy and the establishment of a structured, auditable privacy management system.
- **OECD** *(Organization for Economic Co-operation and Development)* **Guidelines:**
  - **Guidelines on the Protection of Privacy and Transborder Flows of Personal Data:** An international framework for secure and transparent cross-border data transfers under appropriate oversight.
- **UN Global Compact – Principles 1 and 10:** Promotes the protection of fundamental human rights including individual privacy, and supports responsible, transparent business practices.
- **Securities and Exchange Commission (SEC) & Stock Exchange of Thailand (SET) Governance Code:** Encourages listed companies to practice transparency, information security, and fairness in data governance for all stakeholders.
- **FTSE Russell ESG Indicators:**
  - SHR07: Social Pillar – Data Privacy – Requires companies to establish clear policies and processes covering the collection, use, access, retention, deletion, and transfer

of personal data. This includes secure complaint mechanisms, audit procedures for data breaches, and appointment of a Data Protection Officer (DPO) to ensure compliance with relevant laws and standards.

(Aligned with FTSE Russell SHR07, GRI 418, ISO/IEC 27701, Thailand PDPA B.E. 2562, OECD Guidelines, UNGC Principles 1 & 10, and SDGs 9, 12, 16, 17)

3) Scope

This policy applies to:

- **All levels of Company personnel:** Including directors, executives, full-time and contract employees, temporary workers, interns, and any individuals acting on behalf of the Company, such as consultants or external contractors who access or process personal data as part of the Company's operations.
- **All business units and facilities:** Encompassing factories, headquarters, distribution centers, support units, and subsidiaries both domestically and internationally, as well as IT systems and cloud platforms used for storing or processing personal data.
- **All stakeholder groups whose personal data is directly or indirectly related to the Company:** Including shareholders, employees, customers, consumers, job applicants, business partners, suppliers, creditors, government agencies, communities, business contacts, and any third parties whose personal data is collected, used, or disclosed by the Company.
- **All Company activities involving the collection, use, disclosure, transfer, or storage of personal data:** Whether in physical documents, electronic records, or digital formats through IT systems, online platforms, or offline channels of any kind.
- **Personal data management, communications, and response to data subject rights:** Including data breach management, complaints handling, and actions taken in compliance with applicable personal data protection laws.

  (Aligned with GRI 418: Customer Privacy, FTSE Russell SHR07: Data Privacy, ISO/IEC 27701, Thailand PDPA B.E. 2562, and SDG 16 – Peace, Justice and Strong Institutions)

4) Definitions and References

- **Personal Data:** Any information that can directly or indirectly identify a natural person, such as full name, national ID number, address, phone number, email, biometric data, or any other data that can be associated with an individual.
- **Data Subject:** A natural person who owns the personal data collected, used, or disclosed by the Company. This includes employees, customers, job applicants, business partners, or any individuals associated with the Company's operations.

- **Data Controller:** A person or legal entity with the authority and responsibility to make decisions regarding the collection, use, or disclosure of personal data.
- **Data Processor:** A person or legal entity that collects, uses, or discloses personal data on behalf of or as instructed by the Data Controller.
- **Data Collection:** The act of obtaining personal data from the data subject directly or from other sources, whether in physical or electronic form.
- **Data Processing:** Any activity performed on personal data, such as collection, storage, use, transfer, analysis, or destruction.
- **Cross-Border Data Transfer:** The act of transmitting or disclosing personal data to a foreign country, or allowing foreign entities to access such data.
- **Data Breach:** An incident involving unauthorized access, use, disclosure, or loss of personal data that may impact the rights and freedoms of the data subject.
- **Data Protection Officer (DPO):** An individual appointed by the Company to oversee, advise on, monitor, and report on activities related to personal data protection to ensure compliance with applicable laws and Company policies.
- **Vanachai Integrated Materiality and Risk Assessment (V-IMRA):** An internal assessment framework used by the Company to identify, assess, and prioritize sustainability-related impacts, risks, and opportunities across its operations and value chain. V-IMRA integrates both impact materiality and financial materiality considerations and provides structured inputs to the Enterprise Risk Management (ERM) system, strategic planning, and management decision-making.
  (Aligned with FTSE Russell SHR07, GRI 418, ISO/IEC 27701, Thailand PDPA B.E. 2562, OECD Guidelines, and SDG 16 – Peace, Justice and Strong Institutions)

5) Governance and Accountability

- **Board of Directors:** Responsible for approving and overseeing the Personal Data Protection Policy, setting strategic direction and operational guidelines for personal data management in alignment with the Personal Data Protection Act B.E. 2562 (PDPA) and international standards. The Board ensures that the Company collects, uses, discloses, and retains personal data lawfully, securely, transparently, and with full respect for the rights of all stakeholders.
- **Audit Committee:** Monitors, reviews, and evaluates the effectiveness of the implementation of the Personal Data Protection Policy. This includes reviewing the adequacy of internal control measures related to personal data management and reporting findings and recommendations to the Board of Directors to enhance operational efficiency.
- **Risk Management and Corporate Governance Committee:** Oversees the integration of personal data protection into the Enterprise Risk Management (ERM) system and

monitors performance in data security and the prevention of personal data breaches. The committee ensures the Company can prevent, mitigate, and respond effectively to incidents that may impact personal data.

- **Data Protection Officer (DPO):** Responsible for implementing data security measures and technical safeguards to prevent unauthorized access, use, or disclosure of personal data. Responsibilities include data backups, encryption, and system audits as outlined in the Company's cybersecurity roadmap.
- **Information Technology Department:** Oversees the execution of technical security measures to ensure the confidentiality, integrity, and availability of personal data. This includes implementing encryption, data backup systems, and monitoring mechanisms aligned with the Company's cybersecurity framework.
- **All Employees:** Are obligated to strictly adhere to the Personal Data Protection Policy by:
  - Understanding the principles of personal data protection and complying with the Company's data confidentiality and security protocols;
  - Performing duties with due diligence and refraining from disclosing or transferring personal data without authorization;
  - Reporting any suspected or actual data breaches to supervisors or the DPO without fear of retaliation;
  - Cooperating with relevant units in transparent investigations and resolution of incidents;
  - Supporting a culture that prioritizes data security and privacy at all levels of the organization.

(Aligned with FTSE Russell SHR07 – Data Privacy and Protection Oversight, GAC07 – Board Oversight and Ethical Governance, GRI 418: Customer Privacy, ISO/IEC 27701, and SDG 16 – Peace, Justice and Strong Institutions)

6) Commitments and Principles

The Company is committed to conducting business with integrity, transparency, and social responsibility, upholding the principles of privacy and personal data protection in accordance with applicable laws and international standards. These commitments aim to foster stakeholder trust and are guided by the following principles:

6.1 Compliance with Laws and International Standards *(FTSE Russell SHR07, GRI 418, PDPA B.E. 2562, SDG 16.10)*:

- The Company complies with the Personal Data Protection Act B.E. 2562 (PDPA), including all relevant laws, regulations, and regulatory requirements at both national and international levels concerning personal data protection.

- It adopts international standards and best practices such as FTSE Russell SHR07 – Data Privacy, GRI 418 – Customer Privacy, ISO/IEC 27701 – Privacy Information Management System (PIMS), OECD Privacy Guidelines, and the UN Global Compact Principle 1 to enhance its data governance framework to global standards.
- The Company promotes strict adherence to these standards among employees and business partners by providing ongoing communication and training on personal data protection.

6.2 Data Protection and Risk Mitigation *(FTSE Russell SHR07, ISO/IEC 27701, GRI 418-1, SDG 16.6):*

The Company conducts annual personal data risk assessments and integrates the findings into its Enterprise Risk Management (ERM) system to identify, evaluate, and manage risks associated with data collection, use, and disclosure.

- Robust internal control measures are in place to prevent unauthorized access, use, or disclosure of personal data, including access logs to ensure traceability and auditability.
- In the event of a data breach, the Company follows a clearly defined incident response procedure and notifies the regulatory authority and affected data subjects within the legally prescribed timeframe to mitigate impacts and prevent recurrence.

6.3 Respect for Data Subject Rights *(FTSE Russell SHR07, GRI 418-1, PDPA Sections 30–35, SDG 16.7)*:

- The Company upholds data subject rights in accordance with legal provisions, including the right to access, rectify, delete, restrict processing, or withdraw consent.
- Clear communication channels and processes are in place to receive and process data subject requests. The Data Protection Officer (DPO) serves as the main point of contact for verification and resolution of such requests.
- Transparency is emphasized through the publication of the Company's Privacy Policy and Privacy Notices on its website at www.vanachai.com
- , enabling data subjects to understand the purposes, methods, and their rights related to data processing.

6.4 Fostering a Culture of Data Security *(FTSE Russell SHR07, ISO/IEC 27001, SDG 9.5)*:

- The Company cultivates an organizational culture that prioritizes data security through regular training programs for employees at all levels on personal data protection, confidentiality, and responsible use of information technology.

- Information security is integrated into performance evaluations (KPIs) for relevant departments, reinforcing that data protection is a shared responsibility across the organization.

7) Risk, Impact, and Dependency Management

The risks, impacts, and dependencies associated with the matters addressed in this policy are identified, analyzed, and prioritized through the Company's Vanachai Integrated Materiality and Risk Assessment (V-IMRA) process. V-IMRA is an internal assessment framework that considers both impact materiality and financial materiality across the value chain.

- **The results of V-IMRA** are integrated into the Enterprise Risk Management (ERM) system to support policy formulation, strategic decision-making, the setting of risk appetite, and the creation of long-term sustainable value.
- **Risk Identification and Assessment:** The Company systematically identifies and assesses personal data protection risks across all processes involving the collection, use, disclosure, transfer, and storage of personal data, whether in physical or digital form. Particular focus is placed on sensitive stages such as the handling of data related to customers, employees, business partners, and job applicants. The objective is to detect potential data breach incidents or unauthorized access.

  Risk levels are assessed based on the severity of potential impact and the likelihood of occurrence. Prioritization is then used to define appropriate preventive control measures. This process is integrated into the Company's Enterprise Risk Management (ERM) framework to ensure continuous monitoring and effective mitigation of personal data risks.
- **Impact Assessment:** The Company assesses the potential impacts of personal data breaches or non-compliant data handling practices across multiple dimensions:
  - **Legal and Financial**: Exposure to lawsuits, regulatory fines, or compensation payments due to personal data breaches.
  - **Reputation and Trust**: Loss of trust among customers, shareholders, partners, and regulators, potentially undermining the Company's long-term reputation.
  - **Operational**: Disruptions to IT systems, loss of critical data, or system failures that impair business performance.
  - **Social and Stakeholder**: Violations of privacy rights that may result in emotional or social harm, weakening stakeholder confidence in the Company's responsible business conduct.

  These assessments are used to enhance internal controls, strengthen preventive measures, and improve incident response plans to ensure risk management remains effective and transparent.
- **Dependency Management and System Integration:** The Company recognizes that personal data management is closely linked with its IT Security Policy and Confidentiality

Policy. Therefore, these policies are integrated into a unified data protection framework—covering system design, access control, and secure data disposal after the end of the intended processing purpose.

Additionally, the Company relies on strong collaboration with its business partners to manage data-related risks. All vendors are required to comply with the Company's data protection standards and maintain equivalent information security protocols.

(Aligned with FTSE Russell SHR07 – Data Privacy and Protection, GAC07 – Governance Oversight, GRI 418-1, ISO/IEC 27701, and SDG 16 – Peace, Justice and Strong Institutions)

8) Targets and Metrics

The Company establishes clear objectives and Key Performance Indicators (KPIs) to continuously monitor and assess its personal data protection practices in a transparent and verifiable manner. These indicators cover prevention, detection, and incident response dimensions to ensure that the personal data of all stakeholders is appropriately and securely protected.

Short-Term Goals *(Within 1 Year):*

- 100% of employees must complete annual training on Personal Data Protection (PDPA Awareness Training) and Cybersecurity.
- All departments must conduct an annual personal data risk assessment and develop a Personal Data Risk Management Plan.
- The Company must formally appoint and announce a Data Protection Officer (DPO), with clearly defined roles and responsibilities.
- A secure, accessible, and confidential channel for reporting personal data breaches must be established and maintained.

Medium-Term Targets *(3–5 years):*

- Develop and certify the personal data management system in compliance with ISO/IEC 27701: Privacy Information Management System (PIMS).
- Conduct at least one internal audit annually on personal data management to ensure compliance with PDPA and internal protocols.
- 100% of business partners and vendors must be certified for Data Privacy Compliance.
- Enhance IT Security Systems to reduce the incident rate by at least 30% within 3 years.

Long-Term Targets *(5 years and beyond):*

- Achieve Zero Confirmed Data Breach Cases across all business operations.
- Be recognized as a Data Privacy Excellence Organization within the industry.
- Integrate data security and privacy into the Company's Core Values, fostering a culture that prioritizes information protection.

Key Performance Indicators

Category	Indicators	Monitoring Frequency	Responsible Unit
Prevention	% of employees completing PDPA & Cybersecurity Training	Annual	HR Department / IT Department
Detection	Number of reported data breach incidents identified and submitted to DPO	Quarterly	DPO / IT Security Team
Response	Average time to respond to and notify data breach incidents	Annual	DPO / Risk Management Committee
Compliance Monitoring	% of departments passing PDPA and Data Privacy Policy compliance audits	Annual	Internal Audit / Legal Department
Partner Engagement	% of business partners passing Data Privacy Compliance assessments	Annual	Procurement / Sustainability Development Task Force
Disclosure Transparency	Inclusion of personal data protection metrics in the Sustainability Report (GRI 418)	Annual	Sustainability Committee / Sustainability Development Task Force

- **Integration with Executive and Organizational Performance:** Personal data protection KPIs will be incorporated into the performance evaluations of senior executives (Executive KPIs) and organizational performance assessments. This ensures shared accountability for transparent, effective personal data management that aligns with the Company's long-term sustainability strategy.

(Aligned with FTSE Russell SHR07 – Data Privacy and Protection, GRI 418 – Customer Privacy, ISO/IEC 27701, Thailand PDPA B.E. 2562, and SDG 16.10 – Access to Information)

9) Supply Chain and Partner Responsibility

- **Partner Selection and Evaluation** *(FTSE Russell SHR07, GRI 418-1, ISO/IEC 27701, SDG 16.6):* The Company assesses and selects business partners involved in the collection, processing, or access to personal data based on key criteria such as ethics, data security, and compliance with personal data protection laws. Particular attention is given to IT service providers, cloud providers, and third parties with access to personal data. Prior to engagement, the Company conducts Data Privacy Compliance Due Diligence and requires all partners to sign a Data Processing Agreement (DPA) to formally establish data protection responsibilities and safeguards.
- **Compliance with the Supplier Code of Conduct** *(FTSE Russell SHR07, GRI 102-16, SDG 8.7, SDG 12.6)***:** All business partners are required to comply with the Company's Supplier Code of Conduct and Personal Data Protection Policy, which include the following principles:

- Compliance with applicable data protection laws and data security standards
- Collection, use, and disclosure of personal data only as necessary and with proper consent from data subjects
- Implementation of technical measures such as encryption, access controls, and audit trails
- Immediate notification to the Company in the event of a data breach, to enable timely incident response

The Company reserves the right to audit or request documentation to verify compliance. Any breach or failure to meet standards may result in suspension of services or immediate termination of the business relationship.

- **Training and Capacity Building** *(FTSE Russell SHR07, GRI 205-2, SDG 17 – Partnerships for the Goals):* The Company encourages partners and business affiliates to deepen their knowledge of personal data protection through training, informational updates, or collaborative workshops. The goal is to align all parties with the Company's data security standards and promote adoption of new technologies that enhance information security across the supply chain.
- **Audit and Monitoring** *(FTSE Russell SHR07, GRI 418-1, SDG 16.10)***:** Ongoing monitoring and audits are conducted to evaluate partners' compliance with personal data protection requirements. This may include site visits, document reviews, or IT system inspections to ensure implementation of appropriate safeguards. Findings are reported to the Risk Management and Audit Committees for strategic review and continuous improvement.
- **Fostering a Responsible Business Network** *(FTSE Russell SHR07, GRI 102-43, SDG 17 – Partnerships for the Goals)***:** The Company seeks to build a partner ecosystem that prioritizes data security and privacy rights. Business partners are encouraged to participate in a Privacy and Data Ethics Commitment to raise industry transparency standards. The Company also collaborates with government bodies, trade associations, and international organizations to exchange best practices in personal data protection.

10) Integration with Corporate Strategy

The Company integrates its Personal Data Protection Policy into its overall operational strategy under the "Forest | Future | Together – for a Sustainable Living" framework—its core vision for achieving a balance between business growth, environmental responsibility, and respect for the human rights of all stakeholders. This policy serves as a key mechanism for strengthening trust, transparency, and governance in the digital era.

- **Forest – Governance and Environmental Responsibility:** The Company manages personal data based on the principles of transparency, security, and accountability—paralleling its commitment to sustainable resource use within the supply chain. The Company aims to minimize the environmental impact of digital technologies and data systems involved in personal data

processing, ensuring alignment with its environmental and governance principles.

- **Future – Innovation and Sustainable Data Management:** The Company develops personal data management systems aligned with modern technologies, such as cloud platforms, data encryption, and AI-powered security tools. These systems enhance data efficiency, reduce cybersecurity risks, and ensure compliance with relevant laws and standards including Thailand's PDPA B.E. 2562, ISO/IEC 27701, and FTSE Russell SHR07.
  Additionally, the Company promotes innovation in data ethics, enabling employees and partners to understand ethical data usage, respect privacy rights, and apply data transparently for business value.
- **Together – Stakeholder Collaboration for Elevated Data Standards:** The Company emphasizes collaboration with employees, partners, customers, government agencies, and communities to co-develop secure, comprehensive, and auditable data management mechanisms. It implements regular training, communication, and awareness activities to involve all stakeholders in fostering a shared culture of Data Privacy and Cybersecurity Responsibility, ensuring ethical and transparent data use across the supply chain.

This Personal Data Protection Policy is also integrated with:

- **Corporate Sustainability Strategy**: To align data governance with the Company's goals in governance (G) and social responsibility (S) under its broader ESG commitments.
- **Enterprise Risk Management** *(ERM):* By incorporating data protection risks into the Company's technology and cybersecurity risk frameworks, enabling effective monitoring, control, and response.
- **ESG Performance Assessment:** Personal data protection performance is used as part of the Company's governance (G) indicators in ESG evaluations under FTSE Russell and GRI Standards, demonstrating its commitment to transparent and rights-respecting digital business practices.
  (Aligned with FTSE Russell SHR07 – Data Privacy, GRI 418 – Customer Privacy, ISO/IEC 27701, PDPA B.E. 2562, UNGC Principle 1, and SDGs 9, 16, and 17.)

11) Implementation and Management Tools

- **Data Privacy Management System** *(DPMS)*: The Company has established a Data Privacy Management System aligned with the Personal Data Protection Act B.E. 2562 (PDPA) and ISO/IEC 27701 standards. This system governs all processes including the collection, use, disclosure, transfer, and disposal of personal data. It includes protocols for access control, audit trails, and authorization processes, ensuring full traceability at every stage.
- **Consent Management System**: A consent management platform has been developed to ensure that the collection and use of personal data is conducted with clear, transparent, and verifiable consent. This system maintains consent records and allows data subjects to withdraw consent at any time through designated channels.

- **Information Security Tools:** The Company protects personal data through an Information Security Management System (ISMS) in accordance with ISO/IEC 27001. Key tools include:
  - **Data Encryption**: Safeguards against unauthorized access and disclosure of data.
  - **Intrusion Detection & Prevention System** *(IDPS):* Monitors and mitigates cybersecurity threats.
  - **Backup and Recovery System:** Ensures data can be restored in case of unexpected incidents.
  - **Identity & Access Management** *(IAM)*: Controls data access rights based on employee roles and responsibilities.
- **Data Breach Response Plan:** The Company has implemented a Data Breach Response Plan to handle incidents swiftly and effectively. This includes:
  - Initial detection and assessment of the incident
  - Containment and mitigation of potential damage
  - Timely reporting to the Data Protection Officer (DPO) and regulatory authorities as required by law
  - Notification to affected data subjects
  - Root cause analysis and documentation of lessons learned to prevent recurrence
- Training and Awareness Program: Ongoing training is provided to all employees to build awareness and competency in data privacy and information security. Training is delivered through in-house sessions, e-learning modules, and hands-on workshops, reinforcing proper understanding of roles and compliance with this policy.
- Monitoring & Audit Tools: The Company has developed tools such as a Privacy Dashboard and a Compliance Monitoring System to help relevant departments track policy adherence, analyze risk trends, and report regularly to the Risk Management Committee and Audit Committee.
- Partner Coordination Mechanism: Communication channels are in place to collaborate with business partners and vendors that process personal data. These cover security information exchange, incident alerts, and preventive measures. Any engagement involving personal data must undergo prior review and approval by the DPO and Legal Department.
  (Aligned with FTSE Russell SHR07 – Data Privacy, GRI 418 – Customer Privacy, ISO/IEC 27701, ISO/IEC 27001, and SDGs 9, 16 – Peace, Justice and Strong Institutions.)

12) Monitoring, Reporting and Transparency

- **Monitoring:**
  - The Company monitors compliance with the Personal Data Protection Policy across all departments through internal audits and compliance reviews at least once annually, to assess preparedness, risk levels, and the effectiveness of current safeguards.

- The Data Protection Officer (DPO) is responsible for auditing, monitoring, and reporting on the status of personal data protection operations to the Risk Management Committee and Audit Committee.
- Digital tools such as the Privacy Dashboard and Incident Reporting System are used to monitor, record, and review incidents of personal data access or breaches in a transparent and systematic manner.

- **Reporting:**
  - The Company prepares an annual performance report on data protection and includes it in its Sustainability Report, aligned with GRI 418 – Customer Privacy and FTSE Russell SHR07 – Data Privacy standards.
  - In the event of a Data Breach, the Company will report to the Office of the Personal Data Protection Committee (PDPC) and notify affected data subjects within the legal timeframe, disclosing corrective actions and preventive measures with full transparency.
  - Personal data protection and cybersecurity performance will be reported to the Audit Committee and presented to the Board of Directors at least once a year, supporting strategic policy decisions and future development planning.
- **Transparency and Disclosure to Stakeholders:**
  - The Company operates transparently by disclosing its Data Privacy Policy and Privacy Notice through the official website www.vanachai.com, enabling stakeholders to access and understand data practices clearly.
  - Dedicated channels are provided for complaints, inquiries, and data subject rights requests, both online and via responsible departments. All complaints are fairly investigated and handled under DPO supervision.
  - The Company commits to full transparency by not concealing any personal data breach incidents and by promptly disclosing the facts and taking corrective action to maintain the trust of shareholders, customers, partners, employees, and the community.
- **Continuous Improvement and Review:**
  - Insights from monitoring and reporting activities are analyzed to improve the personal data management process, incorporating real-world lessons and emerging technologies.
  - The Company reviews the effectiveness of its Data Protection System at least once annually to ensure alignment with legal changes, evolving risks, and cybersecurity trends.

(Aligned with FTSE Russell SHR07 – Data Privacy and Protection, GRI 418 – Customer Privacy, ISO/IEC 27701, PDPA B.E. 2562, and SDG 16 – Peace, Justice and Strong Institutions.)

13) Review and Continuous Improvement

- **Periodic Review:**
  - The Company requires a review of the Personal Data Protection Policy at least once annually or upon any changes in applicable laws, regulations, or standards—such as the Personal Data Protection Act B.E. 2562 (PDPA), ISO/IEC 27701, or FTSE Russell SHR07 criteria.
  - The review is conducted by the Data Protection Officer (DPO) in collaboration with the Risk Management and Corporate Governance Committee, to assess the policy's adequacy and effectiveness and to propose any necessary revisions to the Board of Directors for approval.
- **Continuous Improvement Mechanism:**
  - The Company is committed to continuously enhancing its Data Privacy Management System (DPMS) to address emerging cyber threats and risks, integrating findings from internal audits and risk assessments into the development of improved technical safeguards and internal controls.
  - Feedback from stakeholders, business partners, and regulatory agencies is actively analyzed to refine policies and processes, promoting organizational learning and adaptation in the realm of data privacy.
  - Employees and relevant departments are encouraged to propose innovative ideas for personal data protection, fostering a corporate culture of learning and sustainable development.
- **Emerging Standards and Technology Tracking:**
  - The Company monitors technological and legal trends related to data privacy both domestically and internationally—such as guidelines from the Office of the Personal Data Protection Committee (PDPC) and standards from international bodies (e.g., ISO)—to keep policies and practices up to date.
  - Consideration is given to adopting new tools and technologies, such as Automated Risk Assessment systems or Advanced Encryption Technologies, to strengthen data security management.
- **Stakeholder Engagement for Improvement:**
  - The Company provides opportunities for both internal and external stakeholders to contribute feedback on data privacy practices through communication channels and online surveys. This input is used to enhance operational processes and elevate data security standards on an ongoing basis.
  - The Company is committed to upholding the highest standards in personal data management, viewing data protection not merely as a legal obligation, but as a core element of its corporate culture of governance, transparency, and sustainability.

(Aligned with FTSE Russell SHR07 – Data Privacy and Protection, GRI 418 – Customer Privacy, ISO/IEC 27701, PDPA B.E. 2562, and SDG 16 – Peace, Justice and Strong Institutions)

14) Personal Data Protection Policy Revision History

Version	Date	Policy Owner	Approved by	Key Changes / Comments
1.0	11 November 2025	Risk Management and Corporate Governance Committee / Sustainability Committee / Data Protection Officer (DPO)	Board of Directors	Issuance and implementation of the first Personal Data Protection Policy. This version integrates the Confidentiality Policy and the IT Security Policy to establish a unified framework for managing personal data, encompassing legal compliance, information security, and data subject rights. The policy has been aligned with the PDPA, ISO/IEC 27701, and FTSE Russell SHR07 to support the Company's digital transformation strategy effectively.

This policy is approved and issued for acknowledgement and implementation by all relevant parties.