INFORMATION TECHNOLOGY SECURITY POLICY

Version 2/2026 VNG-GOV-ITS-PL-02

Effective Date: 10 August 2026

VANACHAI GROUP

Information Technology Security Policy
Vanachai Group Public Company Limited and Subsidiaries

Vanachai Group Public Company Limited and its subsidiaries (the "Company") recognize that information technology, cloud computing, digital data, applications, networks and information systems are critical business assets that support manufacturing operations, procurement, logistics, sales, customer service, governance, sustainability reporting and business continuity.

The Company is committed to protecting information technology systems and information assets against unauthorized access, misuse, loss, disclosure, alteration, disruption, cyberattacks, privacy breaches and other threats that may affect business operations, stakeholders, reputation and legal compliance.

This Policy establishes a governance and control framework for managing information technology security across the Company. It promotes confidentiality, integrity, availability, accountability, privacy, resilience, lawful use and responsible digital conduct. The Company also places strong emphasis on cloud security, data backup, recovery capability, business continuity, incident response and third-party information security management.

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

1) Objectives

- Establish principles, rules and responsibilities for the secure management and use of information technology systems and information assets.
- Protect the confidentiality, integrity and availability of the Company's data, applications, networks, cloud services, devices and information systems.
- Prevent unauthorized access, cyber intrusion, malware infection, ransomware, data leakage, loss of information, system disruption and misuse of IT resources.
- Promote lawful, ethical and responsible use of information technology in compliance with applicable laws, regulations, contracts, internal policies and recognized information security standards.
- Strengthen data privacy protection for employees, customers, suppliers, business partners and other stakeholders.
- Support cyber resilience, incident response, backup, recovery and business continuity for critical systems and business processes.
- Build security awareness and accountability among employees, users, contractors, service providers and relevant business partners.

2) Policy Alignment and International Standards

- ISO/IEC 27001:2022 Information Security Management Systems and ISO/IEC 27002:2022 Information Security Controls, where applicable to the Company's context and maturity.
- ISO/IEC 27017 for information security controls for cloud services and ISO/IEC 27018 for protection of personally identifiable information in public cloud environments, where applicable.
- NIST Cybersecurity Framework 2.0, including the core functions of Govern, Identify, Protect, Detect, Respond and Recover.
- ISO 22301 Business Continuity Management Systems, where information technology continuity and recovery support critical business processes.
- Thailand Personal Data Protection Act B.E. 2562, Thailand Cybersecurity Act B.E. 2562, Computer Crime Act B.E. 2550 and amendments, Electronic Transactions Act and other applicable laws and regulations.
- SEC and SET corporate governance expectations relating to risk management, internal control, data protection, business continuity and responsible disclosure, where applicable.
- GRI Standards: GRI 2-23 Policy Commitments, GRI 2-24 Embedding Policy Commitments, GRI 2-27 Compliance with Laws and Regulations, and GRI 3-3 Management of Material Topics 2021.
- FTSE Russell ESG Indicators relating to corporate governance, risk management, data privacy, cybersecurity, internal controls and supply chain governance, where applicable.
- The Company's Code of Conduct, Data Privacy Notice, Business Continuity Management Policy, risk management framework and other relevant internal policies and procedures.

3) Scope of the Policy

This policy applies to:

- This policy applies to the Company, its subsidiaries and joint ventures under the Company's operational control.
- This policy applies to directors, executives, employees, temporary staff, interns, contractors, consultants, outsourced personnel and all users who access or use the Company's information technology systems or information assets.
- This policy applies to suppliers, service providers, cloud service providers, software vendors, system integrators and business partners that connect to, process, store, transmit or manage the Company's data or information systems.

- This policy covers all information technology assets and services, including computers, mobile devices, servers, networks, databases, applications, email, internet access, cloud platforms, backup systems, security tools, user accounts, privileged accounts, access logs and electronic records.
- This policy applies to information throughout its life cycle, including creation, collection, classification, use, storage, transmission, sharing, backup, retention, archiving, disposal and destruction.

4) Definitions and References

To ensure a consistent understanding and application of this Information Technology Security Policy the following key terms are defined as follows.

- **Information Technology Security:** The protection of information systems, digital assets and technology services from unauthorized access, misuse, disruption, modification, disclosure or destruction.
- **Information Asset:** Data, documents, software, systems, applications, databases, hardware, networks, cloud services, credentials, logs and other resources that create value for the Company.
- **Confidentiality, Integrity and Availability:** Core security principles requiring that information is accessed only by authorized parties, remains accurate and complete, and is available when needed for authorized business use.
- **User:** Any person authorized to access or use the Company's information technology systems or information assets.
- **System Administrator:** A person or function authorized to manage, configure, monitor or maintain IT systems, networks, servers, cloud services, accounts or security controls.
- **Authentication:** A process for verifying the identity of a user, device or system before access is granted.
- **Authorization:** A process for determining what information, system functions or activities a user is permitted to access or perform.
- **Accountability and Logging:** The ability to trace activities to users, systems or processes through records such as access logs, application logs, security logs and audit trails.
- **Privileged Access:** Elevated system access that allows administrative, configuration, approval, security or high-impact system actions.
- **Personal Data:** Information relating to an identifiable person, as defined by applicable personal data protection laws.

- **Cloud Security:** Security controls applied to cloud services, including identity management, data protection, encryption, monitoring, backup, recovery and vendor security management.
- **Cybersecurity Incident:** An actual or suspected event that may compromise information systems, data, networks, cloud services, business operations, confidentiality, integrity or availability.
- **Backup and Recovery:** Processes and controls for copying, storing, protecting, testing and restoring information systems and data after disruption, loss or damage.
- **Vanachai Integrated Materiality and Risk Assessment (V-IMRA):** The Company's internal process for identifying and prioritizing sustainability, governance and business risks by integrating impact and financial materiality perspectives to support enterprise risk management, strategic planning and decision-making.

5) Governance and Accountability

- **Board of Directors:** Approves this policy and oversees the Company's strategic direction, governance, risk management and internal control relating to information technology security and data protection.
- **Risk Management and Governance Committee:** Oversees significant cybersecurity, information security, technology continuity and data privacy risks, including integration with the Company's enterprise risk management framework.
- **Audit Committee:** Reviews the adequacy and effectiveness of relevant internal controls, audit findings and corrective actions relating to information technology security and data protection.
- **Managing Director and Management:** Ensure that sufficient resources, budget, personnel, technologies, procedures and management support are provided for the implementation of this policy.
- **Information Technology Department:** Serves as the policy owner and lead function responsible for implementing security controls, managing IT assets, user access, cloud services, network and server security, backup, recovery, security monitoring and incident response.
- **Internal Audit:** Conducts independent audits or reviews to assess compliance with this policy and the effectiveness of IT controls, and reports findings to the relevant governance body.
- **Department Heads and Data Owners:** Identify business requirements, approve access rights, classify information, ensure appropriate use of systems and support security controls in their respective areas.

- **Employees and Users:** Comply with this policy, protect credentials and Company information, use IT resources responsibly, report suspected incidents and complete required training.
- **Suppliers, Contractors and Service Providers:** Comply with contractual information security, confidentiality, privacy and incident reporting requirements when accessing or managing the Company's information assets.

6) Commitments and Principles

6.1 Legal Compliance and Security Governance

- Comply with applicable laws, regulations, contracts and internal policies relating to information technology, cybersecurity, personal data protection, electronic transactions and computer-related offences.
- Maintain an information security governance framework based on risk assessment, defined responsibilities, management oversight, documented procedures, internal controls and continuous improvement.
- Apply the principle of accountability by ensuring that access, changes, approvals and critical activities can be traced and reviewed through appropriate logs and records.

6.2 Identity, Authentication and Access Control

- Require user identification, authentication and authorization before access to Company systems is granted.
- Apply least privilege, segregation of duties and need-to-know principles to access rights, especially for confidential data and privileged accounts.
- Use appropriate authentication controls, such as user ID and password, multi-factor authentication, OTP, biometric verification, secret keys or tokens, depending on system risk and data sensitivity.
- Review user access rights at least annually, or when employees resign, transfer, change roles or no longer require access.

6.3 Information Asset and Acceptable Use Management

- Maintain an inventory of critical IT assets, systems, applications, devices and information assets with assigned ownership and responsibility.
- Use Company computers, devices, networks, email, internet and applications for authorized business purposes and in accordance with applicable policies.
- Prohibit unauthorized installation, modification, copying or use of software, including unlicensed software, hacking tools, malware tools or software unrelated to work.
- Require users to protect Company devices from loss, damage, misuse, unauthorized connection and improper storage conditions.

6.4 Data Classification, Privacy and Encryption

- Classify information based on business value, sensitivity, legal requirements and access restrictions.
- Protect personal data, confidential business information, financial information, employee information, customer data and supplier data through appropriate technical and organizational measures.
- Use encryption or secure communication methods, such as SSL, TLS, VPN or other appropriate mechanisms, for sensitive data transmission over public or shared networks.
- Collect, use, disclose, retain and delete personal data in accordance with the Company's Data Privacy Notice and applicable personal data protection laws.

6.5 Network, Server, Endpoint and Cloud Security

- Manage networks, servers and cloud services using secure configuration, access control, monitoring, logging, malware protection and regular security updates.
- Segment networks by system sensitivity, service type and user group, including internal zones, external zones and restricted administrative zones, where appropriate.
- Control the connection of personal or external devices to the Company's network and prohibit unauthorized changes to routers, switches, IP addresses, servers or network equipment.
- Apply cloud security controls, including authorized access, encryption, activity monitoring, security auditing, backup, recovery and periodic risk assessment.

6.6 Backup, Recovery and Business Continuity

- Establish backup and recovery procedures for critical systems, software and data based on business importance, risk and recovery requirements.
- Store backup data securely, protect it from unauthorized access and periodically test restoration to ensure that recovery can be performed within acceptable timeframes.
- Maintain IT continuity and disaster recovery readiness to support the Company's Business Continuity Management framework and critical business processes.

6.7 Internet, Email and Malware Protection

- Require secure password practices and prohibit sharing of passwords, OTPs, tokens or personal credentials with other persons.
- Use antivirus, anti-malware, email security, firewall, web security or equivalent controls to reduce risks from phishing, malicious websites, suspicious files and unauthorized downloads.
- Prohibit the use of Company email, internet, intranet or communication tools for illegal, offensive, defamatory, harassing, fraudulent or non-business purposes.

6.8 Physical and Environmental Security

- Control physical access to rooms, areas or locations where critical IT equipment, servers, network devices or backup media are stored.
- Protect critical IT assets from fire, flood, overheating, power interruption, humidity, dust, physical damage and other environmental threats through appropriate safeguards such as fire protection, UPS, access control and secure storage.
- Review physical and environmental controls periodically to ensure that they remain suitable for the Company's technology environment.

6.9 Incident Reporting, Response and Escalation

- Require employees, users and relevant parties to immediately report suspected cybersecurity incidents, abnormal system behavior, malware infection, data loss, unauthorized access or other IT security concerns.
- Operate an incident reporting and escalation process through the IT Service Center or designated channel, including administrator@vanachai.com, for receiving, assessing, escalating, resolving and tracking incidents.
- Investigate incidents, contain impacts, recover affected systems, communicate to relevant parties and implement corrective actions to prevent recurrence.

6.10 Prohibited Conduct and Enforcement

- Prohibit unauthorized access, password sharing, impersonation, data theft, unauthorized copying, disclosure of confidential information, deliberate system disruption, use of hacking tools and cooperation with unauthorized external parties to access Company systems.
- Prohibit negligent conduct that may expose Company information or systems to unauthorized access, disclosure, damage or loss.
- Violations of this policy may result in disciplinary action, including verbal warning, written warning, suspension, termination, dismissal and/or civil or criminal legal action, depending on the severity of the violation.

7) Risk, Impact, and Dependency Management

- Information technology security risks, impacts and dependencies are identified, analyzed and prioritized through the Company's Vanachai Integrated Materiality and Risk Assessment (V-IMRA) process and integrated into the Enterprise Risk Management (ERM) system.
- Risk assessment shall consider cyber threats, unauthorized access, malware, ransomware, data leakage, privacy breaches, cloud service disruption, third-party system failures, network outages, human error, physical security threats and business interruption.

- The Company shall identify critical systems, critical data, process dependencies, cloud dependencies, third-party dependencies, recovery priorities and potential impacts on operations, customers, suppliers, employees, regulators and reputation.
- Risk treatment plans shall include appropriate preventive, detective, corrective and recovery controls, including access control, encryption, monitoring, vulnerability management, patch management, backup, disaster recovery, incident response and supplier risk management.
- Major cybersecurity incidents, audit findings, risk events and control failures shall be reviewed, remediated and used as lessons learned for continuous improvement.

8) Targets and Metrics

- Percentage of critical information systems and information assets covered by an updated asset inventory and assigned system owners.
- Percentage of user access rights and privileged accounts reviewed at least annually or upon role change, transfer, resignation or contract termination.
- Percentage of employees and relevant users completing information security and data privacy awareness training.
- Percentage of critical systems with backup and recovery procedures tested within the defined review cycle.
- Number and severity of cybersecurity incidents, data privacy incidents, malware events, unauthorized access events and service interruptions.
- Mean time to acknowledge, contain, resolve and close cybersecurity incidents according to the incident response process.
- Percentage of critical vulnerabilities remediated within the timeframe defined by risk severity.
- Percentage of critical IT service providers, cloud providers and vendors assessed for information security and data privacy controls.
- Annual reporting of information technology security performance, major risks and improvement actions to the appropriate governance bodies.

9) Supply Chain and Partner Responsibility

- The Company recognizes that suppliers, contractors, customers, research institutions, technology providers, and business partners may play an important role in developing and scaling innovation. The Company shall manage collaboration responsibly to ensure mutual benefit, confidentiality, compliance, and clear ownership of innovation outputs.
- Define the purpose, scope, roles, responsibilities, confidentiality obligations, intellectual property ownership, data protection requirements, and commercialization rights before entering significant innovation collaborations.

- Encourage suppliers and business partners to propose solutions that improve product quality, resource efficiency, energy efficiency, safety, circular economy, environmental performance, traceability, and customer value.
- Apply due diligence, where appropriate, to assess partner capability, ethical conduct, regulatory compliance, intellectual property risks, cybersecurity risks, and sustainability performance.
- Include relevant innovation, confidentiality, data protection, intellectual property, and sustainability clauses in contracts or collaboration agreements.
- Promote knowledge sharing and capacity building with strategic suppliers and partners to support responsible innovation and continuous improvement across the value chain.
- Ensure that collaboration with competitors, industry associations, or external parties complies with fair competition laws and the Company's anti-unfair competition commitments.

10) Integration with Corporate Strategy

This policy supports the Company's corporate governance, enterprise risk management, digital transformation, innovation, customer trust, data-driven decision-making and business continuity objectives.

- **FOREST:** Protect operational, sourcing, traceability, production and sustainability data that support responsible management of natural resources and wood-based products.
- **FUTURE**: Enable secure digital transformation, cloud adoption, automation, data analytics, innovation and resilient technology infrastructure for long-term competitiveness.
- **TOGETHER:** Strengthen trusted collaboration with employees, customers, suppliers, communities, regulators and business partners by protecting data, privacy and digital communication channels.

Integrate information technology security considerations into investment decisions, system development, procurement, vendor selection, business continuity planning and sustainability reporting.

11) Implementation and Management Tools

11.1 Information Security Management and Procedures

- Develop and maintain standards, procedures and guidelines covering access control, password management, data classification, acceptable use, backup, recovery, cloud security, network security, endpoint security and incident response.
- Assign system owners, data owners, administrators and approvers for critical systems and data.

11.2 Identity and Access Management

- Maintain controlled user registration, approval, modification, periodic review and termination processes.
- Apply least privilege, multi-factor authentication for high-risk systems, privileged access controls and access logging.

11.3 Data Security and Privacy Controls

- Classify and protect confidential and personal data, apply encryption or secure transmission where appropriate and follow the Company's Data Privacy Notice.
- Maintain data retention, deletion, transfer and disposal practices consistent with legal and business requirements.

11.4 Infrastructure, Cloud and Endpoint Security

- Use technical controls such as firewalls, network segmentation, endpoint protection, anti-malware, patch management, vulnerability management, secure configuration, IDS/IPS or equivalent monitoring tools where appropriate.
- Maintain cloud security monitoring, access controls, security auditing, backup and recovery controls for cloud-based systems.

11.5 Backup, Recovery and Incident Response

- Maintain backup schedules, restoration testing, disaster recovery procedures and recovery documentation for critical systems.
- Operate an incident reporting and escalation process through the IT Service Center and administrator@vanachai.com, including recording, investigation, remediation and closure.

11.6 Training, Awareness and Resources

- Conduct periodic training and communication on cybersecurity, phishing, password security, data privacy, acceptable use, incident reporting and cloud security.
- Allocate sufficient personnel, budget and technology resources to support implementation, monitoring and continuous improvement of this policy.
- Monitoring, Reporting and Transparency

12) Monitoring, Reporting and Transparency

- Monitor security events, access logs, system logs, cloud activity, backup status, vulnerability status, incident tickets and remediation progress on a regular basis.
- Report material cybersecurity risks, significant incidents, control weaknesses, audit findings and corrective actions to the relevant management and governance bodies.

- Maintain records and evidence for access approvals, user reviews, incident reports, backup tests, vulnerability remediation, supplier assessments and training completion.
- Notify regulators, affected data subjects, customers, suppliers or other relevant parties where required by law, contract or internal incident response procedures.
- Disclose information technology security governance, risk management or material incident information through appropriate corporate reporting channels where relevant and legally appropriate.

13) Review and Continuous Improvement

- This policy shall be reviewed at least every two years, or earlier if there are changes in laws, regulations, technology, business operations, stakeholder expectations, risk profile, audit findings or material cybersecurity incidents.
- The Company shall continuously improve its information technology security controls in alignment with evolving cyber threats, recognized standards, regulatory expectations and lessons learned from incidents and exercises.
- The Information Technology Department, in coordination with relevant departments, shall prepare policy review results and improvement recommendations for management and governance review.
- Awareness, testing, audits, incident drills, access reviews and recovery exercises shall be used to strengthen the Company's security culture and cyber resilience.

14) Information Technology Security Policy Revision History

Version	Date	Policy Owner	Approved by	Key Changes / Comments
1.0	11 November 2024	Information Technology Department	Board of Directors	Initial issue of the Information Technology Security Policy focusing on IT security principles, user authentication, asset management, access control, backup, network and server security, internet and email security, encryption, physical security, data privacy, cloud security, prohibited cyber conduct, sanctions and incident reporting.
2.0	10 August 2026	Information Technology Department	Board of Directors	Revised and expanded into the Company's corporate policy structure under VNG-GOV-ITS-PL-02. Strengthened governance, ISO/IEC 27001 alignment, NIST Cybersecurity Framework alignment, cloud security, data privacy, access control, third-party security, cyber risk management, backup and recovery, incident response, KPIs, monitoring, reporting and continuous improvement.