CONTINUITY MANAGEMENT POLICY

Version 1/2026 VNG-GOV-CM-PL-01

Effective Date: 10 August 2026

VANACHAI GROUP

Continuity Management Policy
Vanachai Group Public Company Limited and Subsidiaries

Vanachai Group Public Company Limited and its subsidiaries ("the Company") recognize the importance of organizational resilience and preparedness for disruptive incidents that may affect business operations, production continuity, supply of wood-based products, employees, customers, suppliers, communities, shareholders, and other key stakeholders. The Company is committed to establishing and maintaining a structured Continuity Management framework to ensure that critical activities can continue at an acceptable predefined capacity during disruption and can be restored within appropriate recovery time objectives.

This Continuity Management Policy provides the governance framework for Business Continuity Management (BCM), crisis management, incident response, emergency preparedness, IT disaster recovery, supply chain continuity, and recovery planning across the Company. The policy supports the Company in reducing operational losses, safeguarding people and assets, protecting stakeholder trust, and restoring normal operations effectively after a crisis or significant disruption.

The policy has been developed with reference to ISO 22301:2019 Business Continuity Management Systems, ISO 22313:2020 guidance on the use of ISO 22301, ISO 31000 Risk Management, and relevant corporate governance, enterprise risk management, climate resilience, information security, occupational health and safety, and sustainability disclosure principles. It also reflects the Company's previous Business Continuity Management Policy, which emphasized BCM system development, continuity strategies, crisis response structure, maintenance of BCM documents, and awareness among management and employees.

1) Objectives

- Establish and continuously improve the Company's Business Continuity Management System (BCMS) in alignment with applicable laws, recognized international standards, and the Company's enterprise risk management framework.
- Ensure that critical business processes, manufacturing operations, logistics, information technology, procurement, finance, human resources, customer service, and support functions can continue or be restored within defined recovery objectives during disruptive incidents.
- Define clear governance, roles, responsibilities, escalation criteria, decision-making authority, and communication protocols for business continuity, incident response, emergency management, and crisis management.

- Conduct Business Impact Analysis (BIA), risk assessment, continuity planning, and recovery planning for critical processes, assets, locations, systems, suppliers, and stakeholders.
- Reduce the likelihood and severity of business interruptions caused by natural disasters, climate-related events, fire, flood, drought, energy disruption, machinery failure, raw material shortage, logistics disruption, cyber incidents, public health events, regulatory events, social unrest, or other material threats.
- Promote employee awareness, readiness, and disciplined execution through training, drills, exercises, documentation, and lessons learned.
- Support stakeholder confidence by maintaining continuity of essential operations, protecting employees and communities, and providing transparent communication during disruption and recovery.

2) Policy Alignment and International Standards

This policy is aligned, where applicable, with the following standards, frameworks, and guidance:

- **ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements**, including the 2024 amendment on climate action changes where applicable.
- **ISO 22313:2020 Security and resilience - Business continuity management** systems - Guidance on the use of ISO 22301.
- **ISO/TS 22317:2021 Guidelines for Business Impact Analysis** and ISO/TS 22318:2021 Guidelines for Supply Chain Continuity, where applicable.
- **ISO 31000:2018 Risk Management Guidelines** and the Company's Enterprise Risk Management (ERM) framework.
- **ISO/IEC 27001:2022 Information Security Management Systems and relevant IT** disaster recovery, cybersecurity, access control, and data protection practices.
- **ISO 14001 Environmental Management System and ISO 45001 Occupational Health and Safety Management System,** where business continuity relates to environmental incidents, emergency preparedness, and employee safety.
- **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.
- **TCFD / IFRS S2 climate-related risk and resilience principles**, where climate-related physical and transition risks may affect business continuity.
- **SET and SEC corporate governance expectations** on risk management, internal control, disclosure, business ethics, and board oversight.

- **United Nations Sustainable Development Goals (UN SDGs)**: SDG 8 Decent Work and Economic Growth, SDG 9 Industry, Innovation and Infrastructure, SDG 11 Sustainable Cities and Communities, SDG 12 Responsible Consumption and Production, SDG 13 Climate Action, and SDG 17 Partnerships for the Goals.

3) Scope of the Policy

This policy applies to:

- The Company, its subsidiaries, and joint ventures under the Company's operational control.
- Directors, executives, management, employees, temporary staff, contractors, consultants, and persons working on behalf of the Company.
- All critical business processes and support functions, including production, procurement, logistics, warehousing, sales, finance, human resources, legal, corporate communications, information technology, engineering, maintenance, environmental management, occupational health and safety, and security.
- All operating sites, plants, offices, warehouses, logistics routes, data centers, information systems, and third-party service arrangements that support critical activities.
- Suppliers, contractors, logistics providers, outsourced service providers, technology providers, utilities providers, and other business partners whose performance may materially affect the continuity of the Company's operations or stakeholder obligations.
- All phases of business continuity management, including risk identification, BIA, continuity strategy, prevention, preparedness, response, recovery, restoration, review, and improvement.

4) Definitions and References

- **Business Continuity Management (BCM)**: A holistic management process that identifies potential threats and impacts to business operations and provides a framework for building organizational resilience and effective response capability.
- **Business Continuity Management System (BCMS)**: A documented management system used to establish, implement, operate, monitor, review, maintain, and improve business continuity.
- **Business Continuity Plan (BCP):** Documented procedures and information that enable the Company to respond to a disruption and continue or recover critical activities within predefined objectives.

- **Business Impact Analysis (BIA):** A process for analyzing the impact over time of a disruption on the Company's activities, resources, products, services, stakeholders, and financial and non-financial outcomes.
- **Critical Activities:** Business processes, operations, services, systems, or resources that must be prioritized during disruption because their interruption would materially affect safety, compliance, customer commitments, production continuity, financial performance, reputation, or stakeholder trust.
- **Disruptive Incident:** An event that may interrupt normal operations, including natural disaster, fire, flood, drought, pandemic, cyber incident, system failure, utility outage, supply interruption, logistics disruption, workplace accident, regulatory event, or other crisis.
- **Recovery Time Objective (RTO)**: The target time within which a critical activity or system should be resumed after disruption.
- **Recovery Point Objective (RPO**): The maximum tolerable period in which data might be lost due to a disruption, used mainly for IT and information systems.
- **Crisis Management Team (CMT)**: A designated group of executives and functional representatives responsible for strategic decisions, escalation, communications, resource allocation, and stakeholder management during a crisis.
- **Incident Response Team (IRT)**: A functional or site-level team responsible for immediate response, containment, safety, and initial recovery actions during an incident.
- **IT Disaster Recovery Plan (IT DRP):** Documented procedures to recover critical information technology systems, applications, data, network services, and digital infrastructure.
- **Vanachai Integrated Materiality and Risk Assessment (V-IMRA):** An internal assessment process used by the Company to identify and prioritize sustainability-related and enterprise risk issues by integrating impact and financial materiality perspectives.

5) Governance and Accountability

Board of Directors: Approves this policy, oversees the Company's continuity and resilience direction, ensures that adequate resources are available, and monitors significant risks, incidents, and BCM effectiveness.

Risk Management and Governance Committee: Serves as the policy owner and oversees the integration of BCM into enterprise risk management, corporate governance, internal control, and strategic decision-making. The Committee reviews significant continuity risks, major incidents, exercise results, and improvement plans.

Audit Committee: Oversees the adequacy and effectiveness of internal controls, audit findings, corrective actions, and assurance activities related to BCM, IT disaster recovery, and critical process continuity.

Board of Executive Directors and Management: Ensure implementation of this policy across functions and locations, allocate required resources, approve continuity strategies, and embed BCM responsibilities into management accountability and performance expectations.

Enterprise Risk Team: Coordinates BIA, continuity risk assessment, maintenance of BCM documentation, escalation protocols, exercise programs, management reporting, and integration of BCM with the Company's ERM process.

Crisis Management Team: Provides command, strategic direction, stakeholder communication, resource allocation, and decision-making during major incidents or crises.

Department Heads and Site Management: Identify critical processes, prepare and maintain BCPs, designate response teams, ensure training and exercises, and implement recovery actions at the site and functional levels.

Information Technology Department: Develops, tests, and maintains IT disaster recovery, cybersecurity incident response, backup, restoration, system redundancy, access control, and data recovery procedures for critical systems.

Procurement, Logistics, and Supply Chain Functions: Assess supplier and logistics continuity risks, maintain contingency arrangements for critical materials and services, and coordinate supplier recovery actions during disruption.

Internal Audit: Conducts independent review of BCM governance, documentation, exercises, controls, and corrective actions, and reports material findings to the Audit Committee.

Employees, Contractors, Suppliers, and Partners: Comply with this policy, follow emergency and continuity procedures, report incidents promptly, participate in training and exercises where required, and support continuity and recovery activities.

6) Commitments and Principles

6.1 Legal Compliance and Governance Discipline: The Company shall comply with applicable laws, regulations, contractual obligations, permits, occupational health and safety requirements, environmental requirements, information security

obligations, and internal governance standards relevant to business continuity and crisis management.

6.2 **Protection of Life, Safety, and Well-being**: The Company prioritizes the safety and well-being of employees, contractors, communities, visitors, and affected stakeholders during any incident or crisis. Life safety takes precedence over asset protection and business recovery.

6.3 **Continuity of Critical Operations**: The Company shall identify and prioritize critical activities, products, services, systems, sites, and stakeholders. Continuity plans shall be developed to maintain or restore essential operations within approved RTOs and acceptable operating capacity.

6.4 **Risk-Based Planning and Business Impact Analysis**: Continuity strategies shall be based on BIA, risk assessment, dependency mapping, and criticality analysis covering people, premises, processes, technology, information, suppliers, utilities, logistics, and natural resources.

6.5 **Crisis Management and Escalation**: The Company shall establish clear incident classification, escalation criteria, command structure, decision-making authority, and communication channels for site-level incidents, corporate crises, and cross-functional disruptions.

6.6 **Supply Chain and Critical Partner Resilience**: The Company shall evaluate continuity risks associated with critical suppliers, contractors, logistics providers, utilities, IT service providers, and outsourced partners, and shall maintain contingency arrangements where material exposure is identified.

6.7 **Information Technology and Data Recovery**: The Company shall maintain IT disaster recovery arrangements for critical systems, including data backup, cybersecurity response, system redundancy, access control, recovery testing, and defined RTO/RPO parameters where applicable.

6.8 **Climate, Natural Hazard, and Site Resilience**: The Company shall consider physical climate risks, including flood, drought, extreme heat, storms, water stress, fire risk, and logistics disruption, as part of BCM planning and site resilience measures.

6.9 **Communication and Stakeholder Trust:** The Company shall provide timely, accurate, and controlled communication to employees, regulators, customers, suppliers, investors, communities, media, and other stakeholders during significant disruption, according to approved communication protocols.

6.10 **Training, Testing, and Continuous Improvement:** The Company shall conduct regular awareness activities, drills, scenario-based exercises, plan testing, post-incident reviews, and corrective action tracking to strengthen readiness and improve BCM maturity over time.

7) Risk, Impact, and Dependency Management

The risks, impacts, and dependencies associated with continuity management are identified, analyzed, and prioritized through the Company's Vanachai Integrated Materiality and Risk Assessment (V-IMRA) and Enterprise Risk Management (ERM) processes. The results are used to support strategic decision-making, risk appetite, control design, resource allocation, and long-term resilience planning.

7.1 Risk Identification and Assessment

- Identify internal and external threats that may disrupt critical activities, including natural hazards, climate-related events, fire and explosion, machinery breakdown, energy interruption, water shortage, raw material shortage, logistics disruption, cyberattack, IT failure, occupational health and safety incidents, pandemic or public health events, regulatory actions, social unrest, and geopolitical or market disruptions.
- Assess the likelihood, potential severity, operational impact, financial impact, compliance impact, reputational impact, stakeholder impact, and recovery complexity of identified scenarios.
- Review continuity risks at least annually, or when there are significant changes in operations, sites, suppliers, systems, regulations, technology, or external risk conditions.

7.2 Business Impact Analysis

- Conduct BIA for critical processes and support functions to determine maximum tolerable downtime, RTO, RPO, minimum operating capacity, critical dependencies, resource requirements, legal or contractual obligations, and stakeholder communication needs.
- Prioritize recovery of critical processes based on safety, compliance, customer commitments, production continuity, financial exposure, environmental impact, stakeholder importance, and strategic significance.
- Update BIA results when there are material changes in operations, technology, organizational structure, product lines, supply chain, or external risk profile.

7.3 Dependency Mapping

- Map dependencies across people, premises, production equipment, utilities, raw materials, inventory, IT systems, data, logistics routes, customers, suppliers, regulatory approvals, and third-party service providers.
- Identify single points of failure and develop continuity strategies such as alternate suppliers, buffer stock, backup utilities, alternate logistics routes, preventive maintenance, data backup, remote working arrangements, and mutual support between sites.

7.4 Risk Response and Recovery Strategy

- Develop risk response plans and continuity strategies based on preventive controls, response controls, recovery controls, and restoration measures.

- Ensure continuity strategies are proportionate to risk exposure, operational criticality, cost, technical feasibility, regulatory requirements, and stakeholder expectations.
- Track corrective actions from incidents, exercises, audits, near misses, and risk assessments until closure.

8) Targets and Performance Indicators

The Company shall establish measurable indicators to monitor the effectiveness of continuity management. Targets may be refined annually based on risk assessment, business changes, and operational priorities. Key indicators include:

100% of identified critical processes to have documented and approved BCPs or continuity procedures.

- 100% of critical processes to have reviewed BIA results, RTOs, and key dependencies at least annually or upon significant change.
- At least one corporate-level BCM or crisis management exercise per year, and at least one site-level or functional continuity drill per year for critical operations, where applicable.
- IT DRP testing for critical systems at least annually, with RTO/RPO test results and improvement actions documented.
- Annual BCM awareness or role-based training for relevant employees, management, response teams, and critical function owners.
- Critical suppliers and outsourced service providers to be assessed for continuity risk based on materiality and procurement criticality.
- Corrective actions from audits, incidents, exercises, or post-incident reviews to be tracked and closed within agreed timelines.
- Material business continuity incidents, downtime, production interruption, recovery time, stakeholder impact, and lessons learned to be reported to management and relevant committees.

9) Integration with Corporate Strategy and Decision-Making

The Company recognizes that supply chain resilience is essential to maintaining continuity of wood-based product manufacturing, customer commitments, and stakeholder trust. The following requirements apply to critical suppliers, contractors, and business partners where relevant:

- Identify and classify suppliers, contractors, and service providers that are critical to production, raw material availability, utilities, logistics, information technology, maintenance, safety, and compliance.
- Include continuity, emergency response, service recovery, data protection, safety, environmental, and compliance requirements in supplier evaluation, contracts, service level agreements, or procurement terms where applicable.

- Assess the continuity readiness of critical suppliers, including their recovery capability, alternative sourcing options, financial resilience, geographic concentration risk, cybersecurity posture, and logistics dependencies.
- Develop contingency plans for critical materials and services, including alternative suppliers, emergency procurement procedures, buffer stock, substitute materials, alternate transport routes, and cross-site support arrangements where feasible.
- Require contractors and outsourced service providers working at Company sites to comply with site emergency procedures, safety requirements, incident reporting protocols, and business continuity instructions.
- Coordinate with suppliers, logistics providers, customers, government agencies, utilities providers, and community stakeholders during disruption to minimize impact and accelerate recovery.

10) Monitoring, Reporting, and Disclosure

Continuity management is integrated into the Company's corporate governance, enterprise risk management, sustainability, operational excellence, digital transformation, and stakeholder management practices. The Company shall apply continuity management to support long-term value creation and resilient growth as follows:

- Embed continuity risk considerations into corporate planning, investment decisions, site expansion, plant modernization, procurement strategy, product supply planning, and infrastructure improvement.
- Align BCM with the Company's enterprise risk management and internal control system to ensure that business interruption risks are identified, prioritized, controlled, monitored, and reported.
- Integrate climate-related physical risks and resource dependency risks into continuity planning for critical sites and supply chains, including flood, drought, extreme heat, fire risk, water stress, and logistics vulnerability.
- Strengthen operational resilience through preventive maintenance, energy and utility reliability, critical spare parts management, emergency response readiness, IT resilience, and site-level recovery plans.
- Support the Company's sustainability direction by protecting people, minimizing environmental and social impacts during disruption, and maintaining responsible service to customers and communities.
- Promote a resilience culture through leadership commitment, employee participation, transparent communication, scenario planning, and lessons learned from incidents and exercises.

11) Implementation and Management Tools

The Company shall implement this policy through practical tools, procedures, systems, resources, and governance mechanisms appropriate to the scale and complexity of its operations.

11.1 Integration with Management Systems

- Integrate BCM with ERM, internal control, occupational health and safety, environmental management, information security, maintenance management, procurement, and site emergency response systems.
- Ensure that continuity documents are controlled, reviewed, accessible to authorized users, and updated after material changes or exercises.

11.2 Core BCM Documents

- Business Impact Analysis (BIA) reports and criticality assessments.
- Business Continuity Plans (BCPs) for critical functions, sites, and processes.
- Crisis Management Plan and incident escalation matrix.
- Emergency Response Plans for sites and operational hazards.
- IT Disaster Recovery Plan and cybersecurity incident response procedures.
- Supplier continuity and logistics contingency plans.
- Communication protocols, stakeholder contact lists, and notification templates.
- Exercise plans, test records, post-incident review reports, and corrective action logs.

11.3 Data, Technology, and Communication Tools

- Maintain updated emergency contacts, critical supplier contacts, customer contacts, employee notification lists, site maps, critical asset inventories, and key system inventories.
- Apply secure data backup, redundancy, system access controls, and restoration procedures for critical information and systems.
- Use appropriate communication channels for crisis notifications, management updates, employee instructions, stakeholder communication, and regulatory reporting.

11.4 Training and Exercises

- Conduct BCM awareness training for employees and role-based training for response teams, crisis team members, site management, IT recovery teams, and critical process owners.
- Carry out tabletop exercises, evacuation drills, scenario simulations, IT recovery tests, supplier disruption exercises, and cross-functional crisis exercises where relevant.
- Document lessons learned and ensure corrective actions are assigned, monitored, and closed.

11.5 Resource Allocation

- Allocate appropriate budget, personnel, equipment, technology, training, backup arrangements, and external support to implement BCM effectively.
- Ensure that continuity resources are proportionate to the Company's risk profile, critical operations, stakeholder obligations, and recovery priorities.

12) Implementation and Management Tools

- Monitor BCM performance, plan readiness, exercise results, incident trends, downtime, recovery performance, corrective actions, supplier continuity risks, and IT DRP test outcomes on a periodic basis.
- Report material continuity risks, major incidents, crisis response outcomes, and corrective action progress to management and relevant committees according to escalation requirements.
- Maintain reliable records of BIA, BCP, training, exercises, incidents, management reviews, audits, and corrective actions for assurance and continuous improvement.
- Disclose relevant information on risk management, operational resilience, climate-related resilience, and business continuity practices in the Company's annual reporting or sustainability disclosure where appropriate.
- Ensure that external communication during a crisis is accurate, consistent, timely, and approved by authorized spokespersons, while respecting confidentiality, legal requirements, and stakeholder interests.
- Use audit findings, stakeholder feedback, incident reviews, and exercise results to improve continuity planning and strengthen organizational resilience.

13) Review and Continuous Improvement

- This policy shall be reviewed at least every two years, or earlier if there are material changes in laws, standards, business operations, organizational structure, technology, stakeholder expectations, risk profile, or lessons learned from incidents and exercises.
- BCP, BIA, crisis management plans, IT DRP, emergency response plans, and supplier continuity plans shall be reviewed at least annually or when significant changes occur.
- The effectiveness of continuity management shall be evaluated through internal audits, management review, exercises, post-incident reviews, and performance indicators.
- The Company shall apply lessons learned and corrective actions to improve resilience, reduce downtime, strengthen response capability, and enhance stakeholder confidence.

- Policy review results, significant updates, and improvement recommendations shall be submitted to the Risk Management and Governance Committee and, where appropriate, to the Board of Directors for approval or acknowledgement.

14) Continuity Management Policy Revision History

Version	Date	Policy Owner	Approved by	Key Changes / Comments
1.0	11 November 2024	Enterprise Risk Team	Board of Directors	Initial issue of the Business Continuity Management Policy to establish BCM system development, continuity strategies, crisis response structure, maintenance of related BCM documents, and awareness among management and employees.
2.0	10 August 2026	Risk Management and Governance Committee	Board of Directors	Updated and expanded into a corporate Continuity Management Policy in alignment with ISO 22301, ISO 22313, ISO 31000, enterprise risk management, and corporate governance expectations. Added detailed governance responsibilities, BIA and dependency mapping, RTO/RPO, crisis management and escalation, IT disaster recovery, supply chain continuity, climate and cyber resilience, training and exercises, KPIs, reporting, and continuous improvement mechanisms.