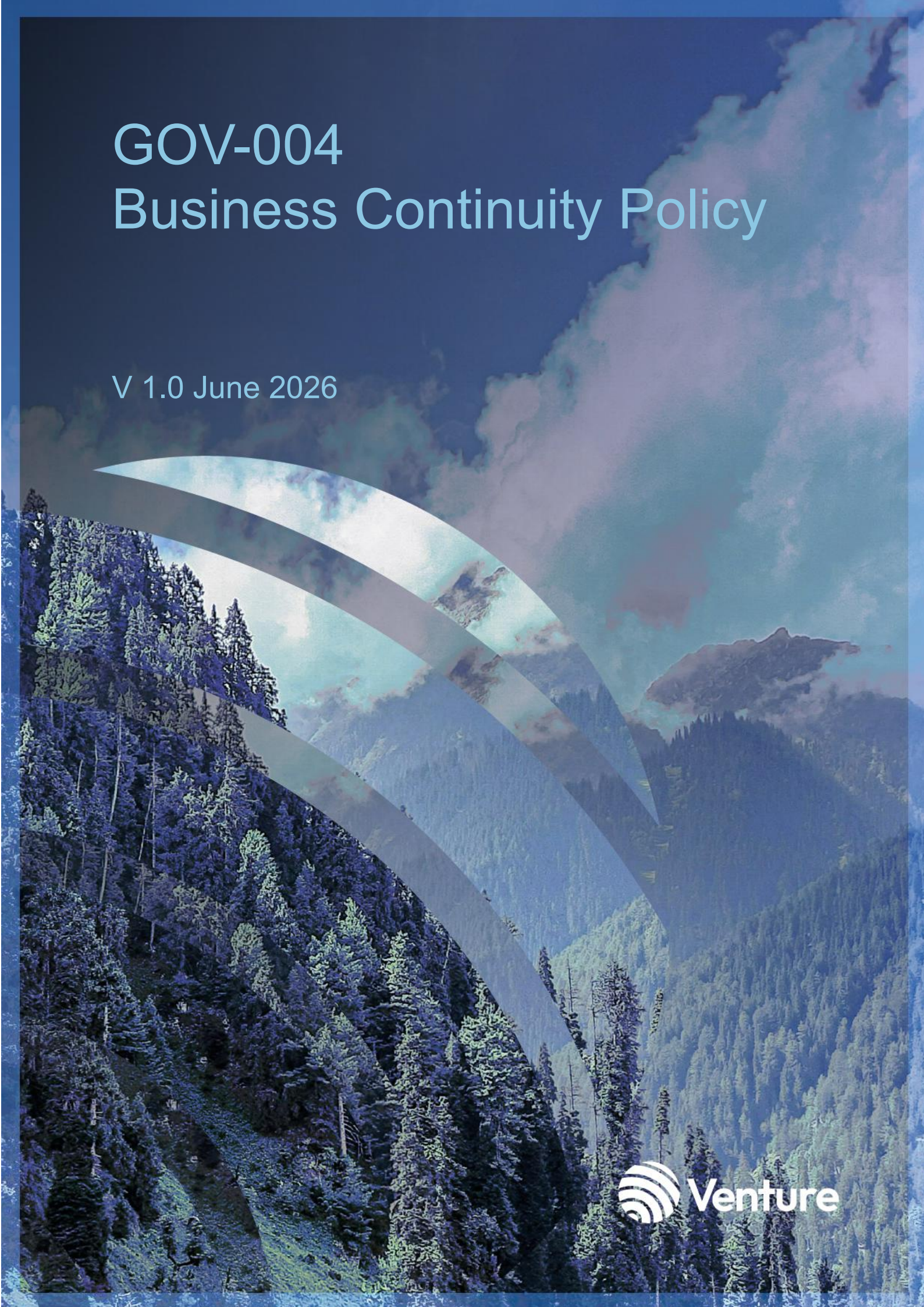
GOV-004
Business Continuity Policy

V 1.0 June 2026



Venture

Version	Date	Author	Changes Made	Next Review
1.0	01 May 2026	HR & Ops Director	Initial policy issue	01 May 2027

Policy Overview

The purpose of this policy is to establish Venture's commitment to maintaining business continuity and organisational resilience during disruptive events.

Venture recognises that interruptions to technology, people, facilities, suppliers, information assets, or operational processes may impact the organisation's ability to deliver services and meet customer commitments. This policy provides the framework through which Venture prepares for, responds to, and recovers from disruptive incidents.

This policy supports Venture's commitment to:

- Protecting customers and stakeholders
- Maintaining operational resilience
- Minimising disruption to service delivery
- Protecting information assets
- Meeting legal, regulatory, contractual, and compliance obligations
- Supporting continual improvement and organisational resilience

This policy supports Venture's Quality Management System (QMS), Information Security Management System (ISMS), and wider governance framework.

Scope

This policy applies to all Venture employees, contractors, suppliers, systems, services, facilities, and business processes that support organisational operations and customer service delivery.

The policy covers continuity arrangements relating to:

- Business operations
- Customer service delivery
- Information technology and cloud services
- Information security
- Communications
- People and workforce availability
- Third-party suppliers
- Critical business processes
- Remote working capabilities

The policy applies across all Venture business activities and locations.

Policy Statement

Venture is committed to maintaining appropriate business continuity capabilities that enable the organisation to respond effectively to incidents and recover critical operations within acceptable timeframes.

Business continuity shall be integrated into business planning, risk management, information security, supplier management, and operational decision-making.

The organisation shall maintain documented continuity and recovery arrangements appropriate to its size, complexity, risks, and operational requirements.

Business Continuity Principles

Venture will:

Protect People

Prioritise the safety, wellbeing, and welfare of employees, contractors, customers, and visitors during disruptive events.

Protect Customer Services

Maintain critical customer-facing services and contractual commitments wherever reasonably practicable.

Protect Information and Assets

Safeguard information assets, systems, and data throughout disruption and recovery activities.

Minimise Operational Impact

Reduce downtime, service interruption, financial loss, and reputational damage through effective planning and response.

Recover Critical Operations

Restore priority systems, services, and business processes within defined recovery objectives.

Continually Improve

Review and improve continuity arrangements through testing, exercises, incidents, audits, and management reviews.

Business Continuity Framework

Venture maintains a Business Continuity Framework consisting of:

- Business Continuity Policy
- Business Continuity Plan

- Corporate Risk Register
- Supplier Management Processes
- Information Security Management System
- Testing and Exercising Programme

The Business Continuity Plan shall act as the operational document supporting this policy.

Risk Based Approach

Business continuity arrangements shall be aligned with Venture's risk management framework.

Risks that may affect organisational resilience include:

- Cyber security incidents
- Ransomware attacks
- Cloud service outages
- Supplier disruption
- Telecommunications failures
- Loss of key personnel
- Technology failures
- Major operational disruption
- Information security breaches

Business continuity risks shall be identified, assessed, monitored, and managed through the Corporate Risk Register and associated risk management processes.

Continuity and Recovery Strategy

Venture operates a cloud-first and remote-capable operating model designed to support continuity during disruption.

Key continuity controls include:

- Secure remote working capabilities
- Multi-factor authentication (MFA)
- Cloud-hosted collaboration platforms
- Managed and encrypted devices
- Regular data backups
- Disaster recovery arrangements
- Information security monitoring
- Supplier escalation processes

Where disruption occurs, recovery activities shall focus on restoring critical services and minimising impact to customers and business operations.

Incidence Management and Response

All incidents that may affect operational capability, information security, or customer services shall be reported promptly.

Venture shall maintain documented incident management procedures covering:

- Incident identification
- Assessment and classification
- Escalation
- Containment
- Recovery
- Communication
- Lessons learned

Incident severity shall be assessed according to business impact, customer impact, security implications, and recovery complexity.

Communication During Disruption

Clear and timely communication is essential during continuity events.

Venture shall maintain communication mechanisms to support:

- Employee communications
- Customer communications
- Supplier communications
- Regulatory communications
- Management communications

Only authorised personnel may issue public statements or customer-facing communications relating to significant incidents or continuity events.

Information Security During Continuity Events

Information security requirements remain in force during disruptive incidents and recovery activities.

Business continuity activities shall not compromise:

- Access control requirements
- Authentication controls
- Data protection obligations
- Encryption standards
- Monitoring requirements
- Change management processes

Emergency changes shall be documented and reviewed through established governance processes following recovery.

Supplier Continuity

Venture recognises the importance of supplier resilience to operational continuity.

Critical suppliers shall be subject to appropriate due diligence and ongoing review, including consideration of:

- Business continuity capabilities
- Disaster recovery arrangements
- Security controls

- Incident management processes
- Escalation arrangements

Supplier continuity risks shall be considered within supplier management and risk management activities.

Testing and Exercising

Venture shall maintain a programme of business continuity testing to validate the effectiveness of continuity arrangements.

Testing activities may include:

- Tabletop exercises
- Backup restoration testing
- Cyber incident simulations
- Remote working tests
- Supplier escalation exercises
- Management reviews

Results shall be documented, reviewed, and used to drive continual improvement.

Roles and Responsibilities

Senior Leadership Team

Responsible for:

- Approving this policy
- Providing resources for continuity activities
- Reviewing continuity performance and resilience risks
- Supporting continual improvement

Finance and Commercial Director

Responsible for:

- Coordinating continuity activities
- Supporting incident response and recovery
- Maintaining continuity documentation
- Coordinating testing and exercising

Practice Directors

Responsible for:

- Identifying continuity requirements within their areas
- Supporting continuity planning
- Ensuring employees understand their responsibilities

Employees

Responsible for:

- Following continuity procedures
- Reporting incidents promptly
- Supporting continuity and recovery activities
- Maintaining awareness of continuity requirements

Training and Awareness

Venture shall ensure employees understand their business continuity responsibilities.

Training and awareness activities shall include:

- Continuity awareness training
- Incident reporting requirements
- Remote working expectations
- Information security awareness
- Role-specific continuity training where required

Training records shall be maintained in accordance with the Document Retention Register.

Related Documents

- Risk Management Policy
- Venture Quality Policy
- IT Security Policy
- Business Continuity Plan
- Corporate Risk Register
- Supplier Management Procedure
- Document Control and Retention Policy

Communication and Review

This policy shall be communicated throughout the organisation and made available to relevant interested parties where appropriate.

The policy shall be reviewed annually, following significant incidents, or following major organisational, technological, legal, or regulatory changes.