Business Continuity & Disaster Recovery Plan

VERSION	EFFECTIVE DATE	POLICY OWNER
1.0	2026-07-31	Matt Sapio, CISO

APPROVED BY
Matt Sapio

1. Purpose

This plan defines Eigenomic's business continuity and disaster recovery (BC/DR) strategy to support the resilience and recovery of critical business operations during disruptions. It is intended to minimize downtime, protect information and services, and support Eigenomic's SOC 2 security objectives.

2. Scope

This plan applies to all Eigenomic personnel, systems, cloud services, and third parties involved in continuity and recovery activities. Eigenomic has fewer than five employees, operates fully remotely, and uses AWS as its cloud infrastructure.

3. General Requirements

- **Risk Assessment and Mitigation:**
  - Regular risk assessments identify potential threats and vulnerabilities.
  - Mitigation and recovery priorities must be based on potential impact to Eigenomic's business operations and customers.
- **Plan Maintenance and Testing:**
  - The BC/DR plan is subject to regular testing, reviews, and updates to ensure effectiveness against evolving threats and changes in organizational structure.
  - Testing results must be documented and used to improve recovery procedures.

4. Alternate Work Facilities

- **Activation and Readiness:**
  - Because Eigenomic operates fully remotely, personnel may continue critical functions from suitable alternate remote locations when a normal work location is unavailable.
  - Alternate remote work arrangements must maintain applicable information security and access-control requirements.

5. Communications and Escalation

- **Communication Protocols:**
  - Clearly defined channels for internal and external communications ensure timely, accurate updates during incidents.
  - Escalation procedures outline the flow of information to senior management, stakeholders, vendors, and clients.
  - Communication plans include measures for safeguarding sensitive information per applicable privacy requirements.

6. Roles and Responsibilities

The following roles are defined to ensure effective implementation and ongoing management of the BC/DR plan:

Role	Responsibility
CISO / BC/DR Coordinator	Owns the BC/DR plan, coordinates activation, testing, review, and recovery oversight.
IT/Technical Recovery Role	Coordinates AWS, application, backup, restoration, and technical recovery activities.
Designated Management Role	Coordinates alternate remote-work arrangements if needed; Eigenomic does not rely on a primary corporate facility.
Communications Lead	Coordinates internal, customer, vendor, and other required communications during a disruption.

Role	Responsibility
System/Process Owners	Maintain continuity and recovery procedures for critical systems and business processes under their responsibility.

7. Continuity of Critical Services

- **Service Identification and Recovery Strategies:**
- **Customer Support:**
  - Responsible Department: Operations
  - Recovery Strategy: Transition to alternate facilities or remote work setups.
- **Business-Critical Administrative Services:**
  - Responsible Role: Finance or designated management role
  - Recovery Strategy: Use available cloud services and documented alternate procedures to restore critical administrative functions.
- **AWS Systems, Data Storage & Backups:**
  - Responsible Role: IT/Security
  - Recovery Strategy: Use AWS recovery, backup, and restoration capabilities configured for the applicable system.
- **Customer and Compliance Obligations:**
  - Responsible Role: CISO or designated compliance role
  - Recovery Strategy: Use documented alternate procedures where automated systems are unavailable.

8. Plan Activation

- **Activation Criteria and Procedures:**
  - The BC/DR plan is activated upon identification of any disruption that impacts critical business functions.
  - Activation is communicated via established channels, and responsible teams immediately initiate recovery procedures.
  - Continuous situation assessments are performed, guiding adjustments to the recovery strategy based on current threat landscapes and compliance obligations.

9. Appendices

Appendix A – Business Continuity Procedures by Scenario

- **Scenario-Specific Guidance:**
  - Recovery procedures should address relevant disruption scenarios, including cyber incidents, AWS or service outages, loss of endpoint access, and other events affecting critical operations.
  - Each scenario includes immediate response actions, identification of critical functions to be sustained, and clear escalation paths.

Appendix B – Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)

- **Defined Metrics:**
  - Critical systems and services are assigned specific RTOs and RPOs.
  - RTOs and RPOs must be defined for critical systems based on business and customer requirements and reviewed periodically.

10. Exceptions

- **Approval Process:**
  - Exceptions to this policy require formal approval from senior management, accompanied by documented risk assessments and mitigation measures.
  - All exceptions are reviewed periodically to verify that compensatory controls remain effective.

11. Violations and Enforcement

- **Compliance and Consequences:**
  - Non-compliance with the BC/DR plan may lead to disciplinary actions, including termination, depending on the severity and impact of the violation.
  - Employees must be familiar with BC/DR protocols and participate in regular training sessions to ensure readiness and adherence to this policy.