



## **Disaster Recovery Policy for Data Privacy**

Document Type: Policy & Operational Runbook  
Version: 1.0  
Effective Date: 2026-01-01  
Approved by: Executive Management  
Applies to: All Origen Tech employees, contractors, systems,  
and third parties handling company or customer data

# 1. Purpose

This Disaster Recovery (DR) Policy defines Origen Tech's framework for protecting personal, confidential, and business-critical data in the event of a disruption. The objective is to ensure data availability, integrity, confidentiality, and regulatory compliance during and after incidents.

This policy supports Origen Tech's commitment to:

- Data privacy and protection
  - Business continuity
  - Regulatory compliance (GDPR, ISO/IEC 27001, SOC 2)
  - Customer trust and operational resilience
- 

# 2. Scope

**This policy applies to:**

- All production and non-production systems
- Cloud and on-premise infrastructure
- Customer, employee, and partner data
- Third-party systems integrated with Origen Tech platforms

**Including but not limited to:**

- ERP systems (SAP)
  - CRM platforms
  - Data warehouses
  - Backup and archival systems
- 

# 3. Regulatory & Standards Alignment

This policy aligns with:

## **GDPR**

- Article 32 – Security of Processing
- Article 33 – Personal Data Breach Notification
- Article 34 – Communication of a Breach to Data Subjects

## **ISO/IEC 27001**

- Annex A.5 – Information Security Policies
- Annex A.8 – Asset Management
- Annex A.12 – Operations Security
- Annex A.17 – Information Security Aspects of Business Continuity

## **SOC 2 (Trust Services Criteria)**

- Security
- Availability
- Confidentiality

## 4. Definitions

- Disaster: Any event causing significant disruption to IT systems or data availability
  - DR: Disaster Recovery
  - RTO: Recovery Time Objective
  - RPO: Recovery Point Objective
  - PII: Personally Identifiable Information
- 

## 5. Roles & Responsibilities

### **Executive Management**

- Approves DR strategy and funding
- Ensures organizational commitment

### **Delivery Head (Disaster Recovery Owner)**

- Owns DR execution and continuous improvement
- Ensures alignment with customer SLAs

### **Delivery Ambassadors**

- Represent delivery excellence across products
- Ensure DR controls are implemented consistently

### **IT & Security Team**

- Executes backup, recovery, and testing
- Maintains documentation and monitoring

### **Data Protection Officer (or Assigned Role)**

- Oversees GDPR compliance
  - Manages breach notification processes
- 

## 6. Risk Assessment & Impact Analysis

Origen Tech conducts annual Business Impact Assessments (BIA) to:

- Identify critical systems and data
- Evaluate operational, legal, and reputational risks
- Define recovery priorities

## 7. Recovery Objectives

System Classification	RTO	RPO
Mission Critical	4 hours	15 minutes
Business Critical	8 hours	1 hour
Standard Systems	24 hours	24 hours

---

## 8. Backup Strategy

- Automated daily backups
- Encrypted backups (AES-256)
- Geo-redundant storage
- Access restricted by least privilege

Backup verification is performed quarterly.

---

## 9. Incident Response & Escalation

1. Incident detection and classification
2. Immediate containment
3. Activation of DR procedures
4. Internal escalation within 1 hour
5. Regulatory assessment within 24 hours

If personal data is impacted, GDPR breach assessment is initiated immediately.

---

## 10. Data Privacy Controls During Recovery

- Encryption in transit and at rest
- Segregation of environments
- Logging and audit trails
- Role-based access control

Temporary access granted during recovery is revoked post-incident.

## 11. Communication Plan

### Internal

- Executive briefing
- Delivery and Security teams

### External

- Customers (as contractually required)
- Regulators within 72 hours (GDPR)

All communications are coordinated by Legal and Data Protection functions.

---

## 12. Testing & Training

- DR testing conducted annually
- Tabletop exercises for executives
- Staff training on incident response

Test results are documented and corrective actions tracked.

---

## 13. Continuous Improvement & Innovation

**Origen Tech allocates an annual innovation budget to:**

- Improve DR automation
- Enhance monitoring and alerting
- Adopt emerging security technologies

Delivery workshops are conducted to refine procedures and SLAs.

---

## 14. SLA Levels

SLA Tier	Availability	DR Priority
Standard	99.5%	Medium
Premium	99.9%	High
Enterprise	99.99%	Highest

## 15. Policy Review

his policy is reviewed annually or following major incidents.

---

## 16. Approval

Approved by Origen Tech Executive Management

Document Classification: Internal & External (Controlled)  
Owner: Information Security & Delivery Leadership  
Review Cycle: Annual or upon significant regulatory/  
operational change