**Disaster Recovery Policy (DRP)**

**Policy ID:** SEC-DRP-001  
**Version:** 1.0  
**Approval Date:** [Insert Date]  
**Next Review Date:** [Insert Date + 12 months]  
**Owner:** Chief Information Security Officer (CISO)  
**Applies To:** All employees, IT teams, and service providers responsible for system continuity and recovery

**1. Purpose**

This Disaster Recovery Policy establishes the requirements for preparing, testing, and executing recovery efforts following disruptions to [COMPANY NAME]’s critical information systems. It ensures resilience, business continuity, and compliance with legal and regulatory obligations.

**2. Scope**

This policy applies to all systems, infrastructure, applications, services, and personnel involved in the recovery of IT operations following disruptive incidents. Covered environments include:

* On-premises servers and storage systems
* Cloud-hosted services and virtual infrastructure
* Network and communication systems
* Critical business applications and databases
* Backup systems and failover environments

**3. Policy Statements**

**3.1 Recovery Planning**

* All critical systems must have documented Disaster Recovery Plans (DRPs) that outline roles, processes, and recovery steps. *(NIST CP-2; ISO 27001 A.5.30)*
* DRPs must include defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each critical asset. *(NIST CP-4; ISO 27001 A.5.31)*

**3.2 Data Backup and Restoration**

* Systems and data classified as critical must be backed up regularly and stored in secure, geographically diverse locations. *(NIST CP-6, CP-9; ISO 27001 A.8.12, A.5.31)*
* Backups must be encrypted, access-controlled, and tested periodically for integrity and restorability. *(NIST MP-5, CP-10; ISO 27001 A.5.14, A.8.12)*

**3.3 Roles and Responsibilities**

* Disaster Recovery roles and contact information must be documented and updated regularly. *(NIST CP-3; ISO 27001 A.5.30)*
* Designated recovery personnel must be trained and available to support plan execution during declared disasters. *(NIST AT-3; ISO 27001 A.6.3)*

**3.4 Testing and Exercises**

* All DRPs must be tested at least annually using tabletop, simulation, or failover exercises. *(NIST CP-4; ISO 27001 A.5.31)*
* Lessons learned from exercises must be documented and used to improve DRPs. *(NIST CP-2(3); ISO 27001 A.5.26)*

**3.5 Communication and Notification**

* Recovery plans must include documented internal and external communication procedures. *(NIST IR-4, CP-2; ISO 27001 A.5.25, A.5.30)*
* Regulatory bodies, customers, and vendors must be notified in accordance with contractual and legal obligations during major outages. *(NIST IR-6; ISO 27001 A.5.25)*

**4. Roles and Responsibilities**

|  |  |
| --- | --- |
| **CISO** | Owns the DRP; ensures alignment with risk management, compliance, and executive oversight. |
| **Disaster Recovery Manager (DRM)** | Coordinates the activation, execution, and deactivation of the DRP. Maintains DR documentation and test schedules. |
| **IT Infrastructure Team** | Ensures recovery of networks, systems, and core infrastructure. Maintains backup systems and failover readiness. |
| **Application Owners** | Document application-specific DR procedures and validate post-recovery functionality. |
| **Data Protection Officer** | Ensures backup policies are enforced; verifies integrity and restorability of backup data. |
| **Business Continuity Lead** | Ensures DRP alignment with Business Continuity Plans (BCP) and assists with business process restoration. |
| **Compliance/Legal Team** | Reviews DR documentation and ensures notification obligations (e.g., GDPR, HIPAA, CCPA) are met. |
| **Executive Team** | Approves DR strategy and provides funding and authority for execution and escalation. |

**5. Compliance and Enforcement**

Noncompliance with this policy may lead to extended downtime, data loss, legal penalties, and reputational harm. All staff involved in recovery operations must adhere strictly to documented DRPs.

**6. Review and Maintenance**

This policy and associated DRPs must be reviewed annually and after significant changes in systems, risk profile, or business operations. The CISO or delegate is responsible for policy updates and oversight.

**7. Acknowledgment and Agreement**

I acknowledge that I have read and understand [COMPANY NAME]’s Disaster Recovery Policy. I agree to fulfill the responsibilities assigned to me within applicable DR plans and procedures.

|  |  |  |
| --- | --- | --- |
| **Name (Print):**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |