**Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)**

1. **Introduction**

CyberTech Innovations is committed to maintaining operational resilience and ensuring business continuity in the event of a cyber incident, natural disaster, or system failure. This document outlines the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) to safeguard critical business functions and IT infrastructure.

1. **Business Continuity Plan (BCP)**
   1. **Purpose**

**The Business Continuity Plan (BCP) ensures that CyberTech Innovations can continue critical business operations with minimal disruption in the event of a crisis.**

* 1. **Key Business Functions and Recovery Objectives**
* Customer Data Management System (CDMS): Restore access within 4 hours.
* Research & Development (R&D) Network: Resume operations within 24 hours.
* Supply Chain Management System (SCMS): Resume logistics within 12 hours.
* Payment Processing System (PPS): Restore transactional integrity within 2 hours.
  1. **Business Continuity Strategies**
* Data Backups: Daily backups stored in offsite and cloud-based locations.
* Redundant Systems: Failover systems ensure continuity during primary system failure.
* Remote Work Enhancement: Secure remote access to critical systems.
* Emergency Communication Plan: Define notification protocols for stakeholders and employees.

1. **Disaster Recovery Plan (DRP)**

* 1. **Purpose**

**The Disaster Recovery Plan (DRP) defines the steps to restore IT infrastructure and data in the event of a disaster, ensuring minimal downtime and data loss.**

* 1. **Disaster Recovery Objectives**
* Restore full operational capacity within 24-48 hours.
* Minimize data loss to less than 1 hour of transactions.
* Ensure compliance with all regulatory and security requirements.
  1. **Disaster Recovery Strategies**
* Incident Response Team (IRT): Assign roles to IT and security teams for rapid response.
* Data Recovery Process: Implement automated and manual data recovery procedures.
* Cloud-Based Recovery Solutions: Utilize cloud infrastructure for rapid application recovery.
* Regular Testing & Drills: Conduct semi-annual disaster recovery drills
  1. **Disaster Recovery Executive Steps**

1. Incident Identification: Detect failures via SIEM monitoring and alerts.
2. Containment & Assessment: Isolate affected systems and assess the impact.
3. Recovery Implementation: Restore systems from backups and failover solutions.
4. Verification & Validation: Test restored systems for full functionality.
5. Post-Recovery Review: Analyze incidents and update the DRP accordingly.

Sign-Off Sheet

The following personnel acknowledge that the **Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)** have been reviewed and approved:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Title** | **Department** | **Date** | **Signature** |
| [Name] | Chief Information Officer | IT Leadership | [Date] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [Name] | IT Security Manager | IT Security | [Date] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [Name] | Compliance Officer | Compliance | [Date] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [Name] | Risk Management Lead | Risk Management | [Date] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| [Name] | Audit Team Representative | Internal Audit | [Date] | \_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |  |  |

By signing this document, the individuals listed confirm that they have reviewed and acknowledge the **BCP and DRP**.