COIT13236 – Cyber Security Project

**KN University Network Design**

1. **Disaster Recovery and Business Continuity Plan**

Group 02

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Student ID** |
| Krishan Himesh Abeyrathne | System Administrator | 12217274 |
| Narayan Parajuli | System Security Analyst | 12144248 |

# Disaster Recovery and Business Continuity Plan

**Disaster Recovery and Business Continuity Plan**

Ensuring that a network can recuperate rapidly from disturbances and keep up with business tasks during emergencies is critical for minimizing downtime and guaranteeing functional versatility. This includes detailed planning, preparation, and testing.

**Components:**

**Disaster Recovery Strategy:**

Data Backup: Consistently back up critical data to secure areas (both on-premises and in the cloud).

Recuperation Procedures: Create and record strategies for data and system recovery.

|  |  |
| --- | --- |
| Component | Description |
| Regular Backups | Schedule daily incremental and weekly full backups. Use automated tools to ensure consistency. |
| Backup Locations | Store backups locally, offsite, and in the cloud. Encrypt backups and restrict access. |
| Recovery Objectives | Define RTO and RPO for each critical system and data set. |
| Priority Restoration | Prioritize restoration of critical business systems and data. |
| Data Validation | Verify restored data for integrity and completeness. |
| System Recovery | Document hardware replacement, software reinstallation, and configuration restoration procedures. |
| Regular Testing | Conduct regular tests and drills, including scenario-based exercises. |
| Continuous Improvement | Update recovery procedures based on testing outcomes and real incident experiences. |

**Business Coherence Plan:**

Critical Functions: Recognize and focus on basic business works that need to stay functional.

Alternate Sites: Lay out alternate sites for tasks on the off chance that essential destinations are compromised.

**Testing and Drills:**

Regular Drills: Conduct regular disaster recuperation drills to test the viability of recuperation strategies.

Plan Updates: Update the disaster recovery and business progression plans in view of drill results and changes in the environment.

**Communication Plan:**

Contact List: Keep in touch of up-to-date contact list of key work force and partners.

Communication Channels: Establish Communication channels for notifying stakeholders during a disaster.

# References

IBM (2024) Data Backup and Disaster Recovery. Available at: https://www.ibm.com/services/business-continuity/data-backup (Accessed: 1 August 2024).

Anderson, D. and Williams, J. (2018) ‘Best Practices in IT Disaster Recovery Planning’, *International Journal of Business Continuity and Risk Management*, 4(2), pp. 115-128. doi:10.1504/IJBCRM.2018.091214.