KN University Network Design

COIT13236 – Cyber Security Project

Document Title	Disaster Recovery and Business Continuity Plan
Document Type	Technical Artefact
Document Status	Completed
Document Version	V_2.01
Group No	02
File name	group02-disaster-recovery-and-business-continuity-plan.docx
Created By	Narayan Parajuli (12144248)
Create Date	05/08/2024
Reviewed By	Krishan Himesh Abeyrathne (12217274)
Reviewed Date	15/08/2024

Table of Contents

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:

1. **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.

2. **Business Coherence Plan:**

   i. Critical Functions: Recognize and focus on basic business works that need to stay functional. Distinguish and focus on basic business works that are crucial for the college's activities. This incorporates centre scholarly administrations, regulatory cycles, students' data frameworks, and exploration support. Guarantee that these capabilities stay functional in any event, during disturbances or crises.

   ii. Alternate Sites: At KN University, develop designs for substitute destinations to keep up with tasks assuming that essential areas are compromised. Lay out optional data centre or cloud for critical data and applications, set up remote work abilities for staff and personnel, and plan physical areas for transitory work areas or teaching environments in crises.

3. **Testing and Drills:**

   i. Regular Drills: Consistently lead disaster recovery and business continuity drills to test recuperation systems and response plans. Utilize different drill types, including tabletop works out, recreation penetrates, and full-scale practices including all divisions and outside accomplices. Utilize devices like simulation software, and coordinate with crisis services to assess both technical reactions and communication among staff.

   ii. Plan Updates: After each drill at KN University, break down results to distinguish and address shortcomings in recuperation plans. Use criticism to refine methodology and update contact records, while consolidating changes in innovation, hierarchical construction, and guidelines to keep the plans pertinent and successful.

4. **Communication Plan:**

   Maintain list for key staff and outside accomplices, including inner staff, personnel, and executives, as well as crisis administrations and merchants. Routinely review and update this list to reflect current jobs and contact details, guaranteeing it stays exact following changes in the association or outside connections.

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.