UNIVERSITY OF
Baguio
SCHOOL OF INFORMATION AND TECHNOLOGY

NAME: Hyra Cayambas	DATE PERFORMED: 11/19	/40
Section: IDC1	DATE SUBMITTED: 11/20	

SYSADM1 – Data Loss

Instructions:

Read and analyze the data loss scenarios provided. Create a data recovery plan by providing impact assessment, recovery plan and preventive measures for each scenario. Lastly, answer the reflection question.

Evaluation Criteria Guide:

1. Impact Assessment:
   - Accurately identifies the potential consequences of the data loss.
   - Quantifies the potential financial, operational, and reputational impact.
2. Recovery Plan:
   - Proposes a detailed, feasible, and timely recovery plan.
   - Includes steps for data restoration, system recovery, and business continuity.
   - Identifies the necessary resources and personnel.
3. Preventive Measures:
   - Recommends specific measures to prevent similar incidents in the future.
   - Addresses potential vulnerabilities in security, hardware, and software.
   - Proposes regular backups, security audits, and employee training.
   - Recommends appropriate RAID levels for data redundancy and performance.

Scenario	Impact Assessment	Recovery Plan	Preventive Measures
A system administrator accidentally deletes a critical database containing customer information while performing routine	-Service disruption for customer -Loss of trust with client -Possible regulatory fines	-Stop all related operations to prevent further damage -Implement database recovery mechanism to	-Implement role-based access control to minimize accidental deletions -Regular employee

maintenance.	for data non-compliance	retrieve deleted data -Restore data from most recent backup -Notify stakeholders and provide recovery timeline	training -Test backups routinely
A major hard drive failure occurs on a server hosting essential business applications, resulting in data loss.	-Business downtime costs and expenses for repair/replacement - Disruption in service and loss of productivity -Delayed services could lead to client frustration	-Replace failed drive -Use RAID to rebuild data automatically if available -Restore data from most recent backup if RAID unavailable -System tests to ensure business applications are operational	-Use RAID with redundancy -Schedule regular hardware inspections and upgrade old components
A powerful earthquake strikes a data center, causing significant damage to hardware and power infrastructure.	-Costly hardware/infrastructure replacement and repair -Extended downtime and loss of access to critical systems -Delayed service recovery could weaken client trust	-Activate disaster recovery plan -Use remote backups stored offsite to restore services -Set up temporary operational environments for business continuity -Coordinate with vendors and contractors to repair and replace damaged infrastructure	-Designate an offsite data center as a hot standby for emergencies -Employ seismic-resistant racks and secure server placement -Regularly test disaster recovery plans and update them based on risk assessments
A ransomware attack encrypts critical data, rendering it inaccessible.	-Ransom payment, regulatory fines, and loss of revenue -Halted workflows, delayed service delivery -Customer and partner distrust in company security practices	-Isolate infected systems to prevent malware spread -Report the incident to authorities and involve cybersecurity experts -Restore data from clean backups, avoiding any ransom payment -Reinstall operating systems and applications to ensure no malware remnants	-Conduct regular vulnerability assessments and patch management -Implement multi-factor authentication and endpoint security software -Train employees
A system administrator misconfigures a backup	-Reduced efficiency due to data loss and manual	-Identify the root cause of misconfiguration and stop	-Conduct regular audits of

system, leading to data corruption and loss.	corrections -Loss of confidence in IT processes -Increased costs for re-creating or repairing data	the backup system temporarily -Restore data from the most recent valid backup -Cross-verify restored data against source files to ensure integrity -Implement manual corrections for corrupted	backup configurations -Implement backup verification processes after every backup cycle -Use backup systems with built-in integrity checks and error recovery mechanisms

Reflection Question

Despite our best efforts, some data could not be recovered due to the severity of the incident. We deeply regret the inconvenience caused and assure you that we are taking this matter seriously. Our team is already implementing stronger backup systems, more frequent testing, and enhanced security protocols to prevent future issues. Your trust is our priority, and we are committed to supporting everyone affected with tailored solutions.

Mitigation steps:

-Provide clear communication and support for affected parties.

-Offer compensatory measures where applicable.

-Invest in advanced recovery tools and employee training for long-term measures.

Grading Rubric

Criteria	Excellent (10 pts)	Satisfactory (7 pts)	Needs Improvement (4 pts)	Score
Impact Assessment	[✓ Accurately identifies all significant impacts.]	Identifies some key impacts but misses others.	Fails to identify significant impacts.	10
Recovery Plan	Proposes a comprehensive, detailed, and feasible plan.	[✓ Proposes a basic plan but lacks detail or feasibility.]	Fails to propose a viable plan.	7
Preventive Measures	[✓ Recommends strong, specific preventive measures, including appropriate RAID levels.]	Recommends some preventive measures but lacks detail or specificity.	Fails to recommend any preventive measures.	10
Reflection Question:	Clearly and concisely explains the situation to stakeholders, acknowledging the limitations of data recovery.	[✓ Provides a basic explanation but lacks clarity or empathy.]	Fails to provide a satisfactory explanation.	7
			Total Score:	34/**40**