UNIVERSITY OF Baguio SCHOOL OF INFORMATION AND TECHNOLOGY		
NAME: Cabay Marcial	DATE PERFORMED:	
Section:	DATE SUBMITTED:	/40

SYSADM1 – Data Loss

Instruction/s:

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 maintenance.	Data loss. System downtime. Customer dissatisfaction.	Restore the database from backup. Notify affected customers.	Provide seminars/training on database handling. Use Redundant Backups. Enforce strict access controls and permissions on handling databases.
A major hard drive failure occurs on a server hosting essential	System downtime. Financial Loss.	Replace/Repair the failed hardware.	Use RAID. Perform regular hardware maintenance.

business applications, resulting in data loss.	Delays in business operations.	Restore data from recent backup. Notify affected customers.	Use Redundant Backups.
A powerful earthquake strikes a data center, causing significant damage to hardware and power infrastructure.	Power Loss. Possible loss of data. Service Downtime.	Conduct a thorough assessment of damages to hardware. Repair/Replace damaged hardware. Restore data from most recent backup.	Develop a comprehensive disaster recovery plan. Use redundant power supplies.
A ransomware attack encrypts critical data, rendering it inaccessible.	Data inaccessibility. Financial Loss. Disrupt business operations.	Isolate infected systems. Hire cybersecurity professionals to assist with data recovery and ransomware removal.	Provide seminars or training to employees on recognizing phishing attempts. Regularly update and patch all software and systems. Regular security audits and vulnerability assessments.
A system administrator misconfigures a backup system, leading to data corruption and loss.	Data Loss/Corruption. Operational Disruption. Financial Loss.	Identify the last known backup before the misconfiguration and attempt data recovery from it. Correct the misconfiguration in the backup system and test thoroughly before restoring operations.	Perform regular tests and audits of the backup system. Use Redundant Backups. Training for System administrators on proper backup procedures.

Reflection Question

How would you explain to your company's stakeholders if, despite your best efforts, some data was still unrecoverable after implementing data recovery measures? What steps would you take to mitigate the impact of this data loss and prevent future occurrences?

- By explaining to them thoroughly the incident, and all the steps done to recover the data, including the data that is lost and what is the effect. Lastly is to reassure to the stake holders that this will be a lesson and such that steps will be taken to ensure that the incident will not happen again.
- To mitigate the impact, ensure that anyone affected by the incident is given a detailed report about the incident and that actions are being taken to address the incident. To prevent this from happening again, implementing a comprehensive back up strategy like using both off site and on-site backup will be done, and conduct regular testing of backup and recovery processes. Furthermore, invest in advanced monitoring tools for detecting issues, and provide seminars or training to staff of how to handle data. Lastly, the incident will be properly documented and will serve as a reminder and for strengthening future preventive 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.	
Recovery Plan	Proposes a comprehensive, detailed, and feasible plan.	Proposes a basic plan but lacks detail or feasibility.	Fails to propose a viable plan.	
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.	
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.	
			Total Score:	**/40**