**Disaster Recovery Plan**

Name

Professor's Name

Institution of Affiliation

Course code

Date

**Introduction**

A disaster recovery plan is a structured approach that shows how an organization can resume its operations after an unplanned event. A disaster recovery plan is essential in organizations for business continuity. However, the plan depends on the organization's information technology infrastructure (Wallace & Webber, 2017). The main objective of a DRP is to recover the lost data and the system's functionality to operate after the disaster. A plain mainly consists of precautions that minimize disaster impacts for the organization to resume its operations. The company analyses its processes and needs for continuity while generating the plan. Therefore, it is crucial to define its data recovery and protection strategies due to increased cybercrime activities. Quick response to disasters saves the organization's reputation and financial damages. In addition, a disaster recovery plan ensures that the company has a clear way of recovering from the catastrophe while meeting the compliance requirements. The significant objective of the recovery plan is to respond to emergencies like security breaches, fire, earthquakes, and floods to reduce their impacts on business operations.

**Roles and Responsibilities**

The recovery team is responsible for drafting the company's disaster recovery plan, developing its procedures and processes, and implanting it when the unplanned event occurs. The disaster recovery plan is as crucial as the team involved in successfully bringing the business back to its normal operations. Therefore, the disaster recovery team comprises various individuals across the organization's department to leverage their expertise to cover the areas with greater risk. The disaster recovery coordinator is the team plan leader who executes the whole disaster plan (Felter, 2021). The coordinator ensures that the disaster recovery plan aligns with the business objectives in its impact analysis. Also, all the members are made aware of the program. The coordinator also initiates the recovery proves and coordinates with the information technology team in every step until every asset gets recovered successfully. However, any person from a higher IT management level can take the position. A critical business unit advisor works with the committee to determine and evaluate the policy considerations, budget, strategy, and selecting disaster recovery team members. They help the disaster recovery team in overseeing the recovery plan and process. Also, they should have detailed information for every department for a successful program. The IT profession requires the advisor to have detailed information on how critical each department got affected. The IT profession then calculates the accurate downtime tolerance of each department during the planning process. The advisor can be the head of the departments.

The business continuity expert's role is to consider the company's strategy and company-wide initiative and the non-IT recovery aspects. The expert ensures this by establishing temporary resources, telecommunications, and workplaces for the organization to resume its operations soonest possible. The continuity expert acts as the link between the entire company and the IT department to ensure effective communication in the company. Business continuity is essential in the recovery plan; hence, the business continuity expert clarifies the procedures and gathers the relevant information for a successful recovery. The human resource manager can be the business continuity expert. The recovery team involves the women and the men with more responsibilities in the recovery process. The team comprises IT experts from all information technology infrastructure units to cater to storage, databases, servers, and network. In addition, the team understands the information infrastructure landscape the ways to implement the strategies to support the infrastructure's integrity. The disaster recovery plan team includes the experts on the managerial level of every IT department unit.

**Incident Response**

Incident response refers to the measures taken to cope with various emergencies like security breaches, fire, floods, earthquakes, and more affect an organization. Risk mitigation and preparedness require a comprehensive and detailed incident response plan. The incidence response expert ensures a uniform approach and that all the steps are keenly followed (Whitman & Mattord, 2021). The expert also determines the cause of the problem to prevent such incidents from recurring in the future. Lastly, the expert updates the response plan to ensure that it addresses the business's needs. For example, a security breach affects the information technology infrastructure integrity. Such attacks include DDoS attack which interrupts the server traffic, website and network. Also, ransom and malware is a standard attack that gets confidential information from the systems. Phishing is a threat in which the attack attaches a malicious program. The receiver is tricked into giving personal information like bank details and passwords on other sites that look genuine. Insider threat happens when former employees or other business associates want to harm the organization for their gain by stealing their data. The main objective of the security recovery plan is to protect the data from the breach ("ISO 24762 Information Technology – Security Techniques Guidelines for Information and Communications Technology Disaster Recovery Services", 2021). After a security breach, the disaster recovery team surveys the damage by performing an internal investigation to determine the impacts of the disaster on the essential business operations.

Investigation allows the team to find out the attacker and find out the security vulnerabilities to improve. The unit can limit additional damage by filtering, re-routing network traffic, and isolating affected parts. The disaster team records the details of the actions taken together with the affected system, disrupted services, compromised accounts, the damage amount, and affected data and network. Security breaches should be reported to the law enforcement agencies like the FBI or the state and the local government. However, the organization's disaster recovery team must have met with law enforcement earlier to know when and how to report an incidence (Dhillon, 2021). The disaster recovery team then notifies the affected people to protect themselves. However, with the help of law enforcement, they direct the company on whether to inform the concerned people immediately or delay the further investigation. The affected individuals can be notified in person through a letter or phone to ensure no further damages (Alawanthan et al., 2017). The last step is learning from the breach by documenting the mistakes, assessing how the organization would have avoided the mistakes, and conducting training aligning with the learned lesson.

A fire disaster is one of the most destructive disasters in an organization due to unconsciousness (Baylis & Boomhower, 2019). Fire disasters are common in the organization's stores, burning all the available stock and hindering the supply chain operations. However, many fires are avoidable by taking the proper precautions and having many fires escape exits to vacate the building for the safety of employees and employers. Fire disaster response involves calling for help in case of smoke or fire, activating the nearby pull station, and giving the location details. The disaster recovery team then directs everyone towards the fire exits to evacuate the building. The people can exit through the nearest doors that lead to the outside. People should avoid using the elevators and use the protected stairwells. In case of smoke, the employees may notify their supervisors of its cause. Flood disaster involves water overflow in heavy raining areas with tsunamis and cyclones (Mansell, 2017). Also, the disaster recovery team keeps people from the flooded regions because even one-foot-deep water can harm people and call for the rescue team. Flood affects the whole organization by destroying available stock, the systems, and other items vulnerable to moisture.

Earthquake disaster involves violent ground shaking together with everything on it. If the building is occupied during the earthquake, the disaster recovery team instructs the people to drop to their knees and hands and stay in safe places (Rom & Kelman, 2020). If outside, the people should keep away from buildings, utility wires, street lights and get down until it stops. After an earthquake, the disaster recovery team can keep the people off the building due to aftershocks and cases falling after weakening, listen to the news for updates, stay away from the damaged structures and help the injured and the trapped people. Also, the disaster recovery team may inspect the building after the earthquake to look for impacts on the walls, electrical, roof, or foundation, leave the building in case of chemical or gas leakage, and notify the insurance company about the damage. Lastly, the employees and employers should not get back to work until the disaster recovery team declares the building safe.

**Plan Activation**

Plan activation involves the means of executing the action documented in the disaster recovery plan. Timely activation involves taking the related procedures and steps addressing various business requirements like effective communication, life safety accounting, and more. Plan activation identifies the disaster's condition by its severity, type, duration, and impact. Assessment procedures involve evaluating the disaster events for successful activation criteria. In addition, considering the IT management professionals, company executives, and the management personnel for approval mechanisms. Activation logistics are essential to ensure that the required items for activation are available to support the process. Lastly, the communication procedures are critical for informing the employees and others like the public on the decisions and the related activities. The activation steps include reacting to the disaster, responding by activating the disaster recovery plan, recovering the everyday operations, and evaluating the process to improve response capabilities. For example, with the fire disaster, the business should store their stock in various areas to avoid total loss and completely blocking the supply chain from its operations. Also, a company can encourage its employees to work from home and ensure that they keep effective communication to keep track of their progress. The organization can make the organization's data accessible from any location for the employees to work from home using iCloud services with unique passwords for every employee. The disaster recovery team can push for a shared database to track employees' work from various working stations.

**Document History**

Disaster management documentation occurs in various ways depending on the company's devices ("Documentation in Disaster Management - Where do we start?", 2021). Some companies use their handheld devices to record the disaster strikes, and others wait for the central operation center. However, the communication method does not matter. The leading causes of the emergencies must be documented during and after the crisis. Therefore, documentation begins after the disaster strike notification is given until it ends. Documentation involves applicable documentation and compiling the notes from the response team members and employees. Documentation consists of the time and the location that the incident took place. Suppose the people at risk called for an evacuation and the time required to evacuate all of them. The functionality of the designated alarms is documented, and safety of the assembling areas after the disaster stroke for safety.

The effectiveness of the communication channels and accountability of all employees is essential to tell their safety. Satisfaction of the on-site during the disaster and any other additional equipment brought gets documented. The emergency plan procedures are written, that is, if they were followed as described. The documentation also contains the areas that require improvement during the disaster. The disaster emergency team also documents any assistance they might have received from the local jurisdiction and any suggestions they offered for improvement. Lastly, the documentation includes any changes that the emergency plan requires to improve on their response capabilities. Documentation of a disaster is essential; written audio or visual recordings should have detailed emergency response steps to understand the event's occurrence clearly. The lessons learned and the information recorded is critical in making a better operational emergency plan in the future.

**Procedures**

Procedures in documenting are essential inadequate documentation of the event's occurrence from the time the disaster strikes till everyone is saved. The first step is recording the facts that happened during the disaster. If the employees are unaware of the events, the disaster recovery team should not document speculations because they give wrong information. Avoid criticizing other people's efforts and methods. Everyone's effort during the disaster to help is essential. In addition, the disaster recovery team should write facts and avoid speculations on the disaster causes. The information is necessary for learning and making a better recovery plan in the future. Also, the insurance company requires properly documented work on the disaster to know the causes before compensating the company's losses. Lastly, the disaster recovery team should avoid unqualified opinions that affect the documentation authenticity.

**Conclusion**

To sum up, organizations require disaster recovery plans for unplanned emergencies and business continuity. A disaster recovery plan contains a policy protecting the business's infrastructure from further damage by taking the necessary steps to recover. A disaster recovery plan reduces the disaster impact but cannot save the company from disasters. Therefore, a disaster recovery team is essential in developing a strategy that aligns with the business's primary needs. The group consists of the top managerial as the members and lower administrative staff as team members. The disaster recovery team is essential during and after the disaster strikes to ensure safety and immediate business continuity. However, a business should have a disaster plan for various disasters to prevent intense damage. A disaster recovery plan is cost-efficient, scalable, increases productivity, and improves customer retention. Lastly, documentation is essential to know the causes of the disaster, the disaster recovery procedures are taken, and their effectiveness. The documentation contains information from the time the disaster recovery team gets notified about the emergency to the end, where everyone is safe. In addition, the record helps in learning from past events and making better disaster recovery plans.

Reference

Alawanthan, D., Dorasamy, M., & Raman, M. (2017, July). Information Technology Disaster Recovery process improvement in the organization. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.

Baylis, P., & Boomhower, J. (2019). *Moral hazard, wildfires, and the economic incidence of natural disasters* (No. w26550). National Bureau of Economic Research.

Dhillon, G. (2021). Retrieved 10 August 2021, from <https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf>.

*Documentation in Disaster Management - Where do we start?*. Jensen Hughes. (2021). Retrieved 11 August 2021, from <https://www.jensenhughes.com/insights/documentation-in-disaster-management-where-do-we-start>.

Felter, B. (2021). *How to Build a Disaster Recovery Team Full of the Right People*. Vxchnge.com. Retrieved 10 August 2021, from <https://www.vxchnge.com/blog/disaster-recovery-team>.

*ISO 24762 Information Technology – Security Techniques Guidelines for Information and Communications Technology Disaster Recovery Services*. Pecb.com. (2021). Retrieved 11 August 2021, from <https://pecb.com/whitepaper/iso-24762-information-technology--security-techniques-guidelines-for-information-and-communications-technology-disaster-recovery-services>.

Mansell, H. (2017). The disaster control plan. In *Disaster management for libraries and archives* (pp. 30-57). Routledge.

Rom, A., & Kelman, I. (2020). Search without rescue? Evaluating the international search and rescue response to earthquake disasters. *BMJ global health*, *5*(12), e002398.

Wallace, M., & Webber, L. (2017). *The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets*. Amazon.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of incident response and disaster recovery*. Cengage Learning.