Disaster Recovery Plan(DRP)

Lucas Jones
Nocturnal Sentinel
1234 Fake Street
Mooresville, ST 12345

Company Name: Nocturnal Sentinel

Plan Version: 1.0

Last Updated: October 25th, 2024

Prepared by: October 25th, 2023

---

1. Introduction

1.1 Purpose

The Disaster Recovery Plan (DRP) is the procedures for responding to unforeseen events that disrupt business at Nocturnal Sentinel. This plan aims to minimize the impact and risk on our services, clients, and operations. The purpose is to have this before anything happens so we are prepared.

1.2 Scope

This DRP covers critical systems and processes related to the company's IT infrastructure, data management, and client services. The data of our users and company is critical.

---

2. Risk Assessment

2. Risk Assessment

Overview of Risks

Understanding potential risks that could take place is how we develop a robust DRP. Below are key risks that could impact Nocturnal Sentinel along with strategies to mitigate them.

Identified Risks and Mitigation Strategies

- Cybersecurity Threats: Risks from malware, phishing, and other attacks pose a high impact on our operations. To mitigate these risks, we will implement strong firewalls, conduct regular security training for employees, and utilize intrusion detection systems (IDS).
- Natural Disasters: Events such as earthquakes, floods, or hurricanes can severely disrupt business operations. To prepare, we will develop an offsite data backup strategy and establish partnerships with recovery centers.
- System Failures: Hardware or software failures may lead to downtime, categorized with a medium impact level. To address this, we will maintain an inventory of spare hardware and implement routine system maintenance checks.
- Human Error: Mistakes by employees that could lead to data loss also have a medium impact. To reduce these risks, comprehensive training will be provided, along with clear protocols for data management and system usage.
- Supply Chain Disruptions: Interruptions from third-party vendors can also impact operations. We will mitigate this by diversifying our suppliers and maintaining clear communication channels with them.

Risk Evaluation Process

1. Identify Assets: List critical systems and data that require protection.
2. Assess Vulnerabilities: Analyze potential weaknesses in current systems and processes.
3. Evaluate Impact: Determine the potential impact of identified risks on business operations.
4. Prioritize Risks: Rank risks based on their likelihood and potential impact to focus on the most critical areas.

Sure! Here's a revised version of the Risk Assessment and Key Roles and Responsibilities sections without using tables:

---

2. Risk Assessment

Overview of Risks

Understanding potential risks is crucial for developing a robust DRP. Below are key risks that could impact Nocturnal Sentinel along with strategies to mitigate them.

Identified Risks and Mitigation Strategies

- Cyberwar Attacks: Risks from malware, phishing, and other attacks pose a critical impact on our operations. To mitigate these risks, we will implement strong firewalls, conduct regular security focuses for employees, and utilize intrusion detection systems (IDS). We will also have software that is approved before downloading.

- Natural Disasters: Earthquakes, floods, or hurricanes can severely disrupt business operations. To prepare, we will develop an offsite data backup strategy and establish partnerships with recovery centers. We will have robust backup power solutions.
- System Failures: Hardware or software failures may lead to downtime, this is a medium impact level. To address this, we will maintain an inventory of spare hardware and implement routine system maintenance checks. If you have any issues please submit a ticket.
- Human Error: Mistakes by employees that could lead to data loss also have a medium impact. To reduce these risks, comprehensive training will be provided, and clear protocols for data management and system usage.
- Supply Chain Disruptions: vendors can also impact operations. We will mitigate this by diversifying our suppliers and maintaining clear communication channels with them. We will also research our vendors and keep updated information on them.

Risk Evaluation Process

1. Identify Assets: List critical systems and data that require protection.
2. Assess Vulnerabilities: Analyze potential weaknesses in current systems and processes.
3. Evaluate Impact: Determine the potential impact of identified risks on business operations.
4. Prioritize Risks: Rank risks based on their likelihood and potential impact to focus on the most critical areas.

---

4. Key Roles and Responsibilities

Overview of Roles

Effective DPR requires a clear understanding of roles and responsibilities among team members. Here are key roles essential for the successful execution of the DRP.

Roles and Responsibilities

- Disaster Recovery Coordinator: This individual oversees the implementation of the DRP and ensures that all team members are trained and prepared for their responsibilities.
- IT Security Specialist: Responsible for managing cybersecurity measures, monitoring for threats, and implementing security protocols to safeguard our systems.
- Business Continuity Planner: This role focuses on aligning the DRP with broader business continuity strategies and conducting impact analyses to ensure that critical functions remain operational.
- Operations Manager: Coordinates recovery efforts with operational teams to ensure minimal disruption during a disaster.
- Communication Liaison: This person is responsible for internal and external communications during a disaster, keeping stakeholders informed about recovery progress and actions being taken.

Collaboration and Communication

Regular meetings will be scheduled monthly to discuss updates on the DRP and any potential risks. Additionally, a feedback loop will be established for team members to provide input on the DRP and suggest improvements. We will have monthly meetings to discuss the DRP.

3. Recovery Objectives

- Recovery Time Objective (RTO): 4 hours
- Recovery Point Objective (RPO): 1 hour

---

5. Disaster Recovery Procedures

5.1 Incident Detection

- Monitor systems for alerts indicating a disaster or breach.
- Employees must report incidents immediately to the IT Lead.

5.2 Activation of the DRP

- The DPR Manager will evaluate the incident and decide whether to activate the DRP.

5.3 Recovery Steps

1. Data Restoration:
    - Use the latest backups stored in the cloud.
    - Ensure all data is restored within the RPO timeframe.
2. System Recovery:
    - Reboot affected systems and restore configurations.
    - Verify that all critical applications are operational.
3. Communication:
    - Notify clients and stakeholders about the incident and recovery progress via email and website updates.

---

6. Training and Testing

- Training Schedule: Quarterly training sessions for all employees on DRP protocols and responsibilities.
- Testing Plan: Conduct annual DRP drills to test response times and system recovery procedures.

---

7. Plan Review and Maintenance

This DRP will be reviewed and updated annually or after any significant incident to ensure its effectiveness and relevance. We will keep the DRP updated and make sure to stay up to date.

Conclusion

Nocturnal Sentinel is committed to maintaining business continuity through effective disaster recovery strategies. By implementing this DRP, we aim to protect our clients, employees, and assets against unforeseen disruptions. This is our plan to fall back to durning a disaster.