Disaster Recovery Plan

Policy Statement: This Cybersecurity Disaster Recovery Plan has been established to provide a clear framework for responding to Ransomware/Malware attacks. The primary objective is to ensure the swift restoration of operations while upholding the highest standards of professionalism and ethical conduct.

Plan Overview:

- **Policy Statement:** Established a clear policy statement outlining the purpose and objectives of the disaster recovery plan.
- **Recovery Time Objective (RTO):** Set an ambitious RTO of less than 2-4 hours to minimize downtime.
- **Work Recovery Time (WRT):** Ensured a maximum WRT of 1 hour to swiftly resume critical operations.
- **Recovery Point Objective (RPO):** Determines an RPO of 24 hours for optimal data recovery.

Key Steps:

- **Initial Response:**

    - **Isolate Affected Systems:** Immediately disconnect all devices from the internet to prevent further spread.
    - **Secure Network:** Reset routers to factory settings to eliminate potential vulnerabilities.
    - **Safe Mode Activation:** Boot all systems in safe mode to limit malware activity.

- **Malware Identification and Removal:**

    - **Malware Analysis:** Identify the type of malware through rigorous analysis.
    - **Multi-Scanner Approach:** Conduct thorough scans using multiple reputable anti-malware programs.
    - **Complete Removal:** Persistently scan and remove malware until no detections are found.

Recovery Resources:

- **Hot Site Preparation:** Recommended the establishment of a Hot Site to facilitate rapid recovery.
- **VPN Implementation:** Utilize a secure VPN connection for remote access during recovery.
- **Data Backup:** Regularly back up essential files to ensure data integrity and availability.

- **Incident Notification:** Promptly notify the Chief Information Security Officer (CISO) and all affected users.

Achievements:

- Successfully designed a comprehensive disaster recovery plan to safeguard against Ransomware/Malware attacks.
- Defined precise recovery objectives, minimizing downtime and data loss.
- Demonstrated the ability to handle critical incidents while adhering to ethical and professional standards.

Note: This project was undertaken with a strong commitment to ethical cybersecurity practices and the utmost consideration for legal and organizational guidelines. The name "ScriptKiddies" used in the initial description has been replaced with a more professional and credible identity. The presented plan is a concise and structured outline of a disaster recovery strategy tailored to address cybersecurity threats effectively and efficiently.