Disaster Recovery Plan: Abramek, Inc.

1. DRP Overview

Introduction

This document functions as the Disaster Recovery Plan (DRP) for Abramek, Inc., presenting a comprehensive strategy aimed at restoring standard operations after a disruptive event. It supplements the current Business Continuity Plan (BCP), Business Impact Analysis (BIA), and Incident Response Plan (IRP) by outlining the post incident recovery process. It provides the necessary steps to reinstate crucial business functions, data, and infrastructure. DRP aims to attain regular operations while reducing downtime.

Major Goals:

Ensuring the safety of IT personal and of live during emergencies

Minimize downtime and data loss to maintain business continuity of IT services.

Efficiently restore critical systems an operations following a disaster

Provide regular DRP updates

Test the DRP to ensure effectiveness in the IT environment

Key Personnel:

Easy flow of information is a key to a successful Disaster Recovery at Abramek, Inc. A full contact list of key members and team owners can be obtained from the Configuration Management Plan (CMP). For major disaster emergencies contact:

Chief Technology Officer (CTO) | Kamil Abramek – kamilabramek@abramek.com

Communication Protocol:

During the recovery phase, maintaining consistent communication is vital. The Disaster

Recovery Plan (DRP) outlines precise communication protocols to ensure timely updates for all involved parties, which include:

- Regular updates provided to management, staff, and Recovery Teams
- Timely notifications extended to customers, partners, and media
- Strategically managing external communications to uphold brand reputation

Master List of Critical IT Application and Assets:

CMP provides all information required to successfully configure all assets with the current company standards and regulations, to include:

- List of backup assets and resources available to rebuild data centers, networking equipment and server
- Configuration diagrams for site set-up
- Full inventory profile of IT hardware and software (Version, License Keys, Geo-Locations)

Information Services Backup Procedures:

- Alternate hot site setup with redundant servers and networking infrastructure
- Scheduled backups of critical data and configurations
- Off-site storage or cloud backups
- Constant monitoring of backup system health
- Server backups are conducted daily at 2:00 AM
- Database backups are performed hourly during business hours
- Backup data is stored on redundant off-site servers

Emergency Disaster Response Procedures

- Procedures for shutting down critical systems in emergencies

- Evacuation routes
- Emergency contact lists

Disaster Site Rebuilding:

- Floor plan of the IT data center including rack layouts and equipment placement
- Assessment of hardware needs and alternatives for rebuilding IT infrastructure
- Data center specifications: square footage, power requirements, cooling systems, and security measures

Recovery Action Procedures

1. Prioritized recovery based on criticality of the system
2. Procedures for restoring data and software to reduce downtime
3. Transparent Communication Plan to inform key stakeholders and sponsors about the recovery process

Recovery Stages

Stage 1: Assessment and Activation

- Asses the severity of the damage
- Kickstart the recovery plan and gather our Recovery Teams
- Securing our main site and systems while keeping everyone in the loop

Stage 2: Infrastructure Restoration

- Restoring vital infrastructure
- Data retrieval from backups
- Eliminate vulnerabilities, apply necessary patches, and secure networks

Stage 3: Recovery of Business Functions

- Prioritizing essential business operations taking the BIA into consideration

- Recovering critical business functions

Stage 4: Transitioning to Normal Operation

- As things stabilize, operations will be shift back to the main site

  (In case of damage beyond the point of restoration a Reconstruction Plan will be initiated)
- A detailed review and lessons learned conducted
- Regular testing and evaluation of DR plan components including failover and restoration procedures.
- Update the DRP based on findings

2. Business Resumption

We'll customize recovery plans for each business function based on the priorities identified in the Business Impact Analysis (BIA). Our recovery teams will follow predetermined Business Continuity Plan (BCP) strategies to promptly and effectively restart essential operations. These strategies might involve:

- Remote access: Allowing employees to work from remote locations using cloud-based apps or VPN connections.
- Alternate site utilization: Activating designated alternate site(s) equipped with pre-configured systems and replicated data.
- Collaboration with third-party providers: Partnering with external vendors to temporarily support vital functions.
- Contract fulfillment: Contracting out current Abramek, Inc., operations while still maintaining full control

Depending on the circumstance, Abramek, Inc., will utilize the following until adequate systems restoration:

- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)

3. Safeguarding Organization's Information

By combining BCP, BIA, and IRP methodologies with this DRP, we ensure comprehensive information security. Key protective measures include:

- Regular data backups: Maintaining offsite backups in various locations to mitigate the risk of data loss
- Access controls: Enforcing strict access controls and user authentication for critical systems
- Data encryption: Encrypting sensitive data both at rest and during transmission to safeguard against unauthorized access
- Vulnerability management: Consistently updating software and patching vulnerabilities to eliminate potential cyber threats
- Incident response readiness: Ensuring a well-trained and equipped Incident Response Team is in place for swift threat mitigation

4. Lessons Learned

In the process of planning and implementing the DRP, it's essential to document and assess lessons learned. This practice enhances future readiness and enhances the efficacy of the plan. Key aspects of post-incident analysis include:

- Identifying deficiencies and vulnerabilities: Examining DRP execution to pinpoint areas needing enhancement

- BCP, IRP, and BIA assessment and review : Evaluating the effectiveness of BCP strategies, BIA priorities based on practical experience and effectiveness of IRP
- Testing and training enhancements: Fine-tuning testing protocols and conducting additional training sessions to address identified shortcomings
- Knowledge sharing: Disseminating lessons learned throughout the organization to bolster overall readiness

Conclusion

In conclusion, the Disaster Recovery Plan underscores the critical importance of safeguarding data in today's digitally reliant business landscape. With downtime incidents affecting a significant majority of organizations and the potential financial and reputational repercussions, having a robust DRP is indispensable. Built upon foundational documents like the Business Impact Analysis (BIA), Business Continuity Plan (BCP), and Incident Response Plan (IRP), the DRP is tailored to organization’s needs. It encompasses comprehensive strategies for restoring operations, ensuring information security, and post-incident analysis. By continuously documenting lessons learned, evaluating effectiveness, and enhancing preparedness through testing and training, Abramek, Inc., can navigate past disruptions and resume operations, safeguarding its data, continuity, and reputation

References

7 reasons you need a disaster recovery plan. Complete Technology Solutions. (n.d.). https://ctscomplete.com/7-reasons-you-need-a-disaster-recovery-plan/

Rock, T. (2023, March 27). *Know key disaster recovery statistics and save your business*. Invenio IT. https://invenioit.com/continuity/disaster-recovery-statistics/

Walker, R. (2023, January 17). *4 phases of every successful Disaster recovery plan*. Coruzant Technologies. https://coruzant.com/business/4-phases-of-every-successful-disaster-recovery-plan/

What is a disaster recovery plan?. Kyndryl. (n.d.). https://www.kyndryl.com/us/en/learn/disaster-recovery-plan#:~:text=A%20disaster%20recovery%20plan%20(DR,and%20any%20other%20disruptive%20events.