title: "ROAR Business Continuity and Disaster Recovery" subject: "ROAR Business Continuity and Disaster Recovery" keywords: [ROAR, Business Continuity, Disaster Recovery] lang: "en" ...

Version: `1.9`
Last Updated by Commit: `6c37d80bb76c7f409b4b1506c3ae0f8f6fa91ea8`
Last updated on: `2024-10-18 15:30:57`

> Note: This document is in draft form and is not currently enforced.

The Business Continuity and Disaster Recovery (BC/DR) Plan for ROAR outlines the processes and strategies in place to ensure the continuation of critical operations and the rapid recovery of essential services in the event of a disruption. The plan is designed to address a range of potential disruptions, including system failures, security incidents, natural disasters, and other unforeseen events that could impact ROAR's ability to provide its services.

The goal of the BC/DR plan is to minimize downtime, protect the integrity of data, and ensure that ROAR can continue to meet its obligations to educational partners, researchers, and other stakeholders.

1. Business Continuity Strategy

   The business continuity strategy focuses on maintaining essential services during disruptions and ensuring that ROAR can operate effectively even under adverse conditions. Key components of the strategy include:

   - Critical Service Identification: Identifying the critical services that must be maintained for ROAR to function. These services include:
     - Access to ROAR's platform for users (students, teachers, and administrators).
     - Data availability for research and reporting purposes.
     - Security controls to protect personal data and comply with privacy regulations.
   - Priority Levels: ROAR's services are classified into priority levels based on their criticality:
     - High-Priority Services: Services that must remain operational with minimal downtime, such as the core platform, data access for partners, and security monitoring systems.
     - Medium-Priority Services: Services that can withstand limited interruptions but must be restored within a specified time frame, such as non-essential reporting tools or background data processing.
     - Low-Priority Services: Services that can be temporarily paused during a crisis without immediate impact, such as development environments or non-critical internal tools.

- Alternate Operations Plan: In the event of a major disruption, alternative operational processes may be implemented, including:
  - Rerouting essential services to secondary infrastructure or cloud environments.
  - Temporarily reducing non-critical operations to focus on restoring high-priority services.

2. Disaster Recovery Plan

   The disaster recovery plan focuses on restoring normal operations as quickly as possible following a disruption. The plan ensures that ROAR can recover from hardware failures, system outages, cyberattacks, or other emergencies that could affect service availability.

   Key Elements of the Disaster Recovery Plan include:

   - Incident Response Coordination: In the event of a disaster, the incident response team will be activated to assess the scope of the disruption and implement the disaster recovery plan. This team is responsible for:
     - Coordinating the initial response.
     - Communicating with stakeholders.
     - Implementing restoration procedures.
   - Disaster Recovery Teams and Roles:
     - Incident Response Lead: Oversees the overall response effort, assesses the severity of the incident, and activates the disaster recovery plan.
     - Technical Recovery Team: Responsible for restoring the affected infrastructure, including servers, databases, and network components.
     - Communications Lead: Manages communication with internal teams, educational partners, and other stakeholders to ensure timely and transparent updates.
     - Data Integrity Officer: Ensures the integrity and security of data throughout the recovery process and works with the backup and restoration teams to validate data post-recovery.
   - Disaster Scenarios: The plan covers a variety of potential disaster scenarios, including:
     - System Failures: Hardware or software malfunctions that cause a loss of service.
     - Cyberattacks: Ransomware attacks, data breaches, or other malicious actions that disrupt service or compromise data.
     - Natural Disasters: Floods, fires, or other physical events that could damage infrastructure or data centers.
   - Recovery Time Objective (RTO): ROAR aims to restore critical services within 24 hours of a major disruption. Non-critical services may take up to 72 hours to fully restore.

- Recovery Point Objective (RPO): ROAR's objective is to recover data up to the point of the last successful backup. This ensures minimal data loss in the event of a system failure or other disaster.

3. Communication and Reporting Protocols

   Clear communication is critical during a disaster or significant disruption. ROAR's BC/DR plan includes the following communication protocols:

   - Internal Communication: Immediate notification to internal teams and key stakeholders about the nature and scope of the disruption. Regular updates are provided throughout the recovery process.
   - External Communication: ROAR will notify educational partners, researchers, and users in the event of a disruption that affects service delivery. These notifications will provide details on the nature of the incident, expected recovery times, and any potential impact on data or services.
   - Post-Recovery Reports: Once normal operations are restored, a detailed post-recovery report will be prepared. This report will include an assessment of the incident, the effectiveness of the recovery efforts, any data that was affected, and actions taken to prevent future incidents.

4. Testing and Updating the BC/DR Plan

   To ensure the effectiveness of the BC/DR plan, ROAR regularly conducts disaster recovery drills and business continuity simulations. These tests are conducted at least annually and involve:

   - Simulating various disaster scenarios.
   - Testing the recovery of critical systems.
   - Evaluating the response time and coordination among recovery teams.

   Additionally, the BC/DR plan is reviewed and updated as necessary to reflect changes in infrastructure, technology, or organizational priorities. Any lessons learned from real incidents or test exercises are incorporated into the plan to improve future responses.

5. Dependencies on Third-Party Services

   ROAR relies on several third-party services, including cloud infrastructure and security monitoring tools, to maintain its operations. As part of the BC/DR plan, ROAR ensures that:

   - Service Level Agreements (SLAs) with third-party vendors include clear recovery time commitments.
   - Third-party vendors have their own disaster recovery and business continuity plans that align with ROAR's requirements for service restoration.

- Continuous monitoring of third-party services is in place to detect potential disruptions and coordinate responses as needed.