

Disaster Recovery Plan Prologic Invoice Software

Disaster Recovery Plan for Prologic Invoice Software

1. Introduction

Purpose: This plan aims to ensure business continuity and minimize downtime for Prologic Invoice Software during disasters such as cybersecurity threats, technical issues, and data-related problems. The disaster recovery plan (DRP) provides a structured approach for responding to unforeseen events that could disrupt business operations. The goal is to restore normal business operations as quickly as possible, thereby minimizing financial loss and operational downtime.

Scope: This plan covers all disaster recovery aspects, including data protection, system recovery, communication, and business resumption activities. The scope encompasses all critical components of the Prologic Invoice Software infrastructure, including databases, applications, and network systems. It also involves coordination among various teams such as IT, management, support, and communications.

2. Risk Assessment and Business Impact Analysis

Potential Risks:

- ☐ **Cybersecurity Threats:** Cybersecurity threats pose significant risks to Prologic Invoice Software. These include:
 - ☐ **Malware:** Malicious software designed to damage or disrupt systems.
 - ☐ **Viruses:** Programs that can replicate and spread, causing harm to files and systems.
 - ☐ **Phishing Attacks:** Attempts to trick users into providing sensitive information.
 - ☐ **DDoS Attacks:** Distributed Denial of Service attacks that overwhelm systems with traffic.
- ☐ **Technical Issues:** Technical issues that could disrupt service include:
 - ☐ **Server Downtime:** Unplanned outages of server hardware or software.
 - ☐ **Slow Load Times:** Performance issues that degrade user experience.

☐ **Data-Related Issues:** Problems related to data integrity and security, such as:

- ☐ **Data Accuracy:** Ensuring the correctness of data.
- ☐ **Data Breaches:** Unauthorized access to sensitive information.
- ☐ **Backup Failures:** Inability to restore data from backups.
- ☐ **Data Integration Issues:** Problems with synchronizing data across systems.
- ☐ **Compliance:** Adhering to legal and regulatory requirements.

☐ **Impact Analysis:**

☐ **Critical Systems:** Identifying critical systems helps prioritize recovery efforts. For Prologic Invoice Software, these include:

- ☐ **Database Servers:** Storing and managing invoice data.
- ☐ **Application Servers:** Running the core software applications.
- ☐ **Network Infrastructure:** Ensuring connectivity and communication.

☐ **Recovery Time Objective (RTO):** 4 hours. This metric defines the maximum acceptable downtime for Prologic Invoice Software. In practical terms, the system should be restored and operational within 4 hours of disruption to avoid significant business impact.

☐ **Recovery Point Objective (RPO):** 1 hour. This metric specifies the maximum acceptable data loss measured in time. In the event of a failure, data recovery should restore information to a point no more than 1 hour before the incident, ensuring minimal data loss.

3. Define Recovery Objectives

- ☐ **Recovery Time Objective (RTO):** 4 hours. This indicates the maximum allowable time the system can be down without causing substantial business disruption. The RTO is critical for ensuring continuity and minimizing operational losses.
- ☐ **Recovery Point Objective (RPO):** 1 hour. This represents the maximum time frame within which data might be lost from an IT service due to a major incident. The RPO helps determine the frequency of backups and the speed of data recovery processes.

4. Backup Strategies

- ☐ **Frequency:** Daily backups are implemented to ensure data is regularly saved and can be restored if needed. Daily backups minimize the risk of data loss and ensure that the most recent information is available for recovery.
- ☐ **Storage:** Backups are stored both on-site and in cloud storage to provide redundancy and ensure data availability even if one storage location is compromised. On-site storage allows for quick access, while cloud storage offers an additional layer of security and availability.
- ☐ **Verification:** Automated tools, checksum verification, restore testing, backup logs review, and data integrity checks are used to ensure the backups are accurate and complete. Regular verification processes help identify and address issues with backups before they become critical.
- ☐ **Nodebalancer:** A tool used to distribute traffic across multiple servers to ensure smooth operations and avoid overloading a single server. Nodebalancers help maintain performance and availability, especially during high-traffic periods.

5. Communication Plan

- ☐ **Internal Communication:**
 - ☐ **Channels:** Communication channels for internal coordination include:
 - ☐ **Email:** Used for detailed communication and documentation.
 - ☐ **Phone:** For immediate notifications and critical updates.
 - ☐ **Messaging Apps:** For real-time updates and coordination.
 - ☐ **Steps:**
 - ☐ **Initial Notification:** Immediate phone call or messaging app notification to the IT and support teams. This step ensures that key personnel are aware of the incident and can begin response activities.

- ☐ **Status Updates:** Regular updates via email and messaging apps to keep all stakeholders informed of progress and any changes in the situation. Status updates help maintain transparency and coordination among team members.
- ☐ **Detailed Reports:** Follow-up emails with detailed information and action plans to ensure everyone understands the steps being taken and their roles. Detailed reports provide a comprehensive overview of the incident response and recovery efforts.

☐ **External Communication:**

- ☐ **Channels:** Communication channels for external stakeholders include:
 - ☐ **Email:** Direct communication with customers for critical updates.
 - ☐ **Website Notifications:** Banner or pop-up notifications on the website to inform users of ongoing issues and expected resolution times.
 - ☐ **Social Media:** Updates on platforms like Twitter, Facebook, and LinkedIn to reach a broader audience and provide real-time updates.
- ☐ **Steps:**
 - ☐ **Initial Notification:** Email to all affected customers with information about the disruption. This initial communication should include details about the nature of the incident, its impact, and expected resolution times.
 - ☐ **Status Updates:** Regular updates via email, website notifications, and social media to keep customers informed of progress and any changes in the situation. Status updates help manage customer expectations and maintain trust.
 - ☐ **Recovery Confirmation:** Final notification to inform customers when the issue is resolved and services are fully restored. Recovery confirmation should include details about the resolution, any steps customers may need to take, and assurances about future reliability.

Key Contacts:

| Role | Name | Phone Number | Email Address |
|---------------------|------------------|---|---|
| IT Team Lead | Muzzammil Kamaal | Landline: 01206860720 Mobile: 9555545345 | mmkamaal@prologicwebsolutions.com |
| Support Team Lead | Sohrab Alam | Landline: 01206860789 Mobile: 7004771608 | sohrab.alam@prologicwebsolutions.com |
| Management | Mayank Jain | Landline: 01206860710 Mobile: 9582794444 | admin@prologicwebsolutions.com |
| Communications Lead | Mufid Ansari | Landline: 01206860750 Mobile: 7827034330 | mufid@prologicwebsolutions.com |
| Customer Support | Ankur Parashar | Landline: 01206860789 Mobile: 9627680628 | ankur.parashar@dev.prologicwebsolutions.com |

6. Disaster Recovery Procedures

Steps to Restore Data:

1. Identify Affected Data:

- **Action:** Determine the scope of data loss or corruption. The first step involves assessing which data has been affected and the extent of the damage.
- **Responsibility:** IT Team Lead (Muzzammil Kamaal).

2. Access Backup Data:

- **Action:** Locate the most recent verified backup. This step involves retrieving the most current backup available to ensure minimal data loss.
- **Responsibility:** IT Team.

3. Verify Backup Integrity:

- **Action:** Check the integrity and completeness of the backup data. Verification ensures that the backup data is not corrupted and is complete.
 - **Responsibility:** IT Team.
 - 4. **Restore Backup Data:**
 - **Action:** Use backup tools to restore the data to the primary storage system. Restoration involves transferring the backup data to the main system to replace lost or corrupted data.
 - **Responsibility:** IT Team.
 - 5. **Validate Restored Data:**
 - **Action:** Verify the accuracy and completeness of the restored data. Validation ensures that the restored data matches the expected data set and is free from errors.
 - **Responsibility:** IT Team.
 - 6. **Notify Stakeholders:**
 - **Action:** Inform relevant stakeholders that data restoration is complete. Notification includes updates to internal teams and external customers about the successful restoration of data.
 - **Responsibility:** Communications Lead (Mufid Ansari).
- **Steps to Restore Services:**
 1. **Assess Impact:**
 - **Action:** Evaluate the extent of the service disruption. Impact assessment helps determine the severity of the incident and prioritize recovery efforts.
 - **Responsibility:** IT Team Lead (Muzzammil Kamaal).
 2. **Initiate Disaster Recovery Plan:**
 - **Action:** Activate the disaster recovery plan and notify the recovery team. This step involves mobilizing the recovery team and initiating predefined recovery procedures.
 - **Responsibility:** Management (Mayank Jain).

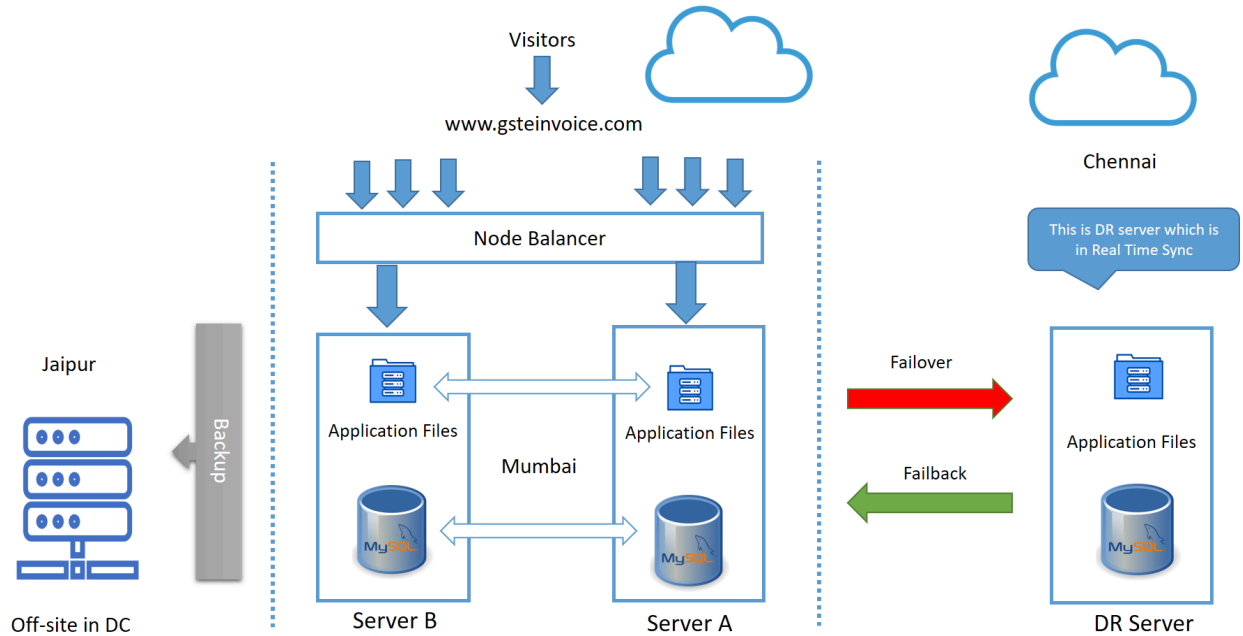
3. **Set Up Temporary Infrastructure:**
 - **Action:** Deploy temporary servers and infrastructure if necessary. Temporary infrastructure provides a stopgap solution to maintain services while permanent repairs are underway.
 - **Responsibility:** IT Team.
4. **Restore Application Services:**
 - **Action:** Reinstall and configure the Prologic Invoice Software. This step involves re-establishing the software environment and ensuring it operates correctly.
 - **Responsibility:** IT Team.
5. **Restore Network Connectivity:**
 - **Action:** Ensure all network connections are re-established and tested. Network restoration involves reconfiguring and testing network components to ensure connectivity.
 - **Responsibility:** IT Team.
6. **Perform System Tests:**
 - **Action:** Conduct thorough testing to ensure all services are functioning correctly. System testing includes verifying that all applications and systems are operating as expected post-recovery.
 - **Responsibility:** IT Team.
7. **Monitor System Performance:**
 - **Action:** Monitor the system closely for any issues post-restoration. Performance monitoring helps detect and address any residual issues that may arise after restoration.
 - **Responsibility:** IT Team.
8. **Communicate with Users:**
 - **Action:** Inform users that services have been restored and provide any necessary instructions. User communication ensures that all end-users are aware of the recovery and any steps they need to take.
 - **Responsibility:** Communications Lead (Mufid Ansari).

Roles and Responsibilities:

| Role | Responsibility |
|---------------------|---|
| IT Team Lead | Oversee restoration and coordinate team efforts. |
| IT Team | Execute data and service restoration, verify backups, and test systems. |
| Support Team Lead | Coordinate user communication and support. |
| Support Team | Assist users post-recovery and provide technical support. |
| Management | Activate plan, make decisions, and ensure coordination. |
| Communications Lead | Inform stakeholders to handle external communication. |
| Customer Support | Address customer inquiries and provide recovery status. |

7. Network Diagram

Network Diagram



Server Details

Configuration for Servers A, B, and DR Server:

- **DC Location:** Mumbai for Servers A and B, Chennai for DR Server
- **RAM:** 16 GB
- **CPU:** 8 Core
- **Storage:** 320 GB
- **Cloud Firewall**
- **DDOS Protection**
- **DNS Manager**
- **Server A IP:** 192.46.209.119 (Mumbai)
- **Server B IP:** 192.46.209.166 (Mumbai)
- **DR Server IP:** 172.235.28.201 (Chennai)

Node Balancer Details

Node Balancer Overview:

- ☐ **Role:** The node balancer is a crucial component in managing and distributing application traffic. It acts as a traffic cop, ensuring that incoming requests are efficiently distributed across multiple servers, optimizing performance and reliability.
- ☐ **Server Setup:** Two primary servers (Server A and Server B) are used in the node balancer setup, both having identical configurations.

Synchronization Mechanism:

- ☐ **File Synchronization:** Application files are synchronized between Server A and Server B every 5 minutes, ensuring consistency and availability.
- ☐ **Database Synchronization:** Using MySQL Master-Slave architecture, the database is continuously synchronized in real-time between Server A and Server B, maintaining data integrity and consistency.
- ☐ **Bidirectional Sync:** Both servers are in bidirectional sync to ensure that changes in one server are reflected in the other, providing high availability and fault tolerance.

Backup Process

- ☐ **Daily Backup:** A daily backup process is in place, where data from Server A is backed up both on-server and off-server, providing multiple layers of security.
- ☐ **Data Security:** This process ensures that data is secure and recoverable, safeguarding against data loss due to hardware failures, software issues, or other unforeseen events.

Disaster Recovery Server (DR Server)

DR Server Configuration:

- ☐ **Location:** Chennai
- ☐ **RAM:** 16 GB
- ☐ **CPU:** 8 Core
- ☐ **Storage:** 320 GB
- ☐ **Cloud Firewall**
- ☐ **DDOS Protection**
- ☐ **DNS Manager**
- ☐ **IP Address:** 172.235.28.201

Key Features:

- ☐ **Spare Server:** The DR Server serves as a disaster recovery server, providing a failover option if Servers A or B experience failures.

- ☐ **Unidirectional Sync:** The DR Server is unidirectionally synced with Server A, ensuring that it has the latest data and application files within a 24-hour cycle.
- ☐ **Real-time Database Sync:** The database synchronization is maintained in real-time, ensuring data consistency between Server A and the DR Server.
- ☐ **Minimal Downtime:** In the event of a disaster, the only required action is to point the domain to the DR Server's IP address, minimizing downtime and ensuring rapid recovery.

8. Preventative Measures and Maintenance

- ☐ **Regular Audits and Testing:** Conduct regular audits and testing of the disaster recovery plan to ensure its effectiveness. This includes simulating disaster scenarios to evaluate response and recovery processes. Regular audits help identify potential weaknesses in the plan and provide opportunities for improvement.
- ☐ **Employee Training:** Regular training sessions for employees on disaster recovery procedures and protocols. Training ensures that all team members are aware of their roles and responsibilities in the event of a disaster.
- ☐ **System Updates and Patches:** Regularly update and patch systems to protect against vulnerabilities. Keeping systems up-to-date reduces the risk of technical failures and cybersecurity threats.
- ☐ **Backup Verification:** Regularly verify the integrity and completeness of backups to ensure they can be used for restoration. Backup verification involves testing backups to ensure they are not corrupted and contain all necessary data.
- ☐ **Redundancy and Failover Systems:** Implement redundancy and failover systems to ensure continuous operation during a disaster. Redundancy and failover systems provide additional layers of protection and help maintain service availability.
- ☐ **Physical Security Measures:** Ensure physical security measures are in place to protect data centers and infrastructure. Physical security includes access controls, surveillance, and environmental controls to safeguard equipment and data.
- ☐ **Review and Update DR Plan:** Regularly review and update the disaster recovery plan to reflect changes in the business environment, technology, and organizational structure. Regular reviews ensure that the plan remains relevant and effective.

Valid from: 20-June-2024