Digester Recovery Plan (DR Plan)

For

Prime Bank E-Signature

Version 1.0.0

**Submitted to**



Prime Bank PLC

**Prepared By:**



SoftCafe IT Solution Limited

BTI Premier Plaza Progoti Sharani Dhaka 1012.

Email:[info@softcafesolution.com](mailto:info@softcafesolution.com)

website:[www.softcafesolution.com](http://www.softcafesolution.com)

**1. Purpose**

The purpose of this Disaster Recovery Plan (DRP) is to ensure the continuity of operations for the bank’s signature management system, which stores physical bank signatures and digital personal information in the database, in the event of a disaster. This plan aims to mitigate risks, recover data, and minimize downtime.

**2. Scope**

This plan covers the application, database, and physical storage systems involved in storing bank signatures and personal information. It includes procedures for recovering both the digital data and the physical files.

**3. Risk Assessment**

Possible risks to the system include:

* **Natural disasters** (floods, fires, earthquakes)
* **Hardware failures** (server crashes, storage device failures)
* **Cyber-attacks** (data breaches, ransomware)
* **Human errors** (accidental deletion or misplacement of physical files)

**4. Recovery Objectives**

* **RTO (Recovery Time Objective):** The maximum acceptable time for system recovery is 4-8 hours.
* **RPO (Recovery Point Objective):** The maximum acceptable data loss is 24 hours (daily backup).

**5. Backup and Recovery Strategy**

**5.1 Digital Data (Database)**

* **Regular backups:** Perform daily backups of the database to a secure, offsite location (cloud storage or a secondary data center).
* **Incremental backups:** Take incremental backups every 4 hours to reduce the risk of data loss.
* **Backup verification:** Perform regular checks to ensure backups are complete and usable.
* **Automated backup system:** Set up automated backup jobs and monitor them to ensure they run as scheduled.
* **Backup Responsibility:** Prime Bank will take the backup.

**5.2 Physical Signatures (Folders)**

* **Offsite storage:** Store backup physical copies of the signatures in a separate, secure location.
* **Environment monitoring:** Ensure that physical storage environments have temperature, humidity, and fire/smoke detection systems to prevent damage to the signatures.
* **Backup Responsibility:** Prime Bank will take the backup.

**6. Recovery Process**

**6.1 Database Recovery**

1. **Identify the failure:** Determine if the failure is caused by a hardware issue, software bug, or cyber attack.
2. **Restore from backup:** Restore the latest backup (incremental or full) to the primary database server. Prime Bank to confirm the database restore.
3. **Validate data integrity:** Run integrity checks to ensure no corruption during the restore process.
4. **Test the system:** Ensure that the restored database is fully functional before bringing it back online.

**6.2 Physical Signature Recovery**

1. **Identify damaged or lost files:** In the event of physical damage to signatures, identify the extent of the damage.
2. **Retrieve digital backups:** If available, use the scanned digital copies to reproduce the lost or damaged physical signatures.
3. **Reprint signatures:** Use high-quality printers to recreate the physical versions, ensuring they meet the necessary security and compliance standards.
4. **Audit storage facilities:** Regularly review and audit physical storage facilities to ensure that preventive measures are in place.

**7. Communication Plan**

* **Internal team communication:** Set up communication channels for informing the IT team, support staff, and management about the disaster recovery progress.
* **Bank communication:** Notify key bank stakeholders about the nature of the disaster, expected recovery time, and any interim measures taken to secure data.
* **Customer notification:** In case customer data is affected, communicate transparently about the recovery efforts and any impact on their services.

**8. Testing the Plan**

* Perform regular disaster recovery drills to ensure the team is prepared for different scenarios.
* Update the plan periodically, especially after system changes or significant infrastructure updates.

**9. Roles and Responsibilities**

* **Disaster Recovery Manager:** Oversees the DRP execution and ensures compliance with procedures.
* **Database Administrator:** Responsible for database backup and restoration.
* **IT Support Team:** Handles physical and digital infrastructure issues and maintains the system.
* **Compliance Officer:** Ensures adherence to regulatory requirements regarding data protection and recovery.

**10. Conclusion**

The bank signature management system’s disaster recovery plan ensures that personal information and physical signatures can be restored efficiently after a disaster. By regularly backing up data, safeguarding physical files, and preparing for different failure scenarios, the system can minimize downtime and maintain data integrity.