University of
SCIENCE
& ARTS
of Oklahoma

# USAO IT Disaster Recovery Plan

## 1. Overview

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect non-public personal information (NPI) and implement safeguards to ensure the security, confidentiality, and integrity of customer information. This IT Disaster Recovery Plan (DRP) is designed to help USAO recover critical IT systems and data in the event of a disaster, while ensuring compliance with GLBA.

## 2. Objectives

- Ensure rapid recovery of critical IT systems in the event of a disaster to minimize downtime.
- Protect and restore non-public personal information (NPI) as required by GLBA.
- Provide clear recovery processes to mitigate the impact on business operations.
- Maintain GLBA compliance through secure backup, recovery procedures, and safeguarding customer information.

## 3. Scope

This DRP applies to all IT systems, applications, networks, databases, and personnel responsible for the protection and recovery of non-public personal information. It covers all types of disaster events, including natural disasters, cyberattacks, power outages, and hardware failures.

## 4. Roles and Responsibilities

**Disaster Recovery Team (DRT)**

The Disaster Recovery Team (DRT) is responsible for executing this plan and ensuring timely restoration of critical IT systems. The team includes:

- **Disaster Recovery Manager**: Oversees the disaster recovery process and ensures the plan is executed according to procedures. This role is filled by the Director of IT. The Director of IT sends communications to all relevant stakeholders consisting of upper leadership at USAO, campus security personnel, offsite backups vendors, and/or other personnel as deemed necessary. This applies to all disaster response phases.
- **IT Infrastructure Lead**: Responsible for the recovery of data centers, servers, networks, and other critical IT infrastructure. This role is filled by the Director of IT.
- **Application Recovery Lead**: Ensures that key applications, especially those involving NPI, are restored to working order. This role is filled by the Assistant to Director of IT or the Senior Technician.
- **Backup Administrator**: Manages the restoration of data from backups, ensuring that sensitive customer data is protected and restored securely. This role is filled by the Assistant to Director of IT or the Senior Technician.
- **Business Continuity Coordinator**: Ensures business operations are maintained or quickly resumed and coordinates with the DRT for resource allocation. This role is filled by the Director of IT.

## 5. Risk Assessment and Business Impact Analysis (BIA)

**Risk Assessment**

Identify potential risks that could result in a disaster, including:

- Cyberattacks (e.g., ransomware, data breaches)
- Hardware failures
- Natural disasters (e.g., floods, fires, earthquakes)
- Utility failures (e.g., power outages, network disruptions)
- Human errors

**Business Impact Analysis (BIA)**

The BIA identifies the potential impacts of an IT disaster and prioritizes systems for recovery based on:

- **Recovery Time Objective (RTO)**: The maximum acceptable time for system restoration. This is currently **48** hours.
- **Recovery Point Objective (RPO)**: The maximum acceptable amount of data loss, in terms of time (e.g., one hour of lost data). This is currently **4** hours.
- **Critical Systems**: Systems that store or process NPI or are vital for business operations. These are prioritized in the recovery process. These systems include those that are under USAO's on-premise infrastructure such as domain controllers, print server/manager, ID card authentication.

## 6. Disaster Recovery Sites and Infrastructure

**Primary and Secondary Data Centers**

- **Primary Data Center**: The main location where critical systems, applications, and NPI are hosted. This is currently OneNet's datacenter in Oklahoma City.
- **Secondary/Backup Data Center**: An off-site location used to store backups and run failover systems. This site is crucial for disaster recovery to ensure continued operations if the primary data center is compromised. This is currently Cove's datacenter in Las Vegas, NV.

**Cloud-Based Backup Solutions**

Cloud-based infrastructure is used for real-time data backups and quick recovery. These services comply with GLBA to ensure customer data remains encrypted and secure during transmission and storage.

## 7. Backup and Recovery Procedures

**Data Backup**

- **Frequency**: Hourly backups of critical systems and databases that store NPI.
- **Types of Backups**: Full backups are performed weekly, with incremental backups performed daily.
- **Backup Locations**: Backups are stored in the secondary data center and in encrypted cloud environments to ensure redundancy and accessibility.
- **Retention Policy**: Backups are retained in accordance with regulatory requirements and internal policies. Data containing NPI is securely disposed of after the retention period.

**Data Encryption**

To comply with GLBA, all NPI in transit and at rest (in backups) must be encrypted using industry-standard encryption protocols. Only authorized personnel have access to encryption keys.

**Testing of Backup and Recovery**

- **Testing Frequency**: Disaster recovery procedures, including data restoration from backups, are tested semi-annually to ensure readiness.
- **Testing Scenarios**: Simulated disaster scenarios such as cyberattacks, natural disasters, and hardware failures are tested. The test results are reviewed to improve the plan and ensure compliance with GLBA.
- **Documentation**: Results from disaster recovery tests are documented and made available for audit purposes.

## 8. Disaster Response Phases

**Phase 1: Activation of the DRP**

- **Incident Identification**: The DRT identifies a disaster or outage that could impact critical IT systems or NPI.
- **DRT Mobilization**: The DRT is immediately mobilized to assess the damage and start recovery efforts.
- **Damage Assessment**: The team assesses the extent of damage and prioritizes system recovery based on the BIA and criticality of systems.

- **Notification**: Internal and external stakeholders, including senior management and regulatory bodies, are notified as appropriate.

**Phase 2: Containment**

- **Isolate Affected Systems**: If the disaster involves a cyberattack or system compromise, affected systems are isolated to prevent further damage.
- **Secure Backup Systems**: Verify the integrity and security of backup systems to ensure they have not been compromised.

**Phase 3: Restoration and Recovery**

- **Initiate Failover Systems**: Transfer operations to backup systems, either in the secondary data center or cloud environment, depending on the extent of the damage.
- **Restore Data**: Critical data, including NPI, is restored from secure backups based on the RTO and RPO. Data integrity is verified during restoration to ensure compliance with GLBA.
- **System Verification**: After restoration, all systems are tested to ensure they are fully operational, secure, and compliant with regulatory requirements.

**Phase 4: Business Resumption**

- **System Recovery**: Ensure all critical IT systems and NPI processing systems are restored to normal operation.
- **Customer Notification**: If customer data has been compromised or affected, notification to customers must be made in accordance with GLBA's privacy and breach notification requirements.
- **Regulatory Notification**: In the event of a data breach involving NPI, regulatory bodies (e.g., the FTC or state agencies) must be notified as required by law.

## 9. Post-Disaster Activities

**After-Action Report**

- **Incident Documentation**: A complete report documenting the disaster, the response actions, and the recovery process is created. This will include timelines, systems affected, customer data involved, and lessons learned.
- **Lessons Learned**: The DRT conducts a post-incident review to assess what went well and what could be improved. This includes reviewing recovery timelines, success of backup restoration, and compliance with GLBA.
- **Post Incident Review**: Steps for mitigation to prevent similar disaster in the future.

**Plan Updates and Continuous Improvement**

- **Plan Review**: Based on the post-incident review, the DRP is updated to address any weaknesses or gaps identified during the disaster recovery process.
- **Audit and Compliance Check**: An internal audit is conducted to ensure the recovery process met GLBA requirements. External audits may also be conducted as part of regulatory compliance.

## 10. Training and Awareness

- **Employee Training**: All employees are trained on disaster recovery procedures and their role in the event of a disaster.
- **DRT Training**: The Disaster Recovery Team undergoes specialized training annually to ensure they are prepared to execute the DRP effectively.
- **Awareness Campaigns**: Regular awareness campaigns are conducted to keep all personnel informed about the DRP and the importance of compliance with GLBA.

## 11. Plan Maintenance and Review

This IT Disaster Recovery Plan will be reviewed annually or after any major incident to ensure it is aligned with current business operations, technological changes, and evolving GLBA requirements. Any updates to the plan must be approved by senior management and communicated to all relevant stakeholders.

## 12. Contact Information

**Disaster Recovery Manager**

- Name: Adeel Siddiqui

- Email: asiddiqui@usao.edu
- Phone: 45-574-1319

Revision History:
Last updated – May, 2025