Disaster Recovery Plan Policy for the Y Bank

Made by: Noor Hamed

SECTION(1)

Table of Contents

1. overview

Since disasters are so rare, it is important to understand that having a contingency plan provide the Y Bank a competitive advantage.

This policy requires management to financially support and rigorously manage disaster contingency planning efforts. Any occurrence that might result in an extended delay in service should be considered. The Disaster Recovery Plan is usually included in the Business Continuity Plan.

2. Purpose

The purpose of this Disaster Recovery Plan Policy is to ensure that The Y Bank is ready to respond to any disruptive incidents, such as natural disasters, cyber attacks, or system failures, in a timely and structured manner. This policy defines the requirement for a baseline disaster recovery plan which will be implemented by the Y Bank that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

3. Scope

The scope of this policy includes IT Management Staff, all critical IT systems, data, and services housed within the Data Center Department at the Bank. It applies to all personnel within the department and outlines the responsibilities and procedures to be followed in the event of a disaster or disruptive incident.

4. Policy

4.1Contingency Plans

4.1.1Computer Emergency Response Plan

Contact Information:

In the event of a computer emergency, the following individuals and entities are to be contacted:

Security Team(CISO, SOC Manager, and IRT)

IT Manager

Network Administrator

System Administrators

External IT Support Provider

Bank Management

External Contacts

Emergency Contact Procedures: In case of physical emergencies

Vendors and Service Providers: For hardware/software issues.

Insurance Providers: To report incidents for coverage.

Local Authorities (if necessary)

- The procedures that must be followed:

Security Breach:

Step 1: Isolate Affected Systems

- Disconnect compromised systems from the network to prevent further spread.

Step 2: Notify Security Team

- Contact the Security Team immediately to begin assessment and containment.

Step 3: Assess the Breach

- Determine the scope and nature of the breach, identifying affected data and systems.

Step 4: Implement Mitigation

- Apply necessary patches ,like change passwords, and enhance security measures.

Step 5: Document and Report

- Record the incident details and report to the DPO and Compliance Officer.

Immediate Actions:

Immediate actions to be taken in the event of certain occurrences include:

-Data Breach: Activate incident response team, contain the breach, and notify affected parties

-Natural Disaster: Secure data center facilities, assess damage, and implement recovery procedures

-Cyber Attack: Isolate affected systems, mitigate attack, and restore services

-Power Outage: Activate backup power systems, monitor systems, and initiate recovery process

4.1.2 Succession Flow of Responsibility

1.Immediate Supervisor:

- Primary Contact: If a staff member is unable to fulfill their duties, their immediate supervisor is the first point of contact.

Contact the next level of management if necessary to escalate the issue.

2. Backup Staff Member:

- Each staff member should have a designated backup who is trained to step in and assume their responsibilities .Additional temporary staff may be brought in if necessary

3. Team Lead or Manager:

- Interim Responsibility: If the immediate supervisor is unavailable, the team lead or manager assumes temporary responsibility.

- Communicate with senior management if the situation requires further escalation.

4. Senior Management:

- Final Escalation: If the situation cannot be resolved at the department level, it is escalated to senior management.

4.1.3 Data study

1. Financial Data:

- Transaction records, account balances, financial statements, and investment portfolios.

-Criticality: Extremely high; essential for daily banking operations

- Confidentiality: Highly confidential.

2. Customer Information:

-Personal identifiable information (PII) such as names, addresses, contact details, and social security numbers.

- Criticality: High; necessary for customer service, account management, and compliance regulations.

- Confidentiality: Very high.

3. Employee Records:

- HR records, payroll information, performance evaluations, and training records.

- Criticality: High; essential for human resource management, payroll processing, and compliance with labor regulations

- confidentiality: High.

4. System Configuration Data:

- Configuration settings, network topology diagrams, and system documentation.

- Criticality: High; necessary for maintaining system integrity, security.

- Confidentiality: Moderate to high; could pose a security risk if exploited.

5. Security Logs and Monitoring Data:

- Description: Logs of security events, access attempts, and system activity monitoring.

- Criticality: High; crucial for detecting and responding to security incidents

- Confidentiality: High; contains sensitive information about system vulnerabilities, user activities, and potential threats.

6. Backup and Recovery Data:

- Backup copies of critical data, system configurations, and disaster recovery plans.

- Criticality: High; essential for recovering from data loss, system failures, or security breaches.

- Confidentiality: High; contains sensitive information and must be protected to prevent unauthorized access or tampering.

4.1.4 Criticality of Service List

Short-Term Recovery

1. Core Banking Services:

- Essential banking services including account management, transactions processing, and fund transfers.

- Order of Recovery: Top priority.

2. Customer Support Systems:

- Systems supporting customer service operations such as call center applications, CRM systems, and online banking portals.

- Order of Recovery: High priority.

3. Security and Monitoring Systems:

- Security monitoring tools, intrusion detection systems, and access control mechanisms.
- Order of Recovery: High priority.

4. Backup and Recovery Infrastructure:
- Description: Backup servers, storage devices, and disaster recovery mechanisms.
- Order of Recovery: High priority.

5. Email and Communication Services:
- Description: Email servers, collaboration platforms, and communication tools.
- Order of Recovery: Medium priority.

Long-Term Recovery

1. Data Analysis and Reporting Systems:
- Business intelligence tools, data analytics platforms, and reporting systems.
- Order of Recovery: Medium to high priority; essential for strategic decision-making and business performance analysis

2. Testing and Development Environments:
- Environments used for software development, testing, and deployment.
- Order of Recovery: Medium priority.

3. Document Management Systems:
- Systems for storing, managing, and retrieving electronic documents and records.
- Order of Recovery: Medium priority.

4. Training and Learning Management Systems:
- Description: Platforms for employee training, skills development, and compliance training.
- Order of Recovery: Low to medium priority.

5. Non-Essential Services and Applications:

- Non-critical applications, specialized tools, and ancillary services.

- Order of Recovery: Low priority.

4.1.5 Data Backup

- *Types of Data Backed Up*: All critical data, including Customer account information, Transaction records, financial records, Employee records, and system configuration files.
- *Backup Media*: Data is backed up to a combination of on-site storage solutions (such as Network Attached Storage (NAS) or Storage Area Network (SAN) devices) and off-site cloud storage providers.
- *Storage Location*:

On-Site: Secure, fireproof, and climate-controlled backup storage rooms within the data center.

Off-Site: Secure cloud storage locations and a secondary data center located in a geographically diverse location

- *Backup Frequency*:

Daily Backups: Only the data that has changed since the last backup is saved, Stored on on-site NAS/SAN devices.

Weekly Backups: A complete backup of all operational data and system configuration files. Stored on both on-site NAS/SAN devices and off-site cloud storage.

Monthly Backups: Full backups stored for long-term archival purposes. Stored on off-site cloud storage

- *Data Recovery Procedures*

Identify: Identify the source of data loss

Retrieve: Access the on-site NAS/SAN devices to retrieve the weekly full backup and the most recent daily incremental backup.

Restore: Use backup software to restore the full backup first, followed by the incremental backup to update the data.

Verify: Verify the integrity of the restored data

Reinstate: Gradually bring the financial transaction system back online, ensuring it operates correctly and securely.

Document: Log the recovery process and conduct a post-recovery review to improve future recovery efforts.

Equipment Replacement Plan: Equipment Replacement Plan for THE Y Bank's Data Center Department essay

1. Server Hardware:

- Rack-mounted servers for hosting critical applications and services.

- Order of Necessity: First priority

- Purchase Source: Certified vendors specializing in enterprise-grade server hardware, such as Dell, HP, or IBM.

2. Network Infrastructure Components:

- Switches, routers, firewalls, and network appliances for data transmission and security.

- Order of Necessity: Second priority.

- Purchase Source: Authorized resellers of networking equipment, including Cisco, Juniper, and Palo Alto Networks.

3. Storage Systems:

- Storage area network (SAN) or network-attached storage (NAS) devices for data storage and retrieval.

- Order of Necessity: Third priority;

- Purchase Source: Storage solution providers such as NetApp, EMC, or HPE.

4. Uninterruptible Power Supply (UPS):

- Backup power systems to provide continuous power supply and prevent data loss during outages.

- Order of Necessity: Fourth priority.

- Purchase Source: UPS manufacturers and distributors like APC by Schneider Electric, Eaton, or Tripp Lite.

5. Cooling and Environmental Monitoring Systems:

- HVAC units, air conditioning systems, and environmental sensors for temperature and humidity control.

- Order of Necessity: Fifth priority.

- Purchase Source: HVAC contractors, environmental monitoring system vendors, and building management system providers.

6. Backup and Disaster Recovery Solutions:

- Backup software, replication tools, and disaster recovery appliances for data protection and business continuity.

- Order of Necessity: Sixth priority.

- Purchase Source: Backup and DR solution providers such as Veeam, Commvault, or Veritas.

4.1.6 Mass Media Management

The Public Relations (PR) Department is primarily responsible for managing communication with mass media outlets on behalf of The Y Bank.

Guidelines for Providing Information:-

-Transparency and Accuracy: All information provided to the mass media must be accurate, truthful, and consistent with Bank's policies, values, and corporate messaging.

Confidentiality and Privacy:

- Respect customer privacy and confidentiality at all times. Do not disclose sensitive customer information or proprietary data without proper authorization.

Crisis Communication:

Designate a spokesperson or team of spokespeople to provide timely updates and information to the mass media

Legal and Regulatory Compliance: Consult legal counsel or regulatory experts when addressing sensitive topics or potentially contentious issues to mitigate legal risks and reputational damage.

5 Policy Compliance

5.1 Compliance Measurement

-The Y Bank’s team will verify compliance to this policy through various methods, including:

-Conduct regular audits to assess adherence to the policy guidelines and protocols.

-Review documentation related to disaster recovery procedures to ensure alignment with the policy.

-Monitor employee training and awareness programs regarding the Disaster Recovery Plan Policy.

-Perform regular testing and simulation exercises to evaluate the effectiveness of the disaster recovery plan in real-life scenarios.

- Analyze incident response reports to identify areas of improvement and ensure policy compliance in crisis situations.

5.2 Exception

Exceptions may be considered under special circumstances, such as:

-Unforeseen emergencies that require immediate action

-Technological advancements that necessitate policy adjustments

-Regulatory changes that impact policy compliance

5.3 Policy Non-Compliance

Any employee found to have violated the Disaster Recovery Plan Policy within the Data Center Department may be subject to disciplinary action, up to and including termination of employment.

6 Definitions and Terms

CISO :Chief Information Security Officer

SOC: Security Operations Center Manager

IRT :Incident Response Team

security breach: is an incident where unauthorized individuals gain access to sensitive, confidential, or protected information.

Short-Term Recovery: refers to the immediate actions and steps taken to restore critical services quickly and minimize downtime

long-term recovery comprehensive planning aimed at achieving full restoration

7 Revision History

Date of change	Responsible	Summary of Change
5/16	Noor	Updated and converted to new format.