ChecklistGuro

Disaster Recovery Case Management Checklist Template 2026

Initial Incident Assessment & Activation

Steps for identifying the disaster type, determining the severity level, and officially activating the recovery response team and emergency protocols.

Incident Discovery Date

Enter date...

Incident Discovery Time

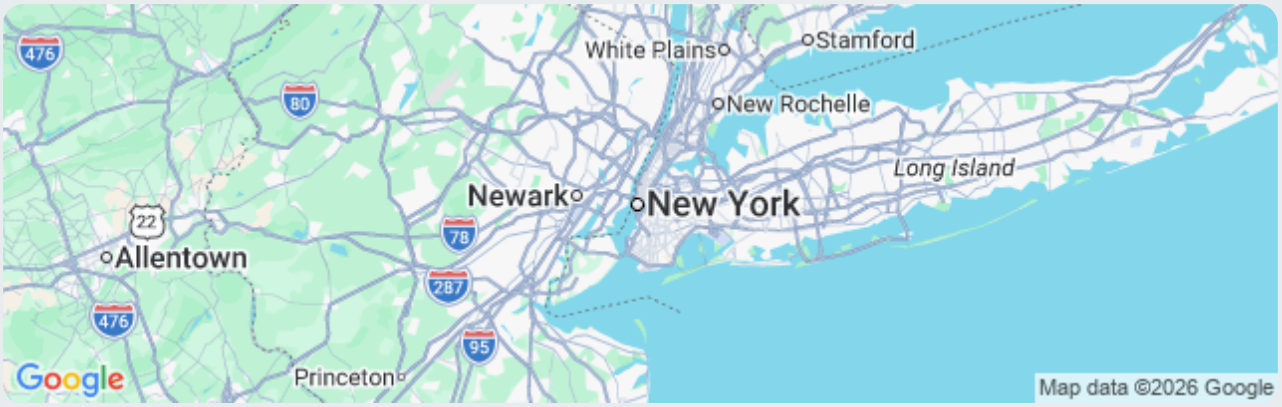
Enter time...

Disaster Type

- [ ] Natural Disaster (Flood, Fire, Earthquake)
- [ ] Cyber Attack / Ransomware
- [ ] Infrastructure / Power Failure
- [ ] Human Error / Accidental Deletion
- [ ] Other

Affected Site/Facility

Set My Current Location



Initial Incident Description

Write something...

Immediate Impacted Services

- [ ] Customer-Facing Applications
- [ ] Internal Database/Storage
- [ ] Employee Communication Tools
- [ ] Physical Office Access
- [ ] Third-Party API/Vendor Integrations

Incident Commander Authorization

Emergency Communications & Stakeholder Notification

Procedures for alerting internal leadership, emergency services, essential vendors, and key stakeholders about the disaster and current status.

Notification Timestamp

Enter date...

Alert Level

- [ ] Low - Informational
- [ ] Medium - Alert
- [ ] High - Immediate Action Required
- [ ] Critical - Full Disaster Activation

Stakeholders Notified

- [ ] Internal Executive Leadership
- [ ] IT & Security Teams
- [ ] All Employees
- [ ] Key Clients/Customers
- [ ] Legal & Compliance Department
- [ ] External Vendors/Partners
- [ ] Emergency Services/Authorities

Communication Summary

Write something...

Proof of Notification

Upload File

Incident Commander Verification

Critical Infrastructure & Data Integrity Audit

Assessment of physical site damage, server integrity, cloud service availability, and the immediate status of vital business records.

Audit Commencement Date

Enter date...

Disaster Impact Severity

- [ ] Low - Minimal disruption
- [ ] Medium - Partial operational impact
- [ ] High - Critical infrastructure failure
- [ ] Extreme - Total site/system loss

Affected Infrastructure Components

- [ ] On-site Servers
- [ ] Cloud Storage/SaaS
- [ ] Network/Connectivity
- [ ] Physical Hardware
- [ ] Database Integrity

Detailed Damage Assessment Notes

Write something...

Damage Evidence Photos or Logs

Upload File

Lead Auditor Verification

Personnel Safety & Accountability

Verification of employee safety, establishment of emergency contact trees, and deployment of necessary onsite or remote support resources.

Incident Commencement Date

Enter date...

Personnel Status Verification

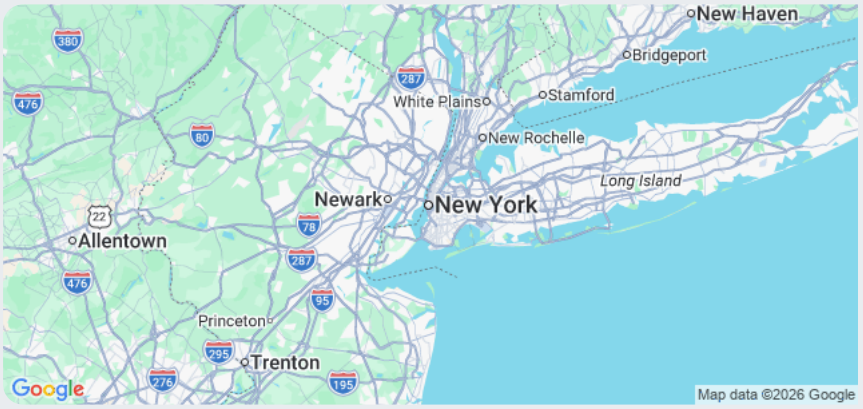
- [ ] All Staff Accounted For
- [ ]
- [ ] Injured/Requires Medical Attention
- [ ] Safe and Evacuated

Incident Injury/Status Details

Write something...

Current Muster Point/Assembly Site

Set My Current Location



Safety Officer Verification

Business Continuity & Workaround Implementation

Activation of secondary operating sites, failover systems, and manual workarounds to maintain essential business functions during downtime.

Primary Workaround Status

- [ ] Fully Operational
- [ ] Partially Operational
- [ ] Not Yet Activated
- [ ] Failed/Inaccessible

Alternative Operating Site Location

Write something...

Active Workaround Methods

- [ ] Manual Paper-Based Processing
- [ ] Secondary Cloud Backup
- [ ] Remote Work/VPN Activation
- [ ] Third-Party Outsourcing
- [ ] Manual Communication Channels

Workaround Activation Date

Enter date...

Description of Operational Gaps

Write something...

Updated Continuity Log/Evidence

Upload File

Data Restoration & System Recovery

Execution of backup restoration procedures, validation of data integrity, and systematic bringing of offline applications back online.

Backup Restoration Date

Enter date...

Restoration Status

- [ ] In Progress
- [ ] Completed
- [ ] Failed
- [ ] Delayed

Restored Systems/Databases

- [ ] Primary Database
- [ ] Cloud Storage/S3 Buckets
- [ ] Email Servers
- [ ] ERP/CRM Systems
- [ ] On-Premise File Servers

Data Integrity Verification Notes

Write something...

System Integrity Validation Report

Upload File

IT Lead Verification Signature

Supply Chain & Vendor Management

Coordination with third-party logistics, backup suppliers, and utility providers to ensure resource availability and service continuity.

Affected Vendor Categories

- [ ] Logistics & Transportation
- [ ] Raw Material Suppliers
- [ ] Cloud & IT Service Providers
- [ ] Utilities & Energy
- [ ] Third-party Manufacturers

Primary Impacted Vendor Name

Write something...

Date of Vendor Service Interruption

Enter date...

Description of Supply Chain Disruption

Write something...

Vendor Incident Report / Proof of Disruption

Upload File

Supply Chain Manager Approval

Resource Allocation & Crisis Budgeting

Monitoring of emergency expenditures, procurement of disaster-related supplies, and management of disaster-related insurance claims.

Emergency Fund Allocated

Enter a number...

Primary Vendor Name

Write something...

Budget Approval Status

- [ ] Pending
- [ ] Approved
- [ ] Denied

Expense Receipts & Invoices

Upload File

Allocated Resources

- [ ] IT Hardware
- [ ] Temporary Labor
- [ ] Logistics/Transport
- [ ] Emergency Supplies

Financial Controller Authorization

Post-Disaster Impact Analysis

Evaluation of total operational downtime, financial loss assessment, and documentation of all actions taken during the incident.

Date of Incident Completion

Enter date...

Total Estimated Financial Loss

Enter a number...

Summary of Operational Downtime

Write something...

Affected Departmental Areas

- [ ] IT/Infrastructure
- [ ] Operations
- [ ] Finance/Accounting
- [ ] Customer Service
- [ ] Logistics/Supply Chain

Damage Assessment Documentation

Upload File

Incident Commander Approval

Post-Incident Review & Plan Optimization

Conducting a 'lessons learned' session to update the 2026 Disaster Recovery Plan and patching vulnerabilities identified during the recovery process.

Review Completion Date

Enter date...

Root Cause Analysis Summary

Write something...

Identified Plan Deficiencies

- [ ] Communication Delays
- [ ] Resource Shortages
- [ ] Technical Failures
- [ ] Data Inconsistency
- [ ] Inadequate Training

Updated Disaster Recovery Plan (Final Version)

Upload File

Compliance Officer Approval

Previous Next Finish

Generate Sample Report