4Thought Marketing Disaster Recovery Plan

Table of Contents

Security Policy Home

Last Update:

October 28, 2025

Statement of Intent

This document outlines our policies and procedures for disaster recovery, both technical and physical, as well as our process-level plans for recovering critical systems and processes. This document summarizes our recommended guidelines. In an emergency, the security officer may modify this document to ensure the physical safety of our team members, systems, and data.

Our mission is to ensure information system uptime, data integrity and availability, and business continuity.

Policy Statement

Corporate management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- The security team will perform a formal risk assessment to determine the requirements for the disaster recovery plan.

- The disaster recovery plan should cover all essential and critical infrastructure elements, systems, and networks to maintain crucial business activities.

- The security officer should conduct periodic tests of the disaster recovery plan in a simulated environment to ensure plan execution is possible in an emergency and that the management and staff understand how the program will work.

- All team members must know the disaster recovery plan and their respective roles in the disaster recovery process.

- The security team will regularly review the disaster recovery plan to consider potential updates for new requirements.

Objectives

The principal objective of the disaster recovery plan is to develop, test, and document a well-structured and easily understood process, which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency that interrupts information systems and business operations.

Additional objectives include the following:

- The need to ensure that all team members fully understand their duties in implementing such a plan

- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to critical customers, vendors, and others

Remote Work Model

Since going fully remote in March 2020 following COVID-19 and the closure of our facilities in Costa Rica and India, 4Thought Marketing moved to fully cloud-based systems and multi-channel communication across our global team.

Cloud Service Infrastructure

4Thought Marketing utilizes multiple cloud service providers to ensure business continuity:

- **Auth0** – Authentication and identity management
- **AWS** – Core infrastructure and compute resources

- **MongoDB** – Database services
- **Egnyte** – Document storage and collaboration
- **Additional cloud systems** – Various SaaS applications for business operations

Specific failover and contingency procedures for each provider are maintained in internal documentation accessible via Egnyte.

Key Personnel and Vendor Contact Information

4Thought Marketing maintains a roster of critical internal and vendor contacts, including primary and alternative email addresses, work and mobile phone, and other contact methods, and a calling tree in Appendix A – Key Contact Information. The disaster recovery team members receive copies both electronically and in hard copy.

Acronyms and Definitions

- **DRP** – Disaster Recovery Plan
- **DRT** – Disaster Recovery Team
- **ERT** – Emergency Response Team

- **BRT** – Business Recovery Team
- **ETeam** – Executive Team
- **RTO** – Recovery Time Objective
- **RPO** – Recovery Point Objective
- **TMAS** – Technical Marketing Automation Services

Plan Overview

Plan Updating

The process for updating the Disaster Recovery Plan (DRP) must be appropriately organized and regulated. Whenever changes are required, the plan and training materials must be thoroughly tested and modified under the supervision of the Security Officer to ensure that they are accurate and up-to-date.

Plan Documentation Storage

The plan is stored electronically and managed on our cloud-based Egnyte server. Senior management members receive a digital copy of the plan on their computers. A physical copy of the plan is also distributed to the Disaster Recovery Team (DRT) after it is revised. The copies distributed to DRT

members will include unredacted appendices not included in the public version for security reasons.

Egnyte Documentation Strategy

- **Primary Repository**: Egnyte serves as the primary document repository for all DRP-related materials
- **Backup Strategy**: Egnyte provides cloud-based redundancy with automatic versioning and 180-day retention
- **Access Control**: ETeam maintains access lists for authorized personnel
- **Recovery Procedure**: In case of primary system failure, documents can be accessed via Egnyte web portal or mobile apps
- **Synchronization**: Critical DRP documents are synchronized locally on key personnel devices

Backup Strategy

Critical business processes and the agreed backup strategy for each are listed below. The approach prioritizes cloud-based systems where the service provider provides redundancy, emergency access, and failover solutions.

KEY BUSINESS PROCESS	BACKUP STRATEGY
Tech Support – Software	Cloud-based hosting with remote backup
Phone, Email, and Collaboration	Cloud-based hosting with remote backup
Finance	Cloud-based hosting with remote backup
Contracts Admin	Cloud-based hosting with remote backup
Sales & Marketing Systems	Cloud-based hosting with remote backup
Human Resources	Off-site data storage facility
Web Sites	Cloud-based hosting with remote backup

Risk Management

In our risk assessment, we've evaluated a range of potential disruptions across the diverse geographic locations of our remote workforce. The data indicates that the distributed nature of our team substantially lowers the risk of widespread business impact from a single disruptive event. Our primary vulnerability lies in potential communication gaps with key individual employees during localized incidents. However, our core systems are cloud-based and engineered for high availability, reducing the risk of system-wide failures. These factors suggest our operational setup is resilient, mitigating key risks and supporting business continuity.

Our cloud-based applications run in data centers engineered to safeguard our business data from hardware issues and environmental hazards. Servers operate in a rigorously controlled environment for peak performance and security. Each is built to endure events like fires and earthquakes up to a magnitude of 8.0. Our servers have backup electrical systems for continuous data access to guard against unexpected power failures and surges. Many of these can pull power from dual grids and have extra UPS modules and a generator to handle broader outages.

We've instituted a multi-person redundancy strategy to ensure uninterrupted access to our cloud-based systems. Specifically, at least two team members receive training to operate each of our critical cloud-based platforms and systems. This approach mitigates the risk associated with a team member unable to participate in recovery efforts in an affected region. By cross-training personnel across different geographic locations, we can quickly activate alternate access, maintaining operational integrity and continuing business functions with minimal disruption.

Emergency Response

Alert, Escalation, and Plan Invocation

Plan Triggering Events

Key trigger issues that would lead to activation of the DRP are:

- Regional Disaster or Health Crisis
- Key system outage
- Cyber security incident
- Extended loss of critical vendor services
- Data breach or corruption

Activation of Emergency Response Team

The Emergency Response Team (ERT) must be activated when an incident occurs. The ERT will then decide how much the DRP is required. All employees must be issued a Quick Reference card containing

ERT contact details for use in the event of a disaster.

Responsibilities of the ERT are to:

- Respond immediately to a potential catastrophe and call emergency services
- Assess the extent of the disaster and its impact on the business data center
- Decide which elements of the DR Plan should be activated
- Establish and manage a disaster recovery team to maintain vital services and return to regular operation
- Ensure employees are notified and allocate responsibilities and activities as required

Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish communication with key DRP team members within 2.0 business hours
- Restore affected critical services within 4.0 business hours of the incident

- Recover to business as usual within 8.0 to 24.0 hours after the incident
- Coordinate activities with disaster recovery team, first responders
- Report to the emergency response team

Emergency Alert, Escalation, and DRP Activation

This policy and procedure ensure that personnel clearly understand whom to contact during a disaster or crisis. Guidelines outline how to establish communication quickly when activating disaster recovery.

The DR plan will rely principally on key members of management and staff who will provide the technical and leadership skills necessary to achieve a smooth technology and business recovery. Suppliers of critical goods and services will continue to support the recovery of business operations as the company returns to normal operating mode.

Emergency Alert

The person discovering the incident calls a member of the Emergency Response Team in the order listed in Appendix A – Key Contact Information.

The Emergency Response Team (ERT) is responsible for activating the DRP for disasters identified in this plan and any other occurrence affecting the company’s ability to perform normally.

During the early stages of the emergency, one of the tasks is to notify the Disaster Recovery Team

(DRT) that an emergency has occurred. The notification will request DRT members assemble at the problem's site and will involve sufficient information to communicate this request effectively. The Business Recovery Team (BRT) will comprise senior representatives from the central business departments. The BRT Leader will be a senior member of the company's management team responsible for taking overall charge of the process and ensuring that the company returns to normal working operations as early as possible.

DR Procedures for Management

Management team members will keep a hard copy of each employee's name and contact numbers on their company-provided computers. In addition, management team members will have a hard copy of the company's disaster recovery and business continuity plans in their homes.

Contact with Employees

Managers will serve as the focal points for their departments, while designated employees will call other employees to discuss the crisis/disaster and the company's immediate plans. Employees who cannot reach staff on their call list should call the staff member's emergency contact to relay information on the disaster.

2.3.4 Backup Staff

If a manager or staff member designated to contact other staff members is unavailable or incapacitated, the designated backup staff member will perform notification duties.

2.3.5 Recorded Messages / Updates

For the latest information on the disaster and the organization's response, staff members can call a toll-

free hotline listed on the DRP wallet card. Messages will include data on the nature of the disaster, assembly sites, and updates on work resumption.

2.3.6 Personnel and Family Notification

If the incident has resulted in a situation that would cause concern to an employee's immediate family, such as hospitalization of injured persons, it will be necessary to notify their immediate family members quickly.

Media

Media Contact

Assigned staff will coordinate with the media, working according to guidelines that have been previously approved and issued for dealing with post-disaster communications.

Media Strategies

1. Avoiding adverse publicity
   Take advantage of opportunities for helpful publicity
   3. Have answers to the following fundamental questions:
      - What happened?

      - How did it happen?

- What are you going to do about it?

Media Team

Refer to Appendix A – Key Contact Information

Rules for Dealing with Media

Only the media team is permitted direct contact with the media; anyone else contacted should refer callers or in-person media representatives to the media team.

Insurance

We have issued several insurance policies for the company's disaster recovery and business continuity strategies. These include errors and omissions, directors' and officers' liability, general liability, cyber liability, and business interruption insurance.

For insurance-related assistance following an emergency out of regular business hours, please contact the security officer. Refer to Appendix B – Insurance Information for details.

Financial and Legal Issues

Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the company’s financial affairs. The evaluation should include:

- Loss of revenue
- Recovery costs
- Insurance deductibles
- Emergency procurement needs
- Regulatory compliance costs

Financial Requirements

The controller and CEO must address the financial needs of the company. These can include:

- Cash flow position
- Temporary borrowing capability
- Upcoming payments for taxes, payroll taxes, and Social Security
- Availability of company credit cards to pay for supplies and services required post-disaster

Legal Actions

The company's legal representation and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event, particularly the possibility of claims by or against the company for regulatory violations.

DRP Exercises

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise, no one passes or fails; everyone who participates learns from exercises – what needs to be improved and how to implement improvements. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DRP plans launch into action smoothly. But it only happens if everyone with a role in the plan rehearses their part multiple times, simulating the potential issues and confirming that the team takes proper steps to resolve them.

Exercise Schedule

The following exercise schedule shall be maintained:

- **Quarterly**: Tabletop exercises focusing on specific scenarios (minimum 4 per year)
- **Semi-Annually**: Functional exercises testing specific systems (minimum 2 per year)
- **Annually**: Full-scale simulation of major disaster scenario (minimum 1 per year)
- **Ad-hoc**: Following any significant system or organizational changes

Exercise Types and Objectives

Tabletop Exercises (Quarterly)

- **Purpose**: Discussion-based review of procedures
- **Duration**: 2-3 hours
- **Participants**: ERT, DRT, and key stakeholders

- **Scenarios**: Rotate through cyber incidents, natural disasters, vendor failures, and pandemic situations

Functional Exercises (Semi-Annually)

- **Purpose**: Hands-on testing of specific recovery procedures
- **Duration**: 4-6 hours
- **Participants**: Technical teams and system administrators
- **Focus Areas**: System restoration, data recovery, failover procedures

Full-Scale Simulation (Annually)

- **Purpose**: Comprehensive test of entire DRP
- **Duration**: 1-2 days
- **Participants**: All teams and departments

- **Scope**: End-to-end disaster scenario including communications, recovery, and restoration

Exercise Documentation

All exercises must be documented including:

- Exercise objectives and scope
- Participants and their roles
- Scenario details
- Timeline of events
- Issues identified
- Lessons learned
- Improvement actions with assigned owners and due dates
- Metrics collected (RTOs achieved, communication effectiveness, etc.)

Success Criteria

Exercises are considered successful when:

- All critical systems are recovered within stated RTOs
- Communication protocols function as designed
- Team members demonstrate understanding of their roles
- Documentation proves adequate for recovery procedures
- 90% of exercise objectives are met
- No critical failures occur that would prevent business recovery

Continuous Improvement

Post-exercise reviews must be conducted within two weeks, with:

- Formal report submitted to ETeam within 14 days

- DRP updates implemented within 30 days
- Follow-up training scheduled as needed
- Action items tracked to completion
- Metrics compared to previous exercises to show improvement trends

Exercise Records

All exercise documentation shall be maintained in Egnyte at:
/Disaster Recovery/Test Results/[Year]_[Quarter]_[Exercise Type].pdf

Records shall be retained for a minimum of three years to demonstrate compliance and improvement over time.

Appendices

Appendix A – Key Contact Information

Emergency Response Team (ERT)

Role	Primary Contact	Backup Contact	Contact Methods
CEO/President	[Name]	[Backup Name]	Mobile: [XXX-XXX-XXXX] Email: [email] Alt Email: [alt-email]
Security Officer	[Name]	[Backup Name]	Mobile: [XXX-XXX-XXXX] Email: [email] Alt Email: [alt-email]
CTO	[Name]	[Backup Name]	Mobile: [XXX-XXX-XXXX] Email: [email] Alt Email: [alt-email]

Disaster Recovery Team (DRT)

Role	Primary Contact	Backup Contact	Contact Methods
IT Manager	[Name]	[Backup Name]	Mobile: [XXX-XXX-XXXX] Email: [email] Alt Email: [alt-email]
Operations Director	[Name]	[Backup Name]	Mobile: [XXX-XXX-XXXX] Email: [email] Alt Email: [alt-email]
Head of TMAS	[Name]	[Backup Name]	Mobile: [XXX-XXX-XXXX] Email: [email] Alt Email: [alt-email]
Marketing Operations Manager	[Name]	[Backup Name]	Mobile: [XXX-XXX-XXXX] Email: [email] Alt Email: [alt-email]

Critical Vendors

Vendor/Service	Account Manager	24/7 Support	Account #
AWS	[Name]	[XXX-XXX-XXXX]	[Account ID]
Auth0	[Name]	[XXX-XXX-XXXX]	[Account ID]
MongoDB	[Name]	[XXX-XXX-XXXX]	[Account ID]
Egnyte	[Name]	[XXX-XXX-XXXX]	[Account ID]
Telco/Conferencing	[Name]	[XXX-XXX-XXXX]	[Account ID]
Insurance Provider	[Name]	[XXX-XXX-XXXX]	[Policy #]

Communication Cascade Tree

CEO/President
├── Security Officer
│ ├── IT Manager
│ └── TMAS Lead
├── CTO
│ ├── Operations Director
│ └── Development Teams
└── CFO
├── Finance Team
└── Legal Counsel

Emergency Hotline Information

- **Toll-Free Disaster Hotline**: 1-800-XXX-XXXX
- **International Hotline**: +X-XXX-XXX-XXXX
- **Status Page URL**: https://status.[company-domain].com
- **Backup Communication Channel**: [Teams Workspace]

Note: Complete contact information is maintained in secure internal documentation accessible to authorized personnel only.

Appendix B – Insurance Information

Insurance Coverage Summary

Policy Type	Provider	Policy #	Coverage Amount	Effective Period	Renewal Date	Contact
Errors & Omissions	[Provider]	[Policy#]	$[Amount]	[MM/DD/YY – MM/DD/YY]	[MM/DD/YY]	[Contact]
Directors & Officers	[Provider]	[Policy#]	$[Amount]	[MM/DD/YY – MM/DD/YY]	[MM/DD/YY]	[Contact]
General Liability	[Provider]	[Policy#]	$[Amount]	[MM/DD/YY – MM/DD/YY]	[MM/DD/YY]	[Contact]
Business Interruption	[Provider]	[Policy#]	$[Amount]	[MM/DD/YY – MM/DD/YY]	[MM/DD/YY]	[Contact]
Cyber Liability	[Provider]	[Policy#]	$[Amount]	[MM/DD/YY – MM/DD/YY]	[MM/DD/YY]	[Contact]

Claim Procedures

1. **Immediate Notification**: Contact insurance provider within 24 hours
2. **Documentation Required**:
    1. Incident report
    2. Loss assessment
    3. Supporting evidence (photos, logs, reports)

3. **Claim Submission Timeline**: Within

Note: Complete insurance information including policy numbers and coverage details is maintained in secure internal documentation.

Appendix C – Technology Disaster Recovery Plan Templates

Critical System Recovery Procedures

System: AWS Infrastructure

Component	Details
System Name	AWS Production Environment
Vendor	Amazon Web Services
Backup Strategy	Automated snapshots, cross-region replication
Recovery Steps	1. Access AWS Console 2. Navigate to EC2/RDS Dashboard 3. Initiate recovery from snapshot 4. Update DNS records 5. Verify connectivity
RTO	2 hours
RPO	1 hour

System: Auth0 Authentication

Component	Details
System Name	Auth0 Identity Platform
Vendor	Auth0 (Okta)

Component	Details
Backup Strategy	Configuration exported weekly, daily user database backup
Recovery Steps	1. Access Auth0 Dashboard 2. Import configuration 3. Restore user database 4. Reconfigure domains 5. Test auth flows
RTO	30 minutes
RPO	24 hours

System: MongoDB Database

Component	Details
System Name	MongoDB Atlas Cluster
Vendor	MongoDB Inc.
Backup Strategy	Continuous backups, point-in-time recovery
Recovery Steps	1. Access MongoDB Atlas 2. Select restoration point 3. Initiate cluster restoration 4. Update connection strings 5. Verify data integrity
RTO	1 hour
RPO	5 minutes

System: Egnyte Document Storage

Component	Details
System Name	Egnyte Cloud Storage
Vendor	Egnyte Inc.
Backup Strategy	Vendor-managed redundancy, 180-day version history
Recovery Steps	1. Access Egnyte portal 2. Navigate to Recycle Bin/Version History 3. Restore files/folders 4. Re-sync local copies 5. Verify permissions
RTO	15 minutes
RPO	Real-time sync

Note: Complete technical recovery procedures with credentials and detailed steps are maintained in

secure internal documentation.

Appendix D – Forms and Documents

Document Repository Structure (Egnyte)

```
/Disaster Recovery/
├── Plans/
│   ├── Current DRP v1.5.pdf
│   ├── Incident Response Plan.pdf
│   └── Business Continuity Plan.pdf
├── Procedures/
│   ├── Emergency Notification Procedure.docx
│   ├── System Recovery Checklists/
│   └── Communication Templates/
├── Contact Lists/
│   ├── Emergency_Contacts_Current.xlsx
│   └── Vendor_Contacts.xlsx
├── Test Results/
│   └── [Year]_[Quarter]_[Exercise Type].pdf
└── Training Materials/
├── DRP_Training_Presentation.pptx
└── Quick_Reference_Cards.pdf
```

Critical Forms Available in Egnyte

1. **Incident Report Form** – Initial documentation of incident

2. **Damage Assessment Checklist** – Systematic evaluation of impact

3. **Recovery Progress Tracking** – Monitor restoration activities

4. **Post-Incident Review Template** – Lessons learned documentation

5. **Communication Log** – Track all disaster-related communications

Access Control

- **Full Access**: ETeam members, Security Officer
- **Read Access**: All managers, DRT members
- **Restricted Folders**: Insurance details, sensitive vendor contracts
- **Offline Copies**: Maintained by Security Officer and CEO

Document Review Schedule

After Each Incident: Relevant procedures and forms

Quarterly: Contact lists, vendor information

Semi-Annually: Procedures and checklists

Annually: Full DRP, insurance policies, training materials