Business Continuity Plan

Last Reviewed: October 8, 2025

# Purpose

This plan describes how MindPath will continue critical business functions and restore services after a disruption. The goals are to:

* Reduce downtime
* Meet customer expectations
* Protect the company’s reputation

# Roles

|  |  |
| --- | --- |
| CTO | Owns this plan and oversees responses. |
| Disruption Response Team | Coordinates cross-team recovery efforts. The response team includes:   * CTO * Lead Software Developer * IT Engineer * Customer Support Director |
| Executive team | Notified of significant disruptions and direct external communication (to customers, vendors, counsel…) |
| Employees | May be asked to help with response. |

# Risk Assessment

This section is about knowing what parts of our business we can’t afford to lose, what might knock them out, and how fast we need them back. Writing them down helps clarify what must be restored first.

**Critical Business Functions**

* SaaS platform (Learning Management System) – product we sell
* Customer support and communications (email, helpdesk, status page)
* Development and deployment pipeline (GitHub, CI/CD, AWS environments)
* Financial functions (billing, payroll)

**Possible Disruptions**

* AWS service outage (regional or account-specific)
* Ransomware, malware, or data corruption
* Accidental deletion or misconfiguration
* Vendor outage (e.g., Transcribeo API down)
* Loss of Google Workspace access (email, identity, SSO)
* Office unavailability (natural disaster, power, connectivity)

**Dependencies**

* AWS (EC2, RDS, S3, IAM, CloudFront)
* Google Workspace (identity, email, Docs, Drive, Meet)
* Transcribeo API (video transcript integration, *service degradation if unavailable*)
* GitHub and CI/CD system (software delivery)
* Stripe (B2B invoicing and payments: ACH, credit card, reminders, reconciliation)

**Recovery Objectives**

* SaaS platform (LMS): Restore within **24 hours** (target RTO). Data loss should not exceed **4 hours** (RPO).
* Customer communications: Alternate method (status page, social media) within **2 hours** if Google Workspace (email) is unavailable.
* Development pipeline: Restore within **3 days** if lost.
* Financial functions: Restore within **5 days**.
* Customer SLA is 99.0%, but goal is **24/7 uptime with prompt notice of any outage**.

**Alternate Work Location**

* All staff can (and usually do) work from home.
* If the office is unavailable, business continues with laptops and cloud services.

# Response & Recovery

This section is about responding to disruptions. It describes the process followed to assess severity, invoke a response team, and work through to a resolution while keeping stakeholders notified along the way.

## Determine Disruption Severity

When disruptions are reported, the CTO determines the severity based on how many customers are affected, how long the issue is expected to last, and whether it risks breaching customer commitments.

| Severity | Description | Examples | Required Actions |
| --- | --- | --- | --- |
| Minor | Small disruption with limited customer impact or lasting less than 1 hour. | Short delay in transcript delivery, small feature outage. | CTO directs a quick resolution without activating the plan. |
| Major | Disruption affecting many customers, or an outage expected to last more than 1 hour but not yet breaching SLA. | Partial LMS outage, Google Workspace email disruption. | CTO activates plan (proceed to steps below.) |
| Critical | Severe disruption breaching the SLA or preventing most customers from using the LMS. | Multi-hour SaaS outage, AWS regional failure. | CTO activates plan  (proceed to steps below.) |

## Assemble the Disruption Response Team

The CTO notifies Response Team members and confirms the communication channel (Google Meet or phone).

If the event severity is not Minor, the CTO also notified executive staff who will direct external communication.

## Assess & Prioritize

Development Lead and IT Engineer report on system status (AWS, Google, vendors).

Customer Support Director reports on customer-facing impact (tickets, complaints, accessibility issues).

Team compares situation against recovery objectives (RTO/RPO).

## Stabilize

Development Lead begins recovery steps in AWS.

IT Engineer escalates to Google or other SaaS vendors as needed.

Customer Support Director drafts initial customer communication.

CTO assigns additional personnel if needed.

## Communicate

**Internal:** CTO provides short updates to all staff so they know who is leading, current status, and how to handle customer inquiries.

**External:** Customer Support Director prepares draft updates; Executives approve before release. Updates may go to the status page, direct email, or social channels depending on impact.

Regular updates are shared until recovery is complete.

## Recover & Monitor

Development Lead restores systems from backups or snapshots as required.

IT Engineer ensures internal tools (Google Workspace, identity, SSO) remain operational.

CTO monitors recovery progress and sets schedule for follow-up communication.

## Close Out

CTO declares systems stable and operations restored.

Executives approve and release final customer update.

Response Team holds a short debrief to record what happened, what worked, and what needs improvement.

# Procedures

The following procedures will assist in resolving some disruptions.

### AWS

Restore from backups or snapshots using AWS Backup and RDS snapshots.

### Google Workspace

Use Google Admin Console to reset accounts, revoke sessions, and restore access.

### Transcribeo (Transcription Service)

If the Transcribeo API is down, video uploads are accepted but transcripts are delayed. If Transcribeo is down more than 48 hours, inform customers that transcripts will be delayed until the vendor recovers. No alternate vendor is currently in place. Executives will review whether to initiate an emergency vendor search.

### Stripe (Billing Services)

If unavailable, invoices can be issued manually from Google Docs/Sheets and payments collected by bank transfer. Reconciliation with Stripe occurs once restored.

# Appendix A: Personnel and Contact Info

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name | Business Contact Info | Alternate Contact Info |
| Security Officer | Archie Tech | archie@mindpath.com | (503) 111-1111 |
| Executive Leadership Team | Maxine Powers Archie Tech Mark Ketter Wynn Moore | max@mindpath.com  archie@mindpath.com  mark@mindpath.com  wynn@mindpath.com | (503) 222-2222  (503) 333-3333  (503) 444-4444  (503) 555-5555 |
| Customer Support Director | Will Fixit | will@mindpath.com | (503) 666-6666 |
| IT Engineer | Grant X. Esse | grant@mindpath.com | (503) 777-7777 |
| Lead Software Developer | Ruby Rails | ruby@mindpath.com | (503) 888-8888 |

# Appendix B: Response Resources

|  |  |  |  |
| --- | --- | --- | --- |
| Resource | URL / Location | Purpose | Owner |
| AWS Console | <https://console.aws.amazon.com/> | Access to AWS services (EC2, RDS, S3, IAM, Security Hub) | CTO / IT Engineer |
| AWS Backup | <https://console.aws.amazon.com/backup/> | Restore database and file snapshots | IT Engineer |
| AWS CloudTrail | <https://console.aws.amazon.com/cloudtrail/> | Review account activity logs | Security Officer |
| AWS GuardDuty | <https://console.aws.amazon.com/guardduty/> | Detect suspicious activity | Security Officer |
| AWS IAM | <https://console.aws.amazon.com/iam/> | Manage accounts, keys, MFA | CTO |
| Google Admin Console | <https://admin.google.com/> | Manage Workspace accounts, reset passwords, enforce SSO | IT Engineer |
| Google Vault | <https://vault.google.com/> | Search Gmail/Drive content if needed | Security Officer |
| Contract & Policy Folder | Google Drive: /MindPath/Security/Contracts | Check for customer/vendor reporting requirements | CTO |