Incident Response Plan

Last Reviewed: October 8, 2025

# Purpose

This plan explains how MindPath responds to security incidents. Our goals are to:

* Limit damage and disruption
* Restore normal operations quickly
* Learn from incidents so we get better over time

# Roles

|  |  |
| --- | --- |
| Security Officer | Owns this plan and oversees responses. |
| Lead Responder | Appointed by the Security Officer to manage a specific incident. |
| Incident Response Team | Small group assembled by the Lead Responder to help resolve an incident. |
| Employees | Must report suspected incidents. May be asked to help with response. |
| Executive Staff | Notified of significant disruptions and direct external communication (to customers, vendors, media…) Decide when to consult outside experts (law enforcement, legal, forensics…) |

# What Counts as an Incident

Anything that threatens the confidentiality, integrity, or availability of MindPath services or data, such as:

* Exposure of sensitive data (malicious or accidental)
* Malware, ransomware, or phishing
* Unauthorized access to accounts or systems
* Denial of service attacks
* Violations of security policy

# Incident Response Process

Based on NIST guidance, MindPath follows these six phases:

| Phase | Description |
| --- | --- |
| 1. Preparation | Reduce risks and be ready to respond. |
| 2. Detection | Notice and confirm incidents. |
| 3. Containment | Limit the spread and impact. |
| 4. Eradication | Remove the root cause and attacker access. |
| 5. Recovery | Restore normal operations securely. |
| 6. Post-incident activity | Review what happened and improve. |

## 1. Preparation

MindPath reduces risks through:

* Asset management
* Identity and access management
* Endpoint protection
* Remote access protection
* Employee security awareness
* Vendor assessments

We also:

* Keep regular backups of critical data
* Train staff to report incidents
* Maintain this plan

## 2. Detection

When an incident is reported, the Security Officer or the Lead Responder assigns it a severity level.

| Severity | Characteristics | Example | Handling |
| --- | --- | --- | --- |
| Low | * Minimal impact * Quickly contained | Email sent to wrong recipient | Handled by Security Officer. No follow-up. |
| Medium | * Noticeable business impact * Needs cross-team response | Malware on one laptop | Lead Responder may be appointed. |
| High | * Major business disruption * Possible legal or reputational damage | Stolen laptop with unencrypted sensitive data. | Response team engaged. Executives notified. |
| Critical | * Severe disruption * May need outside help | SaaS outage halts business for days. | Response team engaged. Executives notified. |

### Communication

Internal discussion of an incident is limited to those involved (“need-to-know”).

The Lead Responder also:

* Notifies any internal stakeholders whose work may be affected and coordinates any other internal announcements.
* Notifies executive staff of any High or Critical event
* Notifies executive staff if contractual obligations may require reporting the event to third parties.

External communication is only through executives and legal. If the situation requires a customer-facing statement before executives have time to respond, the Lead Responder may authorize issuing this pre-approved holding statement to any client whose users may have been affected:

*MindPath is investigating a potential security event. Our team is working to understand the scope and impact. We will provide updates as we learn more.*

Executive Staff and Legal Counsel are responsible for communication with third parties including customers, partners, cyber insurance, media, and law enforcement.

Contact info for key personnel is maintained in Appendix A of the Business Continuity Plan.

### Investigation

The Response Team investigates to determine the likely cause and scope of the incident. Some of the important questions at this point include:

* Who noticed the incident and when?
* When did it start?
* Who and what is affected?
* What steps are needed to recover?

### Evidence Handling

* Do not wipe or re-image systems until the Lead Responder approves.
* Save logs, alerts, suspicious files, and emails.
* Store copies in a secure evidence folder.

### Resources

Appendix B of the Business Continuity Plan is a list of company resource locations that may be useful in assessing and containing security incidents as well.

## 3. Containment

If recovery will take time, the Response Team may in the interim:

* Disable accounts
* Force password resets and revoke sessions
* Disconnect affected devices
* Block attacker Ips or domains
* Suspend SaaS integrations or API keys
* Suspend access to a SaaS application
* Change shared secrets (admin passwords, API tokens)
* Cut off third-party vendor access

## 4. Eradication

The next step is to remove the attacker’s access:

* Malware/ransomware – Rebuild or re-image infected devices.
* Compromised accounts – Reset passwords, revoke tokens, remove backdoors
* Unauthorized changes – Review and undo malicious changes

## 5. Recovery

Service is restored when the Response Team brings systems back safely:

* Restore from clean backups or images
* Re-enable accounts and services once secure
* Apply patches and fixes before return to use
* Monitor for persistence or reinfection

The Lead Responder notifies internal stakeholders that the incident is resolved. Notification to external stakeholders is directed by executive leadership.

## 6. Post-Incident Activity

The Lead Responder holds a short retrospective with everyone involved:

* Identify root cause
* Capture lessons learned
* Suggest improvements to policy, training, tools, or vendor practices

Findings go to the Security Officer, who shares them with executives and assigns follow-up tasks.