Responsible Disclosure Policy

Purpose and Scope

Purpose

Mindsmith Learning, Inc. ("Mindsmith") is committed to ensuring the security and privacy of our systems, applications, and customer data. We recognize the vital role that independent security researchers, ethical hackers, and the broader security community play in improving cybersecurity.

This Responsible Disclosure Policy establishes guidelines for identifying, reporting, and remediating security vulnerabilities discovered within Mindsmith's infrastructure and applications in a safe, transparent, and coordinated manner.

Scope

This policy applies to all security researchers, customers, partners, vendors, employees, and third parties who discover potential security vulnerabilities within Mindsmith services and systems.

In-Scope Targets:

• Mindsmith web applications (including main web platform and API endpoints)

• In-scope cloud infrastructure hosting Mindsmith applications

• Official Mindsmith integrations and webhooks

Out-of-Scope Services & Activities:

• Physical attacks against Mindsmith offices, data centers, or employees

• Social engineering attacks (e.g., phishing, vishing, spear phishing) against Mindsmith personnel or users

• Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks

• Automated scanning tools generating high volumes of traffic or causing degradation of service

• Destruction, modification, or exfiltration of customer or employee personal data

• Vulnerabilities affecting third-party services, vendors, or platforms utilized by Mindsmith (e.g., hosting providers) unless directly affecting Mindsmith's implementation

Roles and Responsibilities

Management & Legal

• Oversees the execution and legal protections associated with the Responsible Disclosure Policy.

- Evaluates policy compliance and ensures alignment with organizational risk management goals.

IT & Security / Engineering Team

• Acts as the primary intake point for vulnerability reports via the designated disclosure communication channel.

• Validates reported vulnerabilities, assigns severity ratings, and manages remediation timelines.

IT & Security / Engineering Team (cont.)

• Maintains regular communication with reporting researchers throughout the triage and resolution process.

Employees & Contractors

- Immediately forwards any external vulnerability disclosures or security inquiries received through non-standard channels to the Security Team.

• Adheres to internal incident handling and vulnerability management procedures when remediating identified issues.

Security Researchers & External Reporters

• Conducts testing ethically and strictly within the boundaries defined in this policy.

• Promptly reports discovered vulnerabilities without publicly disclosing them before authorization or resolution.

Procedures

1. Reporting Guidelines

If you believe you have discovered a security vulnerability in a Mindsmith service or system, please report it promptly using the following procedure:

• Contact Channel: Email the details of your finding to the designated security intake address (e.g., security@mindsmith.ai).

- Required Details:
- ◦ Brief description of the vulnerability and potential impact.
- ◦ Step-by-step reproduction instructions or a proof-of-concept (POC) demonstration (avoiding destructive code or data extraction).
- ◦ Affected URLs, endpoints, or components.
- ◦ Your contact information for follow-up communications.

2. Triage and Response Commitments

Mindsmith commits to handling reported vulnerabilities professionally and predictably according to the following SLAs:

• Initial Acknowledgment: Mindsmith will acknowledge receipt of the report within 2 business days.

• Triage & Validation: The Security Team will review and validate the finding within 5 business days.

• Remediation Timelines: Vulnerabilities are remediated according to the Operations Security Policy's severity-based SLA: Critical within 5 days, High within 10 days, Medium within 30 days, and Low within 60 days of the determined severity.

• Status Updates: Mindsmith will keep the reporter informed of progress as key milestones are reached.

3. Safe Harbor / Legal Protections

Mindsmith considers security research conducted under this policy to be:

3. Safe Harbor / Legal Protections (cont.)

• Authorized: Authorized under applicable anti-hacking laws (e.g., Computer Fraud and Abuse Act), and Mindsmith will not initiate legal action against researchers acting in good faith under this policy.

- Exempt from Restraint: Protected from civil claims as long as research activities comply with the scope and restrictions outlined herein.

If legal action is initiated by a third party against a researcher who adhered strictly to this policy, Mindsmith will make it known that the researcher acted in authorization with this policy.

4. Coordinated Public Disclosure

• Mindsmith asks that security researchers maintain strict confidentiality and refrain from publicly disclosing details of a vulnerability until Mindsmith has remediated the issue and granted written permission for public release.

• When appropriate, Mindsmith will acknowledge the researcher's contribution upon resolution of the issue, subject to mutual agreement.

Compliance

This policy aligns with and supports Mindsmith's compliance obligations under active frameworks:

- SOC 2 (Trust Services Criteria - CC6.8, CC7.1, CC7.3): Establishes mechanisms for detecting, analyzing, and addressing infrastructure and software vulnerabilities, as well as external threat communication.
- ISO/IEC 27001:2022 (Controls A.5.24, A.8.8): Supports management of information security incidents and management of technical vulnerabilities through coordinated vulnerability disclosure.

• GDPR (Article 32 - Security of Processing): Ensures continuous evaluation and testing of technical and organizational security measures to protect Personal Identifiable Information (PII) against unauthorized access and exposure.

Training and Awareness

- All Mindsmith engineering, operational, and customer-facing staff receive security training regarding vulnerability intake, incident handling, and reporting workflows.
- Customer support and non-technical staff are instructed on how to escalate external security reports received through standard support channels to the IT & Engineering Security Team without delay.

Exceptions and Violations

Policy Exceptions

Any exception or deviation from this policy must be documented and approved by the Security Lead or CEO.

Policy Violations

Any intentional breach of this policy by Mindsmith personnel or contractors-such as unauthorized public disclosure of internal vulnerabilities or failure to follow triage procedures-may result in

disciplinary action up to and including termination of employment or contract, as well as potential legal consequences.

Review and Audit

This policy shall be reviewed and evaluated for effectiveness at least annually or following significant changes to Mindsmith's operational environment or regulatory obligations. Updates to this policy must be authorized by executive management.

Version History

Version	Date	Description	Author	Approved By
1.1	2026-09-17	Remediation SLA now matches the Operations Security Policy (5/10/30/60 days).	Bryan Gurr	Justin Lanfell
1.0	2026-08-07	Version 1.0 Initial Draft of Responsible Disclosure Policy	Zachary Allen	Zachary Allen