Mixpeek Incident Response Plan

Version: 1.0 **Effective Date:** April 15, 2026 **Last Reviewed:** April 15, 2026
Owner: Mixpeek Engineering

1. Purpose

This plan establishes procedures for detecting, responding to, containing, and recovering from security incidents affecting Mixpeek systems, data, or customers. It ensures compliance with HIPAA Breach Notification requirements and SOC-2 incident management controls.

2. Scope

This plan covers all security incidents involving Mixpeek production systems, customer data, employee data, and third-party integrations. It applies to all Mixpeek personnel and third-party service providers.

3. Definitions

Term	Definition
Security Incident	Any event that compromises the confidentiality, integrity, or availability of Mixpeek systems or data
Breach	A security incident that results in unauthorized access to, or disclosure of, protected data
PHI Breach	A breach involving Protected Health Information, subject to HIPAA Breach Notification Rule
Severity 1 (Critical)	Active data exfiltration, system compromise, PHI exposure
Severity 2 (High)	Unauthorized access detected, service outage affecting customers

Term	Definition
Severity 3 (Medium)	Suspicious activity, failed intrusion attempts, vulnerability discovered in production
Severity 4 (Low)	Policy violation, minor misconfiguration, informational security event

4. Incident Response Team

Role	Responsibility
Incident Commander	Leads response, makes decisions, coordinates communication
Technical Lead	Investigates root cause, implements containment and remediation
Communications Lead	Manages customer and stakeholder notifications

5. Response Phases

Phase 1: Detection & Reporting

Detection Sources: - ClickHouse audit log anomalies (unusual access patterns, volume spikes) - Sentry error alerts (unexpected exceptions, stack traces with sensitive data) - Infrastructure monitoring (Prometheus/Grafana dashboards) - Customer reports - Employee observations - Third-party notifications (vendor security advisories)

Reporting: - Any suspected incident must be reported immediately to the Incident Commander. - Reports should include: what was observed, when, affected systems, and potential impact. - Do not attempt remediation before the incident is logged and triaged.

Phase 2: Triage & Classification

Within **30 minutes** of detection:

1. Assign severity level (1-4) based on data sensitivity and blast radius.

2. Determine if PHI or PII is involved (check namespace `data_classification` field).
3. Identify affected systems, namespaces, and customers.
4. Document initial findings in the incident log.

Phase 3: Containment

Immediate containment actions by severity:

Severity	Actions
Critical	Revoke compromised API keys immediately (cache invalidation is instant). Isolate affected namespaces. Block suspicious IPs at Cloudflare. Consider service shutdown if active exfiltration.
High	Revoke affected credentials. Enable enhanced audit logging. Review recent access logs in ClickHouse.
Medium	Monitor closely. Restrict access to affected resources. Prepare patches.
Low	Log and track. Schedule remediation.

API Key Revocation: - Revoked keys are immediately invalidated (Redis cache cleared on revocation). - Use the admin API: `PATCH /v1/organizations/api-keys/{key_id}` with `status: "revoked"`.

Phase 4: Eradication

1. Identify and remove root cause (vulnerability, misconfiguration, compromised credential).
2. Patch affected systems.
3. Rotate all potentially compromised credentials.
4. Verify remediation with targeted testing.

Phase 5: Recovery

1. Restore affected services from known-good state.
2. Re-enable access with fresh credentials.
3. Monitor for recurrence (enhanced logging for 30 days).
4. Confirm service stability.

Phase 6: Post-Incident Review

Within **72 hours** of resolution:

1. Conduct a post-incident review with all involved parties.
2. Document timeline, root cause, impact, and actions taken.
3. Identify preventive measures and assign owners.
4. Update security controls, monitoring, and this plan as needed.
5. File the post-incident report in the compliance directory.

6. HIPAA Breach Notification

If the incident involves a breach of unsecured PHI:

6.1 Risk Assessment

Evaluate the following factors (per 45 CFR 164.402): 1. Nature and extent of the PHI involved 2. Who accessed or received the PHI 3. Whether the PHI was actually acquired or viewed 4. Extent to which the risk has been mitigated

6.2 Notification Requirements

Recipient	Timeline	Method
Affected individuals	Within 60 days of discovery	Written notice (email if preferred by individual)
HHS Secretary	Within 60 days if 500+ individuals; annually if fewer	HHS breach reporting portal
Media	Within 60 days if 500+ individuals in a single state	Press release to prominent media outlets

6.3 Notification Content

- Description of the breach (what happened, dates)
- Types of information involved
- Steps individuals should take to protect themselves
- What Mixpeek is doing to investigate, mitigate, and prevent recurrence
- Contact information for questions

7. Communication Templates

Customer Notification (Non-PHI)

> Subject: Security Incident Notification — Mixpeek
>
> We are writing to inform you of a security incident that may have affected your Mixpeek account. On [DATE], we detected [DESCRIPTION]. We immediately [CONTAINMENT ACTIONS].
>
> **What happened:** [DETAILS] **What we're doing:** [REMEDIATION STEPS] **What you should do:** [RECOMMENDED ACTIONS — e.g., rotate API keys]
>
> We take the security of your data seriously. If you have questions, contact info@mixpeek.com.

PHI Breach Notification

> Subject: Notice of Data Breach — Mixpeek
>
> We are writing to notify you of a breach of your protected health information (PHI) as required by the Health Insurance Portability and Accountability Act (HIPAA).
>
> **What happened:** [DETAILS] **Information involved:** [TYPES OF PHI] **What we're doing:** [REMEDIATION STEPS] **What you can do:** [PROTECTIVE STEPS]
>
> Contact: info@mixpeek.com | [PHONE]

8. Evidence Preservation

During any incident: - Do not modify or delete logs, configurations, or artifacts. - Capture ClickHouse audit logs for the affected time period. - Export relevant Kubernetes pod logs and events. - Screenshot or export Sentry error details. - Preserve network flow logs if available.

9. Testing

This plan is tested annually through: - Tabletop exercises simulating incident scenarios. - Technical drills testing containment procedures (API key revocation, namespace isolation). - Review and update of contact information and escalation paths.

10. Plan Maintenance

This plan is reviewed and updated: - At least annually. - After every Severity 1 or 2 incident. - When significant changes occur to Mixpeek infrastructure or personnel.

This document is maintained by Mixpeek Engineering. Questions should be directed to info@mixpeek.com.