Incident Response and Security Management Guide

Overview

Stannp maintains comprehensive incident response and security management procedures to rapidly detect, respond to, and recover from security incidents and service disruptions. Our structured approach minimizes impact, protects customer data including Protected Health Information (PHI), and ensures compliance with breach notification requirements under HIPAA and state privacy laws. We are committed to continuously improving our incident management processes through regular reviews and alignment with ISO 27001 best practices.

What is an Incident?

An incident is any unplanned event that disrupts or threatens to disrupt normal operations, affects service quality, or compromises security. This includes security incidents, data breaches, system outages, malware infections, data corruption, infrastructure failures, and service degradation.

Incident Management Framework

Comprehensive Coverage Our incident management policy provides detailed procedures for handling security incidents, data breaches, and disruptions to critical technical services, equipment, or data. All incidents are classified by severity with corresponding response protocols, escalation procedures, and notification requirements.

Incident Types Addressed Response procedures address unauthorized access attempts, malware infections, data breaches, system outages, denial of service attacks, insider threats, physical security breaches, data corruption, infrastructure failures, and configuration exposures.

Incident Classification

Incidents are classified by severity to ensure appropriate response:

Critical Incidents Active breaches affecting PHI or sensitive data, complete system outages affecting multiple customers, active malware infections spreading across systems, data breaches with unauthorized access, server compromise, or critical software bugs causing data loss.

High Severity / Major Potential data exposure, significant service degradation, successful unauthorized access attempts, security patch failures, configuration exposures, or potential threat to operations or important data but not immediately critical.

Stannp Inc.
250 Fillmore Street Suite
150 Denver 80206
www.stannp.com
1-888-321-2148

Medium Severity / Minor Isolated system failures, suspected security events requiring investigation, minor service disruptions with workarounds available, policy violations, minor configuration errors, and non-sensitive information exposure with minimal impact to data or security.

Roles and Responsibilities

Leadership Accountability The Chief Technical Officer maintains overall accountability for incident response and incident management, supported by dedicated senior technical staff and engineers who coordinate response activities, implement containment measures, and facilitate recovery.

Compliance and Communication The Compliance and Operations Director manages breach notification requirements and regulatory reporting. Business Impact Assessment and customer communication are managed by operations leadership. For HIPAA-covered incidents, our Compliance and Operations Director ensures compliance with breach notification rules.

Employee Responsibilities All employees are responsible for reporting suspected incidents promptly and following incident response procedures.

Incident Detection and Response Times

24/7 Monitoring Our Security Information and Event Management (SIEM) system provides 24/7 monitoring with real-time alerts for security events and anomalies. Incidents are detected through automated monitoring, user reports, or security alerts.

Rapid Response Initial incident reports are logged within 15 minutes of detection. Critical security incidents receive immediate response with containment measures implemented within 30 minutes. All incidents are tracked through resolution with documented timelines, actions taken, and lessons learned.

Incident Response Process

Our structured seven-step incident response process ensures consistent and effective handling of all incidents:

1. Detection & Reporting Incidents are detected through automated monitoring, user reports, or security alerts and logged immediately upon detection within 15 minutes.

2. Classification & Prioritization Initial assessment determines incident severity and potential impact, ensuring appropriate resource allocation and response protocols.

3. Containment Immediate actions are taken to limit the spread and impact of the incident, protecting unaffected systems. Critical incidents have containment measures implemented within 30 minutes.

4. Investigation Technical teams investigate root causes and assess the full scope of impact to determine appropriate remediation steps.

5. Eradication Measures are implemented to remove the root cause and prevent recurrence through system updates, patches, or configuration changes.

6. Recovery Systems and services are restored to normal operation according to defined Recovery Time Objectives, with monitoring to ensure stability.

7. Post-Incident Review Comprehensive analysis identifies lessons learned and improvement opportunities, which are documented in formal incident reports.

Recovery Objectives

We maintain defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for all critical services to ensure rapid restoration:

Platform and API Services Critical platform services including Dashboard and API maintain a Recovery Time Objective (RTO) of 30 minutes with a Recovery Point Objective (RPO) of 48 hours, ensuring rapid restoration with minimal data loss. Platform Database maintains an RPO of 6 hours with RTO of 30 minutes.

Customer-Facing Systems Customer-facing APIs and integration services, including the Website, maintain RTOs of 30 minutes to 1 hour with RPOs of 24 to 48 hours.

Administrative Systems Administrative and reporting systems, Email Systems, and Office Infrastructure maintain RTOs of 4 hours with RPOs of 48 hours.

High Availability Infrastructure Our infrastructure is designed for high availability with 99%+ uptime SLA supported by redundant systems, automated backups every 15 minutes, and geographically separated backup storage.

Breach Notification Procedures

HIPAA Compliance For HIPAA-covered breaches affecting 500 or more individuals, we notify the Department of Health and Human Services and affected individuals within 60 days of discovery.

State Law Compliance We also comply with state breach notification laws, which typically require notification without unreasonable delay.

Notification Content All breach notifications include the nature of the breach, types of information involved, steps individuals should take to protect themselves, what we are doing to investigate and remediate, and contact information for questions.

Communication

Clear communication protocols ensure stakeholders are informed throughout the incident lifecycle. Internal teams receive regular updates, customers are notified of service impacts, and regulatory notifications are made when required by HIPAA or state laws.

Stannp Inc.
250 Fillmore Street Suite
150 Denver 80206
www.stannp.com
1-888-321-2148

Post-Incident Activities

Post-Incident Reviews Following resolution of security incidents, we conduct comprehensive post-incident reviews to identify root causes, document lessons learned, and implement preventive measures.

Incident Reports All significant incidents result in formal incident reports documenting timeline, impact assessment, response actions, effectiveness of controls, and recommendations for improvement. All incidents are thoroughly documented including detection method, classification, actions taken, timeline, resolution, and lessons learned.

Continuous Improvement Findings from incident reviews are incorporated into security awareness training, policy updates, and technical control enhancements. This documentation supports continuous improvement and regulatory compliance.

Continuity Planning

Supporting Procedures While our primary focus is incident response and rapid recovery, we maintain documented business continuity procedures to address potential disruptions including severe weather, technical failures, utility failures, loss of key personnel, and supplier disruptions.

Continuity Objectives These plans ensure staff safety, maintain production output, preserve assets, and sustain business operations according to executive priorities. Plans are reviewed annually and updated based on incident response lessons learned and changing business requirements.

Stannp Inc.
250 Fillmore Street Suite
150 Denver 80206
www.stannp.com
1-888-321-2148