# Incident Response Plan

SentraShield Internal Document — Confidential

---

## Incident Response Team

SentraShield maintains a dedicated 24/7 incident response team composed of senior security engineers and a designated Incident Response Lead. The team is on-call at all times and reachable via a dedicated emergency communication channel.

## Triage and Containment

Security incidents are triaged within 1 hour of detection. Upon triage, the incident is classified by severity (Critical, High, Medium, Low). Critical and High severity incidents trigger immediate containment procedures including network isolation, credential rotation, and evidence preservation.

## Customer Notification

Customers are notified within 24 hours of a confirmed security incident that impacts their data. Notifications are delivered via email to registered security contacts and through the SentraShield customer portal. Notifications include a description of the incident, affected data scope, and immediate remediation steps taken.

## Post-Incident Review

A root cause analysis (RCA) report is completed within 7 business days of incident resolution. The RCA is shared with affected customers upon request. All incidents are documented in an internal incident register and reviewed quarterly to identify patterns and drive preventive improvements.

## Testing and Drills

The incident response plan is tested through tabletop exercises conducted semi-annually. Results are used to update and improve procedures. All incident response team members complete annual training on updated procedures.