**Incident Response Plan — Template**

Hudson Valley CISO • Updated August 14, 2025

Purpose: Provide a concise, actionable playbook to triage, contain, and recover from security incidents. Adapt sections to your environment.

# 1. Scope & Definitions

Define what constitutes a security incident, severity levels (SEV-1 to SEV-4), and systems in scope.

# 2. Roles & Responsibilities

Assign an Incident Lead, Triage Engineer, Comms Lead, IT Ops, Legal/Privacy, HR, Executive Sponsor, and Third-Party contacts (MSSP, insurer). Maintain 24/7 contact info.

# 3. Detection & Triage

Sources: EDR alerts, SIEM, email abuse reports, vendor notices. Triage: verify, classify severity, start incident log, preserve evidence.

# 4. Containment, Eradication, Recovery

Short-term containment (isolate hosts, disable accounts), long-term (block IOCs, reset tokens). Eradication (remove malware, patch). Recovery (rebuild, restore verified backups).

# 5. Communications

Internal updates cadence; single source of truth; external notifications to customers/regulators/insurer as required. Use approved templates and legal review.

# 6. Evidence & Forensics

Time-sync systems; capture volatile data where appropriate; maintain chain of custody; retain logs and images per policy.

# 7. Third Parties & Law Enforcement

When to engage vendors, outside counsel, insurer, or law enforcement. Include criteria and contacts.

# 8. Post-Incident Review

Within 10 business days: root cause, contributing factors, corrective actions, lessons learned, and metrics.

# Appendix A — Contact Roster (table)

Role | Name | Primary | Backup | After-hours | Notes

# Appendix B — Notification Templates

Internal alert, customer advisory, regulatory notice (as applicable).