CIPHERLINE SECURITY

PREPARED BEFORE PRESSURE

Cybersecurity Incident Response Plan

A practical security response plan defining preparation, severity, roles, evidence handling, containment, recovery, communications, and exercises.

PREPARED FOR

Aperture Mobility

Northstar Systems · Mara Klein · 4 August 2026

Document contents

Document convention	Value
Status	Review-ready
Owner	Mara Klein
Reference	NS-060-2026

0.1 Purpose and activation

Define covered events, activation authority, severity criteria, objectives, legal preservation, and links to continuity and crisis plans.

Document control	Detail
Owner	Mara Klein
Reference	NS-060-2026
Effective date	4 August 2026
Status	Ready for review

0.2 Response organization

Assign incident command, security, IT, privacy, legal, communications, HR, vendor, executive, and board responsibilities. **Review record:** Assign the owner, evidence, dependencies, decision date, and next action.

0.3 Detection and triage

Standardize intake, validation, classification, scope assessment, immediate safeguards, documentation, and escalation targets.

Requirement	Component	Verification	Status
Detection and triage	Core boundary	Automated and review test	Specified
Failure path	Integration boundary	Negative test	In review

0.4 Evidence handling

Define collection authority, time synchronization, chain of custody, protected storage, forensic images, retention, and external support. **Review record:** Assign the owner, evidence, dependencies, decision date, and next action.

0.5 Containment and eradication

Set decision criteria for isolation, credential actions, blocking, remediation, threat hunting, and business trade-offs. **Review record:** Assign the owner, evidence, dependencies, decision date, and next action.

0.6 Recovery and validation

Require clean-state criteria, restoration sequence, heightened monitoring, business validation, and authorization to return to service. **Review record:** Assign the owner, evidence, dependencies, decision date, and next action.

0.7 Communications and notification

Map internal updates, customers, regulators, insurers, law enforcement, media, message approval, and notification deadlines. **Review record:** Assign the owner, evidence, dependencies, decision date, and next action.

0.8 Exercises and improvement

Define tabletop and technical exercises, participant coverage, findings, action ownership, metrics, and annual plan review. **Review record:** Assign the owner, evidence, dependencies, decision date, and next action.