Incident Response Playbook

Generated: December 8, 2025

Executive Summary

Step-by-step procedures for ransomware, data breach, and DDoS scenarios.

Includes stakeholder communication templates and regulatory reporting workflows.

Playbook 1: Ransomware Response

IMMEDIATE ACTIONS (0-1 Hour):

& Isolate affected systems from network immediately
& Activate incident response team and war room
& Preserve evidence - do not reboot or modify systems
& Identify ransomware variant using sample analysis
& Check for decryption tools at NoMoreRansom.org

CONTAINMENT (1-24 Hours):

& Map lateral movement using EDR/SIEM logs
& Identify initial access vector (phishing, RDP, etc.)
& Reset credentials for compromised accounts
& Block C2 communication channels
& Assess backup integrity before restoration

ERADICATION (24-72 Hours):

& Remove malware artifacts from all systems
& Patch exploited vulnerabilities
& Rebuild compromised systems from clean images
& Restore data from verified clean backups

Playbook 2: Data Breach Response

DETECTION & ANALYSIS:

& Confirm data exfiltration through log analysis
& Identify scope: what data, how many records, which customers
& Classify data sensitivity (PII, financial, health)
& Determine attack vector and timeline

CONTAINMENT:

& Revoke compromised API keys and tokens
& Block attacker IP addresses and domains
& Enable additional authentication for affected systems
& Preserve all evidence for forensic analysis

NOTIFICATION:

& CBUAE notification within 24 hours if customer data affected
& VARA notification for virtual asset incidents
& Customer notification within 72 hours per PDPL

Playbook 3: DDoS Response

IMMEDIATE RESPONSE:

& Activate DDoS mitigation service (Cloudflare, Akamai)
& Enable rate limiting and geo-blocking if appropriate
& Scale infrastructure horizontally if cloud-based
& Communicate with ISP for upstream filtering

SUSTAINED ATTACK PROCEDURES:

& Activate secondary/tertiary DNS providers
& Enable additional WAF rules for attack patterns
& Implement CAPTCHA challenges for suspicious traffic
& Consider moving to alternative infrastructure

Stakeholder Communication Template

Subject: [SEVERITY] Security Incident - [Brief Description]

Current Status: [Detection/Containment/Eradication/Recovery]

Impact: [Systems/Data/Customers Affected]

Actions Taken: [Summary of Response Steps]

Next Update: [Time of Next Communication]