TEMPLATE INTELLIGENT iT CYBERSECURITY

Cyber Incident Response Plan Template

A ready-to-customize framework for responding to cybersecurity incidents swiftly and effectively.

Every organization needs a documented incident response plan. Customize this template with your team's contact information, escalation paths, and specific procedures.

1. INCIDENT CLASSIFICATION

- Severity 1 — Critical: Active breach, ransomware, data exfiltration in progress. Immediate all-hands response.
- Severity 2 — High: Confirmed malware, compromised account, or unauthorized access. Response within 1 hour.
- Severity 3 — Medium: Suspicious activity, phishing attempt succeeded, policy violation. Response within 4 hours.
- Severity 4 — Low: Failed attack, informational alert, minor policy deviation. Response within 24 hours.

2. RESPONSE TEAM ROLES

Incident Commander

Leads the response effort. Authorizes containment and communication decisions. Typically IT Director or CISO.

Technical Lead

Performs investigation, forensics, and remediation. Senior engineer or managed security partner.

Communications Lead

Manages internal and external messaging. Coordinates with legal, PR, and regulatory contacts.

Executive Sponsor

Provides business authority for critical decisions (system shutdowns, ransom decisions, regulatory disclosure).

3. COMMUNICATION PLAN

- Internal notification: Alert response team via out-of-band channel (phone, Signal) — never use potentially compromised systems.
- Employee communication: Brief staff on need-to-know basis; provide clear instructions (e.g., do not click, change passwords).
- External notification: Engage legal counsel before contacting regulators, customers, or law enforcement.
- Documentation: Log all actions, decisions, and timestamps in the incident log from minute one.

4. CONTAINMENT & ERADICATION

- Isolate affected systems from the network immediately — disable network ports or Wi-Fi, do not power off.
- Reset credentials for all compromised and potentially compromised accounts.
- Block attacker IOCs (IPs, domains, hashes) at the firewall and endpoint level.
- Engage forensics partner if Severity 1 or 2; preserve evidence (disk images, memory dumps, logs).

5. RECOVERY & POST-INCIDENT

- Restore systems from known-good backups after confirming threat is eradicated.
- Monitor restored systems closely for 72 hours for signs of persistence or reinfection.
- Conduct a post-incident review (blameless retrospective) within 5 business days.
- Update this plan, security controls, and training based on lessons learned.