

DIGITAL FORENSICS & INCIDENT RESPONSE

Incident Response: First 24 Hours Checklist

Use this checklist the moment you suspect a cyber incident. Speed matters, but preserving evidence and making deliberate decisions matters more. Aligned with NIST SP 800-61 Rev. 3 and the NIST Cybersecurity Framework (CSF) 2.0.

Hour 0 to 1: Declare and organize

- ☐ Declare an incident and name an Incident Commander
- ☐ Open an incident log: times, actions, decisions, and who made them
- ☐ Switch to out-of-band communication (phone bridge or separate messaging) if email may be compromised
- ☐ Notify executive leadership and legal counsel; consider outside counsel to protect privilege
- ☐ Notify your cyber insurer using the method in your policy; ask which vendors you must use

Hour 1 to 4: Contain without destroying evidence

- ☐ Isolate affected systems from the network (disconnect, do not power off, unless advised)
- ☐ Disable or reset compromised accounts; revoke sessions and tokens; review MFA methods
- ☐ Block known malicious IP addresses, domains, and file hashes
- ☐ Preserve logs: firewall, endpoint, identity, email, cloud audit logs; extend retention
- ☐ Capture memory and disk images of key systems when feasible
- ☐ Confirm backups are isolated and unaffected before relying on them

Hour 4 to 12: Scope and assess

- ☐ Identify initial access, affected systems, accounts, and data
- ☐ Determine whether data was accessed or exfiltrated
- ☐ Engage digital forensics and incident response (DFIR) support if needed
- ☐ Identify legal, regulatory, and contractual notification duties and deadlines
- ☐ Prepare holding statements for employees, customers, and media

Hour 12 to 24: Recover and communicate

- ☐ Prioritize restoration by business impact; rebuild from known-good images and backups
- ☐ Reset credentials broadly (privileged accounts first) and patch the entry point
- ☐ Increase monitoring for re-entry
- ☐ Report to law enforcement (FBI field office or ic3.gov) as appropriate
- ☐ Brief leadership on status, decisions needed, and next update time
- ☐ Schedule a lessons-learned review once stable

General guidance for training and planning, not legal advice. Adapt to your environment, contracts, and regulators.