CYBERSECURITY
INCIDENT RESPONSE PLAN TEMPLATE

HireEffect

Business Name:

Incident Response Lead:

Last Updated:

Contact Info:

Preparation

- ☐ Identify and document all critical systems, data, and access points
- ☐ Assign an Incident Response Team (IRT) with defined roles:
  - Incident Lead
  - IT Support
  - Communications/PR
  - Legal/Compliance
- ☐ Implement data backup procedures and test recovery processes
- ☐ Ensure all employees are trained on basic security protocols (e.g., phishing awareness, password hygiene)
- ☐ Store this plan in both digital and printed formats

Detection & Identification

- ☐ Document how security events will be detected (e.g., antivirus alerts, email from clients, monitoring tools)
- ☐ Classify the incident type:
  - Phishing
  - Malware/Ransomware
  - Data Breach
  - Insider Threat
  - Unauthorized Access
- ☐ Log the time, date, and nature of the incident
- ☐ Notify the Incident Response Lead immediately

CYBERSECURITY
INCIDENT RESPONSE PLAN TEMPLATE

HireEffect

Containment
- ☐ Disconnect affected systems from the network to prevent spread
- ☐ Preserve evidence (e.g., system logs, email headers, screenshots)
- ☐ Disable compromised accounts or user access
- ☐ Communicate with the IRT and relevant staff only on secure channels
- ☐ Inform key vendors or partners, if necessary

Eradication
- ☐ Remove malware or unauthorized access
- ☐ Patch vulnerabilities or update software
- ☐ Scan all systems to ensure full cleanup
- ☐ Reset passwords and access credentials

Recovery
- ☐ Restore data from backups (validate backup integrity first)
- ☐ Reconnect systems in a controlled, monitored manner
- ☐ Monitor network activity and system performance
- ☐ Test key operations to confirm normal functionality

Post-Incident Review
- ☐ Conduct an incident debrief with all team members
- ☐ Document:
  - What happened
  - How it was handled
  - What could be improved
- ☐ Update policies and procedures based on findings
- ☐ Re-train staff if needed

Communication Plan
- ☐ Internal Notifications:
  - Staff
  - Leadership
- ☐ External Notifications:
  - Affected clients
  - Legal counsel
  - Insurance provider
  - Regulatory bodies (if applicable)

CYBERSECURITY
INCIDENT RESPONSE PLAN TEMPLATE

HireEffect

REAL-WORLD SCENARIO

Here is a real-world scenario to illustrate how to use the Cybersecurity Incident Response Plan Template.

Scenario: A Suspicious Email Leads to a Breach

What happened: An employee at a small bookkeeping firm received an email that looked like it came from a regular vendor. The email included a PDF invoice and a request to confirm payment. Without thinking, the employee clicked the link.

Detection: The antivirus system flagged suspicious behavior within minutes. Strange outbound traffic was detected from the user's workstation.

STEPS TAKEN USING THE TEMPLATE

Detection & Identification

- Incident Response Lead was notified.
- Incident was classified as a phishing attempt with potential malware involvement.
- The IT contact reviewed logs and confirmed unauthorized access attempts.

Containment

- Affected machine was immediately disconnected from the network.
- User account was disabled.
- Email with malicious attachment was quarantined and removed from all inboxes.

Eradication

- Malware was removed from the system.
- All employee passwords were reset.
- Patches were installed to fix a known vulnerability exploited in the breach.

Recovery

- Clean backups were restored.
- Services were tested to ensure systems functioned correctly.
- Email filtering rules were adjusted to block similar future threats.

Post-Incident Review

- A full report was created and shared with leadership.
- Employee received additional phishing awareness training.
- The firm updated its vendor verification process and security protocols.

Outcome: The quick response helped avoid any client data loss or extended downtime. The updated plan is now being reviewed quarterly.