Incident Response Plan Quick glance:

(A quick list of what to do in an attack)

1. ***Identify***
2. ***Contain***
3. ***Eradicate***
4. ***Recover***
5. ***Notify***
6. ***learn***

Phase 1: Identification

Goal: Confirm whether an incident has occurred.

Actions:

- User reports suspicious email or behavior
- Security alert or unusual system activity detected
- IT validates the alert and documents findings

✓ ***Document:*** date, time, systems affected, how discovered

---

Phase 2: Containment Goal: Stop the spread and limit damage.

Immediate actions may include:

- Disable compromised accounts
- Disconnect affected devices from the network
- Block malicious IPs or email senders
- Preserve logs and evidence

⚠️ ***Do not power off systems unless instructed*** (preserves evidence).

Phase 3: Eradication Goal:

Remove the threat completely.

Actions:

- Remove malware or malicious tools
- Reset passwords and revoke tokens
- Patch exploited vulnerabilities
- Remove unauthorized access paths

Phase 4: Recovery Goal:

Restore operations safely.

Actions:

- Restore data from verified
- Backups Monitor systems for re
- Infection Re-enable services in
- Stages Confirm systems are functioning normally

✓ ***Recovery validation required before returning to full operation***

Phase 5: Notification & Communication

Goal: Communicate accurately and responsibly. Notifications may include:

- Executive leadership
- Board of Directors Legal
- counsel Insurance
- provider Affected
- individuals (if required)
- Regulators (if applicable)

📢 ***Only designated staff may communicate externally.***

Phase 6: Lessons Learned

Goal: Improve security posture.

Within 14 days:

- Conduct a post-incident review
- Document root cause Identify
- control failures Update policies,
- training, or technology