Incident Response Checklist

Incident Details

Date & Time Reported

Reported By

Description of the Incident

Initial Response

1. Identify and categorize the incident

   Notes

2. Notify the incident response team

   Notes

3. Assign incident handler

   Handler Name / Contact

Containment

1. Isolate affected systems/services

   Actions taken

2. Preserve evidence (logs, images, etc.)

   Actions taken

3. Document current status

   Notes

Eradication

1. Identify root cause

Root cause

2. Remove malicious components/intruders

   Details

3. Apply patches/updates

   Details

Recovery

1. Restore affected systems/services

   Details

2. Monitor for signs of recurring incident

   Monitoring steps

3. Communicate recovery status to stakeholders

   Notes

Post-Incident

1. Conduct post-incident review

   Lessons learned

2. Update documentation and procedures

   Action items

3. Report to required parties (management, compliance, etc.)

   Details

Incident Log

Time	Action	Owner	Notes