Data Center Incident Response Checklist

1. Detection & Identification

- □ Confirm incident alert/notification received
- □ Identify affected systems, devices, or areas
- □ Document date, time, and nature of incident

2. Initial Response

- □ Notify Incident Response Team members
- □ Inform Data Center Manager and relevant stakeholders
- □ Assess severity and potential impact

3. Containment

- □ Isolate affected systems or zones (if necessary)
- □ Preserve evidence/logs
- □ Implement temporary fixes to limit spread/damage

4. Investigation & Analysis

- □ Collect detailed information (logs, surveillance, audits)
- □ Determine incident root cause
- □ Assess damage and affected assets

5. Eradication

- □ Remove threats or unauthorized access
- □ Patch vulnerabilities or misconfigurations
- □ Sanitize compromised devices/systems

6. Recovery

- □ Restore systems and services to normal operation
- □ Monitor affected systems for reoccurrence
- □ Communicate with stakeholders regarding status

7. Post-Incident Activities

- □ Conduct incident debrief/review meeting
- □ Document lessons learned and update procedures

- □ Prepare and submit incident report

> **Note:** This is a sample checklist. Customize as needed for your specific data center procedures and requirements.