

Navigate Incidents Like a Pro with this Incident Response Checklist

Organization: [Your Organization Name]

Plan Version: [Version Number]

Last Updated: [Date]

<p> Incident Response Team </p> <p>Step 1</p> <ul style="list-style-type: none"> ▶ Incident Response Team Leader: [Name] ▶ Technical Lead: [Name] ▶ Communications Lead: [Name] ▶ Legal/Compliance Lead: [Name] ▶ Public Relations Lead: [Name] 	<p> Notification Process </p> <p>Step 5</p> <ul style="list-style-type: none"> ▶ When an incident occurs, the team leader is to be notified immediately. ▶ The team leader will assess the situation and determine the incident's category. ▶ If it's a Category 1 incident (see section 3), the full incident response team will be active. For Category 2 and 3 incidents, only relevant team members will be contacted. ▶ The communications lead will draft incident messages for internal and external stakeholders. ▶ Messages will be sent out through appropriate channels (email, SMS, phone, social media) and can also be posted on your statuspage for real-time updates.
<p> Key Stakeholders </p> <p>Step 2</p> <ul style="list-style-type: none"> ▶ Employees ▶ Customers ▶ Partners ▶ Regulatory Agencies ▶ Local Authorities ▶ General Public 	<p> Team Roles and Responsibilities </p> <p>Step 6</p> <ul style="list-style-type: none"> ▶ Team Leader: Overall incident coordination and decision-making. ▶ Technical Lead: Technical assessment and remediation. ▶ Communications Lead: Message drafting and distribution. ▶ Legal/Compliance Lead: Ensure regulatory and legal compliance. ▶ Public Relations Lead: Manage media interactions and public image.
<p> Incident Categories </p> <p>Step 3</p> <ul style="list-style-type: none"> ▶ Category 1 (Critical): Incidents with a severe impact on operations, safety, or data security. ▶ Category 2 (Major): Incidents with a significant but manageable impact. ▶ Category 3 (Minor): Incidents with a minor impact that require notification and resolution. 	<p> Message Content should include </p> <p>Step 7</p> <p>Nature of the incident, impact on stakeholders, actions being taken to resolve the incident, expected resolution timeline, and contact information for the support team to address any concerns. Here are a few references you can use.</p>
<p> Communication Channels </p> <p>Step 4</p> <p>Email, SMS, Phone calls, Social media, Website Public Status Page.</p>	<p> Training and Drills </p> <p>Step 8</p> <ul style="list-style-type: none"> ▶ Conduct quarterly incident response drills and review sessions. ▶ Ensure all team members are well-versed in the incident response plan.