SOP Template: Roles and Responsibilities Assignment During Incidents

This SOP defines the **roles and responsibilities assignment during incidents** to ensure clear accountability and effective incident management. It outlines the specific duties of each team member, communication protocols, and coordination mechanisms for timely response and resolution. This procedure is designed to enhance organizational preparedness, minimize confusion, and improve overall incident response efficiency.

1. Purpose

To establish a standardized process for assigning roles and responsibilities during incidents to ensure effective incident response, minimize disruptions, and protect organizational assets.

2. Scope

This SOP applies to all staff involved in incident response, across all departments and locations within the organization.

3. Roles and Responsibilities

Role	Responsibilities
Incident Manager	- Lead the incident response team. - Assign roles and coordinate response activities. - Serve as the primary point of contact. - Ensure accurate documentation and reporting.
Communications Lead	- Manage internal and external communications. - Prepare and distribute incident updates. - Liaise with stakeholders as directed by the Incident Manager.
Technical Lead	- Analyze and address the technical aspects of the incident. - Coordinate with IT/Security teams. - Provide technical guidance on response actions.
Documentation Lead	- Maintain a log of all incident-related actions and decisions. - Compile incident reports for review.
Support Staff	- Assist leads as required (logistics, technical work, notifications, etc.). - Perform assigned tasks as delegated by leads.

4. Incident Response Procedure

1. **Incident Detection:** Identify to trigger the SOP when an incident is reported or detected.
2. **Role Assignment:** The Incident Manager assigns primary and backup individuals to each role as per the incident's requirements and availability.
3. **Team Briefing:** Conduct an initial briefing to confirm roles, responsibilities, and communication lines.
4. **Incident Management:**
   - Each member carries out defined responsibilities.
   - Escalate issues to the Incident Manager as needed.
5. **Communications:** All communications follow the designated chain and protocols set by the Communication Lead.
6. **Documentation:** Record all actions, decisions, and changes for review and reporting purposes.
7. **Incident Closure:** After resolution, hold a debriefing to identify lessons learned and update the SOP as necessary.

5. Communication Protocol

- Use designated communication channels (e.g., incident command chat, phone, email).
- All critical updates must be documented and acknowledged by the Incident Manager.
- External communications must be approved by the Communications Lead and Incident Manager.

6. Review and Improvements

- Review this SOP annually and after each major incident.
- Update based on feedback and post-incident reviews.

7. References

- Incident Response Plan
- Business Continuity Policy
- Organization Chart

8. Appendix

Template for Role Assignment:

Incident Type	Incident Manager	Communications Lead	Technical Lead	Documentation Lead	Support Staff
[Specify]	[Name]	[Name]	[Name]	[Name]	[Name]