[Organization Name] Incident Management Procedure - ISO 27001

1. **Purpose**
   * To establish a consistent and effective process for identifying, reporting, responding to, and learning from information security incidents in accordance with ISO 27001 requirements.
   * To minimize the impact of security incidents on the organization's information assets, operations, and reputation.
2. **Scope**
   * This procedure applies to all information security incidents involving the organization's information assets, systems, and personnel, including incidents related to physical security, cybersecurity, and data privacy.
3. **Responsibilities**
   * Management: Ensuring the implementation and continuous improvement of the incident management process.
   * Incident Response Team (IRT): Managing and coordinating the response to information security incidents.
   * Employees: Reporting suspected or confirmed security incidents and cooperating with the incident response process.
4. **Incident Identification**
   * Monitoring: Implement continuous monitoring of systems, networks, and applications to detect potential security incidents.
   * Employee awareness: Provide training and awareness programs to help employees identify and report security incidents.
5. **Incident Reporting**
   * Reporting channels: Establish clear and accessible reporting channels for employees to report suspected or confirmed security incidents (e.g., email, phone hotline, incident reporting form).
   * Incident details: Collect relevant details about the incident, such as the date and time, affected assets, and a description of the event.
   * Confidentiality: Ensure that incident reports are treated confidentially to encourage reporting and protect sensitive information.
6. **Incident Assessment**
   * Triage: Evaluate the reported incident to determine its severity, impact, and priority for response.
   * Escalation: Escalate the incident to the appropriate level of management and the IRT based on the assessment.
7. **Incident Response**
   * Activation: Activate the IRT to coordinate and manage the response to the incident.
   * Containment: Implement measures to contain the incident and prevent further damage or spread.
   * Investigation: Collect and analyze evidence to determine the cause and extent of the incident.
   * Eradication: Remove the cause of the incident and eliminate any remaining threats or vulnerabilities.
   * Recovery: Restore affected systems and processes to normal operations.
8. **Incident Communication**
   * Internal communication: Keep relevant stakeholders informed of the incident status and response actions.
   * External communication: Coordinate communication with external parties, such as customers, vendors, regulators, or law enforcement, as required.
9. **Incident Closure**
   * Incident review: Conduct a post-incident review to identify lessons learned and opportunities for improvement.
   * Corrective actions: Implement corrective actions to address the root cause of the incident and prevent recurrence.
   * Documentation: Update the incident record with the final status, resolution, and any follow-up actions.
10. **Continuous Improvement**

* Incident metrics: Track and analyze incident metrics to identify trends and areas for improvement.
* Procedure review: Regularly review and update the incident management procedure to ensure its effectiveness and alignment with the organization's needs.