# ISO 27001-Compliant Incident Management Communications Plan Template

## Introduction

This Incident Management Communications Plan aligns with ISO 27001 standards, ensuring a structured approach to communicating during security incidents. The plan establishes clear communication channels, roles, and responsibilities to minimize the impact of incidents on organizational operations and stakeholders.

## Purpose

The purpose of this plan is to define a framework for effective communication during security incidents, ensuring accurate and timely information dissemination to relevant parties. Effective communication strengthens organizational resilience by enabling coordinated responses, maintaining stakeholder trust, and ensuring compliance with legal and regulatory requirements. This also helps protect the organization’s reputation during challenging situations.

## Scope

This plan applies to all types of security incidents affecting the organization, including:

* Cyberattacks (e.g., ransomware, phishing)
* Data breaches or leaks
* Physical security breaches
* Service disruptions affecting critical operations

## Policy Statement

The organization is committed to managing incident-related communications effectively by:

* Defining roles and responsibilities for communication during incidents.
* Establishing communication channels for internal and external stakeholders, such as email alerts, intranet announcements, press releases, or social media updates.
* Ensuring accurate, consistent, and timely information dissemination.
* Protecting sensitive information while meeting regulatory and contractual obligations.

The plan includes the following six steps:

1. Incident Identification and Assessment: Determine the nature, scope, and impact of the incident to guide communication strategies.
2. Stakeholder Identification: Identify internal and external stakeholders who need to be informed about the incident.
3. Message Development: Create tailored messages with clear, accurate, and concise information for different stakeholder groups.
4. Approval Process: Establish a process for reviewing and approving messages before dissemination.
5. Dissemination: Use predefined communication channels to distribute messages, such as email, intranet, or press releases.
6. Post-Incident Review: Evaluate the effectiveness of communication efforts and incorporate lessons learned into future planning.

## Roles and Responsibilities

* Incident Response Team Lead: Coordinates communication efforts and ensures alignment with incident response activities.
* Communications Manager: Develops and reviews incident-related messages and ensures consistency across communication channels.
* Information Security Officer: Validates the accuracy of technical details and ensures compliance with ISO 27001 requirements.
* Legal Counsel: Reviews messages to ensure compliance with legal and regulatory requirements.
* Executive Leadership: Approves high-level communications and engages with external stakeholders when necessary.

## Compliance and Monitoring

Compliance with this plan will be ensured through:

* Regular testing of communication procedures during incident response drills.
* Implementation of key performance indicators (KPIs), such as:

- Time taken to disseminate initial incident notifications.

- Accuracy and clarity of messages as evaluated in post-incident reviews.

- Stakeholder satisfaction with communication efforts.

Non-compliance incidents will be documented, and corrective actions will be implemented to address gaps.

## Related Documentation

* Incident Response Plan
* Business Continuity Plan
* Information Security Policy
* Data Breach Notification Procedure

## Review and Revision

This plan will be reviewed annually or following significant incidents. The Incident Response Team Lead will initiate the review process, and updates will be communicated to stakeholders. All changes will be documented and approved through a formal review process.

## Narrative Guidance

This plan emphasizes the critical role of communication in effective incident management. It aligns with ISO 27001 principles of accountability, risk management, and continuous improvement. Organizations should adapt this template to address specific incident types and stakeholder needs.

## Instructions for Use

* Replace placeholders with organization-specific details.
* Ensure alignment with related policies and standards.
* Collaborate with stakeholders to tailor the plan to organizational risks and operational contexts.