NIST Incident Response Communication Plan

To establish a structured approach for responding to and managing security incidents in accordance with NIST guidelines, ensuring timely and effective communication.

Incident Response Phases Table

Phase	Description	Communication Actions
Preparation	Establishing the incident response capability.	Develop communication protocols and contact lists.
Detection & Analysis	Identifying and analyzing incidents.	Notify response team; initiate incident tracking.
Containment, Eradication, & Recovery	Limiting the impact of the incident and removing the threat.	Coordinate with stakeholders; provide status updates.
Post-Incident Activity	Learning from the incident and improving defenses.	Debrief stakeholders; update response strategies.

Communication Channels Graph

- **Internal Channels:** Email Alerts, Intranet Announcements, Secure Messaging.
- **External Channels:** Press Releases, Social Media Updates, Public Statements.

Key Roles and Responsibilities

- **Incident Response Manager**: Oversees incident management, coordinates communication.
- **IT Security Team**: Manages technical aspects of incident response.
- **PR & Communications Officer**: Handles external and internal communications.
- **Legal Advisor**: Advises on legal implications and compliance issues.

Incident Severity Classification

- **Low**: Minimal impact; routine response.
- **Medium**: Moderate impact; coordinated response.
- **High**: Significant impact; immediate and comprehensive response.

Performance Metrics

- Time to detect and respond to incidents.
- Effectiveness of communication (reach and clarity).
- Incident resolution time.
- Stakeholder satisfaction.

Review and Update Cycle

- Regularly scheduled reviews of the communication plan.
- Updates following significant incidents or changes in the organization.

This NIST-based communication plan provides a comprehensive, easy-to-implement framework suitable for any organization seeking to enhance its incident response capabilities. It aligns with best practices for cybersecurity incident management and can be tailored to specific organizational needs