# Security Incident Response Communication Plan

To efficiently manage and communicate during security incidents, minimizing impact and maintaining stakeholder trust.

### Incident Response Communication Strategy Table

| Stage | Action | Tools/Channels |
|---|---|---|
| **Preparation** | Establish communication protocols and emergency contacts. | Contact Lists, Communication Policy Document |
| **Identification** | Notify key stakeholders of potential incident. | Email Alerts, Secure Messaging |
| **Containment** | Provide ongoing updates as incident is being contained. | Internal Briefings, Secure Conference Calls |
| **Eradication** | Communicate eradication measures and progress. | Intranet Updates, Encrypted Emails |
| **Recovery** | Inform stakeholders when normal operations resume. | Company-wide Announcements, Press Statements |
| **Post-Incident** | Conduct post-incident review and communicate lessons learned. | Webinars, Detailed Reports |

### Implementation Timeline Graph

1. **Immediate**: Activation of the communication plan upon incident identification.
2. **Ongoing**: Regular updates throughout containment, eradication, and recovery stages.
3. **Post-Incident**: Summary communication and debrief within one week of incident resolution.

## Key Performance Indicators (KPIs)

- Time to first communication post-incident
- Accuracy of information disseminated
- Stakeholder satisfaction with communication efforts
- Completion of post-incident communication

## Roles and Responsibilities

- **Incident Communication Lead**: Primary point of contact for all communications.
- **IT Security Team**: Provides technical updates and incident status.
- **HR Manager**: Manages internal communications and employee relations.
- **Public Relations Officer**: Handles external communications, including media.

## Budget Considerations

Allocate funds for necessary communication tools, training, and potential external communication assistance.

## Review and Adaptation Plan

Regular assessment of communication effectiveness, with adjustments made based on feedback and evolving security landscapes.
This plan serves as a straightforward, comprehensive guide for handling communication during security incidents, adaptable to different organizational sizes and types.