Communication Protocol for Network Security Incidents

1. Purpose

This document outlines the standardized procedures for reporting, escalating, and communicating network security incidents within the organization.

2. Scope

Applies to all employees, contractors, and third-party vendors who detect or become aware of security-related events impacting the corporate network.

3. Incident Reporting Procedure

1. **Detection:** Identify potential security incident (e.g., suspicious emails, unauthorized access, malware).
2. **Notification:** Immediately inform the IT Security Team via designated channels (e.g., *security@company.com* or phone extension).
3. **Documentation:** Record time, date, and details of the incident. Include affected systems, nature of event, and steps taken.
4. **Containment:** Follow IT Security Team instructions; do not alter affected systems unless directed.

4. Communication Flow

Stage	Responsible	Method	Audience
Initial Notification	Discoverer	Email/Phone	IT Security Team
Incident Assessment	IT Security Team	Email/Meeting	Relevant Department Heads
Escalation	IT Security Manager	Phone/Email	Executive Management
Update & Resolution	IT Security Team	Email/Report	All Stakeholders

5. Roles & Contact Information

- **IT Security Team:** Handles assessment, containment, and eradication.
- **Incident Response Lead:** Point-of-contact for major incidents.
- **Department Heads:** Liaison for affected business operations.

6. Confidentiality & External Communications

- Do not disclose incident details to non-authorized persons.
- All external communication must be approved by Management and the Legal Department.

7. Post-Incident Review

1. Conduct debrief and root cause analysis.
2. Document findings and recommendations.
3. Update procedures and provide training if necessary.

8. Document History

Date	Version	Description

YYYY-MM-DD	1.0	Initial draft