Network Security Incident Escalation Process

1. Purpose

The purpose of this document is to outline the steps and procedures for escalating network security incidents to ensure timely and appropriate response.

2. Scope

This process covers all employees, systems, and data within the organization's network infrastructure.

3. Roles & Responsibilities

Role	Responsibility
Incident Reporter	Identifies and reports network security incidents.
IT Support	Initial incident analysis and documentation.
Security Team	Investigation, containment, and escalation management.
Management	Decision-making for critical escalations.

4. Incident Classification

- **Low:** Minor incidents with minimal impact.
- **Medium:** Incidents with moderate impact, may require coordination.
- **High:** Critical incidents with severe impact on business operations.

5. Escalation Steps

1. **Detection:** Any employee who identifies an incident reports to IT Support.
2. **Initial Assessment:** IT Support gathers details and classifies the incident.
3. **Notification:** Security Team is notified for medium and high impact incidents.
4. **Investigation & Containment:** Security Team investigates and takes initial containment actions.
5. **Escalation:** High impact incidents are escalated to Management for further action.
6. **Resolution:** Incident is resolved, documented, and closed by the Security Team.
7. **Post-Incident Review:** Lessons learned are documented and shared.

6. Contact Information

Team	Contact Method
IT Support	itsupport@domain.com
Security Team	security@domain.com
Management	management@domain.com

7. Document Control

Version: 1.0

Effective Date: [YYYY-MM-DD]

Owner: Network Security Team