

---

# Network Security Incident Report

## Report Details

- **Incident ID:** [Unique Identifier]
- **Incident Date:** [Date]
- **Reported By:** [Name, Title, Department]
- **Contact Information:** [Phone, Email]

## Incident Summary

- **Type of Incident:** [DDoS Attack, Unauthorized Access, Firewall Breach, etc.]
- **Affected Network/Systems:** [List of affected systems]
- **Date and Time Detected:** [Date and Time]

## Incident Description

[Provide a detailed account of the network security incident, including suspicious traffic patterns, vulnerabilities exploited, and detection methods.]

## Immediate Response

- **Actions Taken:**
  - [Action 1: Isolating the affected network segment]
  - [Action 2: Blocking malicious IPs]
  - [Action 3: Updating firewall rules]
- **Responsible Team:** [Name of the team or individual responsible]

## Impact Assessment

- **Affected Services:** [Details of service disruptions]
- **Downtime Duration:** [Hours/Days]
- **Potential Data Loss:** [Details of any compromised data]

### Investigation Findings

- **Root Cause:** [Explain what led to the breach or attack]
- **Key Findings:**
  - [Finding 1: Description]
  - [Finding 2: Description]

### Corrective and Preventive Measures

- **Corrective Actions:** [List actions to resolve the issue]
- **Preventive Measures:** [List network security enhancements]

### Sign-Off

- **Prepared By:** [Name and Signature]
- **Reviewed By:** [Name and Signature]