

---

# IT Security Incident Report

## Report Details

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

## Incident Summary

- **Incident Type:** [Malware Attack, Phishing, Data Breach, Unauthorized Access, etc.]
- **Date and Time of Incident:** [Date and Time]
- **Location/Asset:** [IT System, Database, Endpoint Device, etc.]
- **Affected Systems:** [List of impacted servers, networks, or databases]

## Incident Description

[Provide a detailed account of the IT security incident, including how it was discovered, the timeline of events, and the scope of the impact.]

## Immediate Response

- **Actions Taken:** [List actions to contain and mitigate the threat]
- **Responsible Team:** [Name of the IT team or individual responsible]

## Impact Assessment

- **Data Compromised:** [Details of data loss or exposure]
- **Downtime:** [Duration of service disruptions]

- **Financial Impact:** [Cost of the incident, if applicable]

### **Investigation Findings**

[Summarize key findings, such as root cause, methods of attack, and weaknesses exploited.]

### **Corrective and Preventive Measures**

- **Corrective Actions:** [List actions taken to resolve the issue]
- **Preventive Measures:** [List changes to policies, tools, or infrastructure]

### **Sign-Off**

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