[Company Name] | 1

# Incident Report

Date: [Today’s Date]

Reported by: Team[]

Incident Type:

Affected Host:

Initial Access Timestamp:

Remediated Timestamp:

**Incident Summary:**

[Paragraph format, 2-3 sentences about what happened and how it was resolved]

**Impact**

* [Scope, monetary impact, service downtime, affected accoutn/user, etc]
* [Multiple bullet points, not just one]

**Timeline of Events**

**Investigation:**

* [Source IP address (attacker), destination IP address, port and service, remediated timestamp, detection method]
* [Evidence]

**Eradication:**

* [Explain what was done to eradicate the threat]
* [Evidence]

**Remediation:**

* [Explain how incident was resolved and remediated]
* [Evidence]