**Company Name**Street  
City

**Incident Report**

**Report Date/Time:** January 1, 2004 / 11:00 AM  
  
**Confidentiality**

Distribution of this document is limited to *Company Department*. Access should only be granted to those with a business related need-to-know. If you have any questions pertaining to the distribution of this document, please contact *John Smith*.

##### Point of Contact (POC) Information

Name:

Title:

Telephone:

Fax:

E-mail:

##### Summary

The summary is at a high level, suitable for upper management. Elements include:

° Basic description of the incident

° Systems, services and/or user communities impacted by the incident

° Whether service was not impacted, degraded, or interrupted

° Duration of the incident (start to finish)

##### Details of the Incident

Specifically, what caused the incident (who, what, where, when, how)?

##### The Notification Process

° Include every step in the notification process

° Automated monitoring notification

° An infrastructure team member noticed something out of the ordinary

° A user called in

° Detail the flow of the incident response (i.e. John -> Jim -> Mike)

° Communication of resolution of the outage

##### Technical Details / Fix Actions

° Specific details of troubleshooting

° Specific changes (configuration, hardware, etc)

° Steps to confirm the outage was resolved

° Ticket numbers

##### Conclusion

° What was the basic cause of the incident?

° What could have prevented this?

° impact (none, degraded performance, downtime)

° business criticality (revenue producing, business critical, low)  
° estimated cost (impact + business criticality)

° What prevents the incident from reoccurring?

° What additional actions or research need to happen?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name:

Title:

**APPENDIX**

° Logs or error messages

° Contents of trouble tickets

° Contents of e-mail