**Incident Response Plan**

|  |
| --- |
| **SECURITY INCIDENT REPORT** |
| **Report Classification:** |
| **Report No.:** **Report Organization:** |
| **Report Date:** **Report Type** (Initial, Final, Status): |
| **Report Generated By:**  Date:  Time: |
| Title:  Telephone:  Email: |
| Signature: |
| **SECTION 1 - POC Information** |
| Incident Reported By:  Date:  Time: |
| Location:  Telephone:  Email: |
| Signature: |
| Network Owner Notified (Name):  Date:  Time: |
| Location:  Telephone:  Email: |
| Method of Notification: |
| **Section 2 - Incident Information** |
| Date of Incident:  Time of Incident:  Ongoing? |
| Incident Network Name:  Incident Physical Facility Location: |
| Affected Computer Systems (Hardware and/or Software): |
| Classification of Affected Computer Systems: |
| Physical Location of Affected Systems: |
| Connections of Affected Systems to Other Systems: |
| Type of Incident (Data Destruction/Corruption, Data Spill, Malicious Code, Privileged User Misuse, Security Support Structure Configuration Modification, System Contamination, System Destruction/Corruption/Disabling, Unauthorized User Access, other – please identify): |
| Suspected Method of Intrusion/Attack: |
| Apparent Source (e.g., IP address) of Intrusion/Attack: |
| Apparent Target/Goal of Intrusion/Attack: |
| Mission Impact:  Success/Failure of Intrusion/Attack: |
| Recommendations for Containment/Eradication of incident to network owner |
| Attach technical details of incident thus far. Include as much as possible about the Detection and Identification, Containment, Eradication, and Recovery – steps taken (with date/timestamps), persons involved, files saved for analysis, etc. |