|  |  |
| --- | --- |
| **INCIDENT IDENTIFICATION INFORMATION** | |
| Date and Time of Notification: | |
| Incident Detector’s Information: | |
| Name: | Date and Time Detected: |
| Title: | Location: |
| Phone/Contact Info: | System or Application: |
| **INCIDENT SUMMARY** | |
| **Type of Incident Detected:**  ☐ Denial of Service ☐ Malicious Code ☐ Unauthorized Use  ☐ Unauthorized Access ☐ Unplanned Downtime ☐ Other | |
| **Description of Incident:**  Severity Level:  Counter measure was: | |
| **Names and Contact Information of Others Involved:**   1. **XXXXX Operation Department** 2. **XXXX Operation Department**   **<NGO> Incident Response Team XXXXXX** | |
| **INCIDENT NOTIFICATION – OTHERS** | |
| ☐ IS Leadership ☐ System or Application Owner ☐ System or Application Vendor  ☐ Security Incident Response Team ☐ Public Affairs ☐ Legal Counsel  ☐ Administration ☐ Human Resources  ☐ Other: | |
| **ACTIONS** | |
| **Identification Measures (Incident Verified, Assessed, Options Evaluated):** | |
| **Containment Measures:** | |
| **Evidence Collected (Systems Logs, etc.):**  **Registry changes by malware** | |
| **Eradication Measures:** | |
| **Recovery Measures:** | |

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only.

|  |
| --- |
| **EVALUATION** |
| **Other Mitigation Actions:** |
| **Were the Documented Procedures Followed? Were They Adequate?** |
| **What Information Was Needed Sooner?** |
| **Were Any Steps or Actions Taken That Might Have Inhibited the Recovery?** |
| **What Could Work Force Members Do Differently the Next Time an Incident Occurs?** |
| **What Corrective Actions Can Prevent Similar Incidents in the Future?** |
| **What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents?** |
| **Other Conclusions or Recommendations:** |
| **FOLLOW-UP** |
| **Reviewed By:**  ☐ Security Officer ☐ IS Department/Team  ☐ Privacy Officer ☐ Other |
| **Recommended Actions Carried Out:** |
| **Initial Report Completed By:** |
| **Malware Information:** |

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only.