**Security Incident Response Form**

**Reporter’s Information**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Date and Time of Notification: | | | | |  | | | | | | |
| 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:** | |  |
|  |  | |
|  | |  |

|  |  |  |
| --- | --- | --- |
| **Names and Contact Information of Others Involved:** | |  |
|  |  | |
|  | |  |

**Incident Notification – Others**

|  |  |  |  |
| --- | --- | --- | --- |
| ☐ IT Department | | ☐ Legal Counsel | ☐ System or Application Vendor |
| ☐ Security Incident Response Team | | ☐ Human Resources | ☐ Public Affairs |
| ☐ Administration | |  |  |
| ☐ Other: |  | | |

**Actions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Identification Measures (Incident Verified, Assessed, Options Evaluated):** | | |  |
|  |  | | |
|  | |  | |

|  |  |  |
| --- | --- | --- |
| **Containment Measures:** | |  |
|  |  | |
|  | |  |

|  |  |  |
| --- | --- | --- |
| **Evidence Collected (Systems Logs, etc.):** | |  |
|  |  | |
|  | |  |

|  |  |  |
| --- | --- | --- |
| **Recovery Measures:** | |  |
|  |  | |
|  | |  |

|  |  |  |
| --- | --- | --- |
| **Other Mitigation Actions:** | |  |
|  |  | |
|  | |  |

**Evaluation**

|  |  |  |
| --- | --- | --- |
| **How Well Did Work Force Members Respond?** | |  |
|  |  | |
|  | |  |

|  |  |  |
| --- | --- | --- |
| **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 be done differently to improve the process?** | |  |
|  |  | |
|  | |  |

|  |  |  |
| --- | --- | --- |
| **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 | ☐ IT Department |
| ☐ Privacy Officer | ☐ Other |

|  |  |  |
| --- | --- | --- |
| **Recommended Actions Carried Out:** | |  |
|  |  | |
|  | |  |

|  |  |  |
| --- | --- | --- |
| **Initial Report Completed By:** | |  |
|  |  | |
|  | |  |

|  |  |  |
| --- | --- | --- |
| **Follow-Up Completed By:** | |  |
|  |  | |
|  | |  |