Sample Security Incident Response Report Form

Privileged and Confidential Attorney-Client Communication/Work Product

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:

_____

_____

Names and Contact Information of Others Involved:

_____

_____

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.):

_____

_____

Eradication Measures:

_____

Recovery Measures:

_____

Other Mitigation Actions:

_____

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

Sample Security Incident Response Report Form

Privileged and Confidential Attorney-Client Communication/Work Product

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 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:

_____

Follow-Up Completed By:

_____

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