INFORMATION SECURITY INCIDENT REPORT FORM

INCIDENT IDENTIFICATION INFORMATION	
Incident Detector's Information:	
Name:	Date/Time Detected:
Title:	Location:
Phone/Contact Info:	System/Application:

INCIDENT SUMMARY		
Type of Incident Detected:		
Denial of Service	Malware / RansomWare	Unauthorized Use / Disclosure
Loss / theft		
Unauthorized Access	Unplanned Downtime	Inadvertent site security
Phishing		Other:

Description of Incident:
Names of Others Involved:

INCIDENT NOTIFICATION	
IS Leadership	System/Application Owner
Security Incident Response Team	System/Application Vendor
Administration	Public Affairs
Human Resources	Legal Counsel
Other:	

ACTIONS (Include Start & Stop Times)
(Phase I) Identification Measures (Incident Verified, Assessed, Options Evaluated):
(Phase II) Containment Measures:
Evidence Collected (Systems Logs, etc.):
(Phase III) Eradication Measures:

ACTIONS (Include Start & Stop Times)

ACTIONS (Include Start & Stop Times)
(Phase IV) Recovery Measures

EVALUATION
How Well Did the Workforce 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 the Workforce 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/Recommendations:

FOLLOW-UP		
Review By (Organization to determine)**:**	Security Official	IS Department/Team
	Other:	
Recommended Actions Carried Out:		

Initial Report Completed By:	
Follow-Up Completed By:	