IT and Data Security Incident Reporting Form

1. Contact Information	
Full name: Job title:	
Section/Department:	
Work phone:	
Mobile phone:	
E-mail address:	
[illegible]	

Additional Contact Information:

2. Type of Incident *{Insert X on all that apply)*

☐	Account Compromise *(e.g., Lost Password)*
☐	Denial-of-Service *(Including Distributed)*
☐	Malicious Code *(e.g., Virus, Worm, Trojan)*
☐	Misuse of Systems *(e.g., Acceptable Use)*
☐	Reconnaissance *(e.g., Scanning, Probing)*
☐	Power outage
☐	System unavailable

☐	Social Engineering *(e.g., Phishing, Scams)*
☐	Technical Vulnerability *(e.g., 0-day Attacks)*
☐	Theft/Loss of Equipment or Media
☐	Unauthorized Access *(e.g., Systems, Devices)*
☐	Other (please describe below}

Description of Incident:

3. Scope of Incident *(Insert X on all that apply)*

☐	Critical *(e.g., Affects Society-Wide Information Resources)*
☐	High *(e.g., Affects Entire Network or Critical Business or Mission Systems)*
☐	Medium *(e.g., Affects Network Infrastructure, Servers, or Admin Accounts)*
☐	Low *(e.g., Affects Workstations or User Accounts Only)*
☐	Unknown/Other *{Please Describe Below)*

NOTE: All incidents deemed critical or high require additional notification by phone.

IT and Data Security Incident Reporting Form

Estimated Quantity of Systems	
Affected: Estimated Quantity of Users	
Affected:	

Third Parties Involved or Affected:
(e.g., Vendors, Contractors, Partners)

Additional Scope Information:

4. Impact of Incident *(Insert X on all that apply)*

☐	Loss of Access to Services	☐	Propagation to Other Networks
☐	Loss of Productivity	☐	Unauthorized Disclosure of Information
☐	Loss of Reputation	☐	Unauthorized Modification of
☐	Loss of Revenue Information	☐	Unknown/Other *(Please describe below)*

Additional Impact Information:

5. Sensitivity of Affected Data/Information *(Insert X on all that apply)*

☐	Critical Information	☐	Personally Identifiable Information
☐	(PII)Non-Critical Information	☐	Intellectual/Copyrighted
☐	Information	☐	
☐	Publicly Available Information	☐	Critical Infrastructure/Key Resources
☐	Financial Information	☐	Unknown/Other *(Please Describe Below)*

Data Encrypted?	
Quantity of Information Affected:	

(e.g., File Sizes, Number of Records)

IT and Data Security Incident Reporting Form

Additional Affected Data Information:

6. Systems Affected by Incident *(Provide as much detail if relevant and if possible)*	
Attack Sources *(e.g., IP Address, Port):*	
Attack Destinations *(e.g., IP address, Port):*	
IP Addresses of Affected Systems:	
Domain Names of Affected Systems:	
Primary Functions of Affected Systems: *(e.g., Web Server, Domain Controller)*	
Operating Systems of Affected Systems: *(e.g., Version, Service Pack, Configuration)*	
Patch Level of Affected Systems: *(e.g., Latest Patches Loaded, Hotfixes)*	
Security Software Loaded on Affected Systems: *(e.g., Anti-Virus, Anti-Spyware, Firewall, Versions, Date of Latest Definitions)*	
Physical Location of Affected Systems: *(e.q., State, City, Building, Room, Desk)*	
Additional System Details:	

7. Users Affected by Incident *(Provide as much detail as possible)*	
Names and Job Titles of Affected Users:	
System Access Levels or Rights of Affected Users: *(e.g., regular User, Domain Administrator, Root)*	
Additional User Details:	

IT and Data Security Incident Reporting Form

8. Timeline of Incident *(Provide as much detail as possible)*	
a. Date and Time When First Detected, Discovered, or Was Notified About the Incident:	
b. Date and Time When the Actual Incident Occurred: *(Estimate **If** Exact Date and Time Unknown)*	
c. Date and Time When The Incident Was Contained or When All Affected Systems or Functions Were Restored: *(Use Latest Date and Time)*	
Elapsed Time Between the Incident and Discovery: *(e.g., Difference Between a. and b. Above)*	
Elapsed Time Between the Discovery and Restoration: *(e.g., Difference Between a. and c. Above)*	
Detailed Incident Timeline:	

9. Remediation of Incident *(Provide as much detail as possible)*	
Actions Taken To Identify Affected Resources:	
Actions Taken to Remediate Incident:	
Actions Planned to Prevent Similar Incidents:	
Additional Remediation Details:	