Incident Handling Report Form

Section: Reporter's Contact Information

First Name	
Last Name	
Email Address	
Telephone number	
Department name	

Section: Incident Summary

Who identified the incident?	
What automated system triggered the alert? (if applicable)	
What system(s) was/were involved?	☐Email ☐Internet Access ☐Intranet Access ☐Database ☐Webserver ☐Host Machine (Laptop, Workstation) Other:
What is the approximate time the incident started? (Local time.)	
When was this incident detected? (Local time.)	
What is the potential level of impact to the organization by the incident?	
What is the current status or resolution of this incident?	

Section: High-Level Incident Description

Please provide a short description of the incident and impact.

- How did the incident happen?
- When (as best can be determined) did the incident begin and end?
- What is the verified scope or depth of the incident?
- Who/what was the source of the incident?
- What are the immediate and future recommendations for response?
- The current status of the incident, including current response efforts (when appropriate)
- Short-term incident remediation measures and the impact on business
- Long-term incident remediation measures and the impact on business

Section: Incident Details

Please provide a detailed description of the incident and impact.

System Technical Details: (If applicable please provide)

System Function (e.g., DNS/web server, workstation, etc.)	
Operating System(s), including version, patches, etc.	
Antivirus software installed: (Specify version and latest updates)	
Source IP	
Source port	
Source protocol	
Destination IP	
Destination port	
Destination protocol	

How many systems are impacted by this incident?

Was customer/employee sensitive data involved in the incident?

Was the data involved in this incident encrypted?

-

Was critical infrastructure impacted by this incident?

-

What was the primary method used to identify the incident?

- ☐ End User or HelpDesk
- ☐ Network/System Administrators
- ☐ AntiSpyware/ AntiVirus Software Log Review
- ☐ IDS/IPS Log Reviews
- ☐ Network Device Detection
- ☐ 3rd Party
- ☐ Other:

What is the Incident Category Type (e.g., CAT 1, CAT 2, etc., see table)

-

Incident Category Type

Type	Name	Description
CAT 0	Exercise/Network Defense Testing	This category is used during approved activity testing of internal/external network defenses or responses.
CAT 1	Unauthorized Access	In this category an individual gains logical or physical access without permission to a network, system, application, data, or other resource
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
CAT 3	Lost or Stolen Asset	An asset such as a laptop, Phone/PDA, desktop, tape, disk, etc is stolen or lost.
CAT 4	Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.
CAT 5	Improper Usage	A person violates acceptable computing use policies.
CAT 6	Scans/Probes/Attempted Access	This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.
CAT 7	Investigation	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.