

Incident Identification and Validation

(To be filled by first responder while validating incident)

General Information

Incident Detector's Information:

Name: _____ Date and Time Detected: _____

Title: _____

Phone: _____ Alt. Phone: _____ Mobile: _____

Fax: _____ Alt. Fax: _____ Email: _____

Address: _____ Location(s) Incident Detected From: _____

Additional Information: _____

Detector's Signature: _____ Date Signed: _____

Incident Summary

Type of Incident Detected:

- Denial of Service
- Unauthorized Use
- Espionage
- Probe
- Hoax
- Malicious Code
- Unauthorized Access
- Others: _____

Incident Priority

☐ Critical ☐ High ☐ Medium ☐ Low

Incident Location:

Site: _____

How was the Incident Detected: _____

Site Point of Contact: _____

Phone: _____ Alt. Phone: _____

Mobile: _____ Pager: _____

Fax: _____ Alt. Fax: _____

E-mail: _____

Address: _____

Describe the affected information system(s) (one form per system is recommended):

Hardware Manufacturer: _____

Serial Number: _____

Corporate Property Number (if applicable): _____

Is the affected system connected to a network? • YES • NO

System Name: _____

System Network Address: _____

MAC Address: _____

Is the affected system connected to a router? • YES • NO

Router IP Address: _____

Hardware Manufacturer: _____

Serial Number: _____

Describe the physical security of the location of affected information systems (locks, security alarms, building access, etc.):

Describe the incident validation procedure employed (log analysis/event correlation/network and system profiling):

Is the incident a false-positive? • YES • NO

Additional Information about the incident:

Is the affected system ON or OFF? • ON • OFF

Additional Information obtained from the screen (If it is ON):

Is any external device is connected to the affected system? • YES • NO

Additional Information about the external device (such as USB drive or external HDD):

What are the data sources of the reported incident?

Provide details of the trusted data sources, devices, and people responsible for proper resolution.

Describe the acknowledgement message for the incident reporter (provide additional details of the next steps for incident report):

REPORTING STAFF SIGNATURE: _____

DATE: _____