INFORMATION SECURITY INCIDENT REPORTING FORM

CONTACT INFORMATION

1.	What organization experienced the incident? State Agency, County, Local Municipality, Organization, Private Company, etc.?

2.	Your name, organization, address, email address and phone number? Who is the point of contact at the affected entity?

INCIDENT DETAIL

3.	What date and time did the cyber event occur?

4.	How long has this been occurring (include approximate start time)?

5.	When did you first notice the incident?

6.	What was the primary method used to identify, detect or discover the incident?

7.	What has been impacted by this incident?

8.	How many sites, users and computing devices (computers, systems, cellphones, tablets, etc.) are impacted?

9.	Does the user who experienced the incident have privilege or administrator rights? Job responsibility?

10.	Is this incident related to any incidents that occurred in the past?

11.	Is the affected entity requesting State or Federal assistance?

12.	Who else has been made aware of the incident?

13.	Provide information about the affected system, include primary purpose.

14.	Are you aware of any compromise or disclosure (personnel records, social security #'s, confidential information, etc.)?

15.	Do you have access to the system logs? Do you see a pattern in regards to time, and network traffic?
16.	Brief description the Event/Incident.
17.	What is the current status or resolution?

Technical Detail

18.	What security software is installed?
19.	If known, provide the affected system's IP address in dotted decimal format (e.g. 192.168.1.1).
20.	If known, any TCP or UDP ports involved in the incident.
21.	What is the operating system of the affected system?
22.	If known, provide the attacker's IP address in dotted decimal format (e.g. 192.168.1.1).

Computing Device Detail (only)

23.	Who has possession of the device? Is it shared?
24.	What does the device access (applications or systems?)
25.	Is the device password protected and encrypted? Does it connect to an organization's network?