

## SECURITY INCIDENT REPORT FORM

THIS FORM MUST BE COMPLETED WITHIN 24 HOURS OF DETECTING A SECURITY INCIDENT. (The affected individual is responsible for gathering pertinent information and completing this form.)

### I. GENERAL INFORMATION [Section I, must be completed entirely]

Primary Contact: \_\_\_\_\_  
E-Mail Address: \_\_\_\_\_  
Telephone number: \_\_\_\_\_  
Cell Phone Number: \_\_\_\_\_ FAX number: \_\_\_\_\_  
Pager number: \_\_\_\_\_  
Physical Location of Incident: \_\_\_\_\_

### II. HOST INFORMATION [Section II, must be completed entirely]

Please provide information about all host(s) involved in the incident. Each host shall be listed separately.

Computer name: \_\_\_\_\_  
IP Addresses: \_\_\_\_\_  
Computer hardware: \_\_\_\_\_  
Operating System and version: \_\_\_\_\_  
Where on the network is the involved host? – (Home, Shared Lease space, Regional and Headquarters): \_\_\_\_\_  
Nature of the information at risk on the involved host – NAD Case Files, Personnel, Financial, Privacy Act.

Time zone of the involved host: \_\_\_\_\_  
Was the host the source or victim of the attack or both:  
\_\_\_\_\_  
Was this host compromised as a result of the attack? ☐ Yes ☐ No  
Hours system down \_\_\_\_\_

### III. INCIDENT CATEGORIES

All categories applicable to the incident shall be documented.

Data Loss(es): \_\_\_\_\_

Hardware Loss(es): \_\_\_\_\_

Intruder gained “access” ☐ Yes ☐ No

Cracked password ☐Yes ☐No  
Easily-guessable password ☐Yes ☐No  
Misuse of host(s) resources ☐Yes ☐No

#### IV. SECURITY TOOLS

At the time of the Incident, was the individual using any of the following? ☐Yes ☐No

Authentication/Password tools:

Anti-Virus tools:

Other tools: data encryption, hardware encryption(s)

Were logs being maintained: If so, please describe.

#### V. DETAILED INCIDENT DESCRIPTION

Detailed Incident Description: This should be as detailed as possible, especially when writing lesson learned or after the incident follow-up report. Please use separate sheets of paper to address the following:

A. Duration of Incident:

B. How was the incident discovered?

C. Method(s) used by intruders to gain access to host(s):

D. Detailed discussion of vulnerabilities exploited that are not addressed in previous sections:

E. Hidden files/directories:

G. Did system contain classified/sensitive information? What type?

H. Was the information compromised?

---