VITA's Guidance on reporting incidents

The purpose of this section is to provide information that may be helpful in incident reporting. Incidents will happen and the ability to quickly identify and act in a coordinated manner can lessen the impact of an incident. The incident reporting form is an important first step in handling incidents in a coordinated response.

Definitions

Incident:

Incident refers to an adverse event in an information system, network, and/or workstation, or the threat of the occurrence of such an event

Event:

An event is *any* observable occurrence in a system, network, and/or workstation. Although natural disasters and other non-security related disasters (power outages) are also called events, these reporting requirements are for IS security related events only. Events can many times indicate an incident is happening.

What to Report

An "information security incident" should be reported if:

1. it was intentional and successful AND
2. it resulted in either:

a. exposure of legally protected data in Commonwealth databases, such as financial information protected by GLBA, health information protected by HIPAA;

OR

b. major disruption to normal agency activities carried out via Commonwealth data communications, such as network unavailability for all or significant portions of an agency due to a denial of service (DOS) attack.

You should report events that have a real impact on your organization. A security incident includes, but is not limited to the following events regardless of platform or computer environment:

When damage is done	Access is achieved by the intruder

Loss occurs	Web pages are defaced
Malicious code is implanted	When you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks).
Evidence of tampering with data	Denial of service attack on the agency
Other incidents that could undermine confidence and trust in the Commonwealth's information technology systems	Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources)
Threat or harassment via electronic medium (internal or external)	Virus attacks which adversely affect servers or multiple workstations

Do not report routine probes, port scans, or other common events.

<u>Clues for determining a security incident</u>

The following are clues that a security incident may be in progress, or one may have already occurred. These indicators can have legitimate explanations and be part of day-to-day operations. The key in determining whether a suspected event is a legitimate event or is actually a security incident is recognizing when things happen without an explanation, events that are contrary to your policies and procedures. The *key* word to using these indicators is "***UNEXPLAINED***."

1. Unsuccessful logon attempts
2. Accounting/system/network logs discrepancies that are suspicious *(e.g., gaps/erasures in the accounting log in which no entries whatsoever appear; user obtains root access without going through the normal sequence necessary to obtain this access)*
3. "Door knob rattling" *(e.g., use of attack scanners, remote requests for information about systems and/or users, or social engineering attempts)*
4. New user accounts not created by system administrators
5. New files or unfamiliar file names
6. Modifications to file lengths or dates *(especially in system executable files)*
7. Attempts to write to system files or changes in system files
8. Modification or deletion of data
9. Changes in file permissions
10. Logins into dormant accounts (*one of the best SINGLE indicators)*
11. A system alarm or similar indication from an intrusion detection tool

12. Denial of Service (DoS) (DDoS) (*e.g. inability of one or more users to login to an account; inability of customers to obtain information or services via system)*
13. System crashes
14. Abnormally slow or poor system performance
15. Unauthorized operation of a program or sniffer device to capture network traffic *(e.g., presence of cracking utilities)*
16. Unusual time of usage *(remember, more security incidents occur during non-working hours than any other time)*
17. Unusual usage patterns *(e.g., programs are being compiled in the account of a user who does not know how to program; use of commands/functions not normally associated with user's job)*
18. Physical theft and intrusion *(e.g., theft of laptop computer with critical information)*

Adverse Events Categories: *(*Note: These are not necessarily mutually exclusive*.)*

1. *Malicious Code Attacks.*

Attacks by programs typically written to masquerade presence and often difficult to detect. Include:

a. Viruses
b. Trojan horse programs
c. Worms
d. Scripts used by crackers/hackers to gain privileges, capture passwords, and/or modify audit logs.

2. *Unauthorized Access.*

Large range of incidents, including:

a. unauthorized person logging into a legitimate user's account
b. unauthorized access to files and directories (by capturing superuser privileges)
c. a sniffer program to capture packets

3. *Unauthorized Use.*

Access to a user's account to perpetrate an attack is not absolutely necessary. Unauthorized use includes:

a. using the network file system (NFS) to mount the file system of a remote server machine
b. using the VMS file access listener to transfer files without authorization
c. using inter-domain access mechanisms in Windows NT to access files and directories in another organization's domain

4. *Disruptions or Denial of Service.*

Disruptions to network and computing services. Include:

a. erasing a critical program
b. spamming (flooding accounts with email)
c. altering system functionality (installing a Trojan horse)

5. *Misuse.*

Misuse can be intentional or unintentional. Misuse incidents and response are based on agency risk assessment and defined by agency policy. Include:

a. use of a computing system for other than official purposes
b. changes made to system hardware, firmware, or software characteristics without the agency's knowledge, instruction, or consent.

Please contact Deb Robertson or Shannon O'Neill if you suspect a security incident has happened.

See Computer Incident Report Form below

Download and use this form to report security incidents. If additional information is required, please attach a word document.

Computer Incident Reporting Form

Use this form to report security incidents. If additional information is required, please attach a word document.

STATUS		
☐ Site Under Attack	☐ Past Incident	☐ Repeated Incidents, unresolved
CONTACT INFORMATION		
Name/Last First: MI: Title:		
Organization		
Email		
Phone:	Fax:	
Location/Site(s) Involved		
Street Address Involved		
City: State: Zip:		
INCIDENT DESCRIPTION		
☐	Denial of Service	
☐	Unauthorized Access (e.g. Intrusion/Hack)	
☐	Website Defacement	
☐	Malicious Code (e.g. virus/worm or trojan)	
☐	Threat/Harassment via electronic medium (includes employees)	
☐	Misuse of Systems (internal or external, includes inappropriate use by employees)	
☐	Other (specify):	
DATE/TIME OF INCIDENT DISCOVERY		
Date	Time	
Duration of Incident:		
How did you detect this?		
Has the incident been resolved? Explain.		
WHO ELSE HAS BEEN NOTIFIED (Check all that apply)?		
☐ System Administrator	☐ Department Director	
☐ General Counsel	☐ Law Enforcement (who & when):	
☐ Human Resources	☐ Other (specify)	
IMPACT OF INCIDENT		
☐	Loss/Compromise of Data	
☐	System Downtime	
☐	Damage to Systems	
☐	Other Organizations' Systems Affected	
☐	Damage to the Integrity or Delivery of Critical Goods, Services or Information	
☐	Financial Loss (estimate amount $)	
SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS OR INFRASTRUCTURE		
☐ High (e.g. defaced websites)	☐ Medium (e.g. Trojan detected)	☐ Low (e.g. Small virus outbreak) ☐ Unknown
SENSITIVITY OF DATA		
☐ High (e.g Privacy Act violation)	☐Medium (e.g. local administration)	☐ Low (e.g. Public materials) ☐ Unknown
IDENTIFY THE COMPUTER OPERATING SYSTEM AND ANY OTHER SOFTWARE INVOLVED (Check all that apply.)		
☐Unix	☐ OS2	☐ Linux ☐ VAX/VMS
☐Microsoft XP/2000/NT/95/98	☐ Novell	☐ Sun OS/Solaris
☐ Other Software (specify)		
WHAT STEPS HAVE YOU TAKEN TO RESPOND (Check all that apply)?		
☐ No Action Taken	☐ System disconnected from network	
☐ Restored data from backup	☐ Updated virus definitions & scanned hard drive	
☐ Physically secured computer	☐ Log files examined (saved and secured)	
☐ Other Software (specify)		