
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *Incident Handling*

Guidance on Reporting Incidents

Legislative Directive

Beginning January 1, 2005, all executive branch agencies are required to begin reporting security incidents to VITA. The Code of Virginia [§ 2.2-603.G](#), listed below, describes the reporting requirements agency's must follow.

§ 2.2-603. Authority of agency directors.

G. (Effective January 1, 2005) The director of every department in the executive branch of state government shall report to the Chief Information Officer as described in § 2.2-2005, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence.

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

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *Incident Handling*

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
- Loss occurs
- Malicious code is implanted
- Evidence of tampering with data
- Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources)
- Threat or harassment via electronic medium (internal or external)
- Access is achieved by the intruder
- Web pages are defaced

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

Threat Management: *Incident Handling*

- When you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks).
- Denial of service attack on the agency
- Virus attacks which adversely affect servers or multiple workstations
- Other incidents that could undermine confidence and trust in the Commonwealth's information technology systems

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

Clues for determining a security incident

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 rattlin" (*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*)

**SOUTHSIDE VIRGINIA COMMUNITY COLLEGE
INFORMATION TECHNOLOGY
SECURITY PLAN**

Threat Management: *Incident Handling*

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*)

Virginia Information Technologies Agency
© Commonwealth of Virginia 2007