**Information Security Incident Reporting Procedure Template**

# PURPOSE

To document the reporting procedure for potential information technology (IT) security incidents that threaten the “YOUR AGENCY NAME” IT systems and services.

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners).

# ACRONYMS

CIO: Chief Information Officer

CIRT: Computer Incident Response Team

CSIRT: Computer Security Incident Response Team

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

SEC501: Information Security Standard 501

VCCC: VITA Customer Care Center

URL: Universal Resource Locator

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

[See COV ITRM Glossary](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/EA_PSG_update_011510/ITRMGlossary_011510.pdf)

# BACKGROUND

The Information Security Incident Reporting Procedure at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the IT Incident Response requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibilities as described in the Statement of Policy section. The following Roles and Responsibility Matrix describe 4 activities:

1. Responsible (R) – Person working on activity
2. Accountable (A) – Person with decision authority and one who delegates the work
3. Consulted (C) – Key stakeholder or subject matter expert who should be included in decision or work activity
4. Informed (I) – Person who needs to know of decision or action

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Roles** | CIRT | Information Security Officer | Employee | VCC |
| **Tasks** |  |  |  |  |
| Reporting an it security event |  |  | A | I |
| IT security incident response | A | I |  |  |

# STATEMENT OF PROCEDURE

1. **DEFINITIONS**
   1. IT Security Event: Any observable threatening occurrence to a system, service, network and/or device. Although natural disasters and other non-security related disasters (power outages) are also called events, these reporting requirements are for IT Security events only. Events can many times indicate an IT Security incident is occurring.
   2. IT Security Incident: An IT Security event that has an adverse effect on an IT system, service, network, and/or device, or the threat of the occurrence of such an event. The event could be either intentional or accidental in nature and must pose a threat to the integrity, availability, or confidentiality of an IT system.
2. **REPORTING OF AN IT SECURITY EVENT**
   1. Any suspected IT Security event shall be reported immediately to the “YOUR AGENCY NAME” Customer Care Center (VCCC) or to Commonwealth Security and Risk Management (***see Attachment A and C for guidance***). A suspected IT Security event includes, but is not limited to:
      1. A virus/worm affecting multiple systems; and
      2. Intrusion or damage to (a):
         1. Web site or page;
         2. Computer system or network;
         3. Wireless access;
         4. Cell phones;
         5. Personal digital assistants;
         6. Laptops;
         7. Fax machines;
         8. Voice mail; and
         9. Voice systems.

In the case of a Website intrusion, or any other IT security event originating from a specific Uniform Resource Locator (URL), the suspect URL(s) must be provided to the VCCC.

1. **IT Security Incident Response**
   1. The VCCC will immediately report the IT Security Incident to the VITA Computer Incident Response Team (CIRT).
   2. The CIRT will activate the IT Security Incident Response Procedure.
   3. The CIRT will manage the support staff, which will continue to provide needed assistance to the CIRT for the duration of the incident.
   4. Once the CIRT has verified the incident, the CIRT will determine the appropriate information regarding the incident and the parties to whom this information should be communicated.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” IT Incident Response Policy

“YOUR AGENCY NAME” CUST Customer Service Alert Reporting and Notification Policy & Procedure

“YOUR AGENCY NAME” Information Incident Reporting Procedure

**AUTHORITY**

**REFERENCE** [*Code of Virginia, §2.2-2005 et seq.*](http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-2005)

(Powers and duties of the Chief Information Officer “CIO” ““YOUR AGENCY NAME””)

*Code of Virginia, §2.2-2009, et seq.*

(Additional duties of the CIO relating to security of government databases)

**OTHER**

**REFERENCE** [ITRM Information Security Policy (SEC519)](http://www.vita.virginia.gov/uploadedFiles/Library/PSGs/Security_Policy_519_00_Final_0709.pdf)

[ITRM Information Security Standard (SEC501)](http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Information_Security_Standard_SEC501_06_07012011.pdf)

# ATTACHMENTS

(A) Guidance on Reporting Information Security Incidents

(B) Information Security Incident Reporting Form

(C) Reporting IT Security Incidents by a Secure Webpage and via Telephone

| Version History | | |
| --- | --- | --- |
| Version | Date | Change Summary |
| 1 | 01/13/2004 | Original document titled *Computer Security Incident Notification and Handling Procedure*. |
| 2 | 11/15/2005 | Changed name of document. Definitions added. Material and substantive changes expanded and clarified the Statement of Procedure. |
| 3 | 09/28/2007 | Update policy to align with revised *IT Security Policy* (ITRM SEC500-02) and *IT Security* *Standard* (ITRM SEC501-01) resulted material; changes to Statement of Procedure and Attachments A & C. |
| 3.1 | 09/27/2010 | Administrative changes. |
| 3.2 | 10/29/2010 | Administrative changes. |
| 4 | 07/01/2014 | Formatting changes and role matrix added. |
| 5 | 11/12/2021 | Formatting changes |

### Attachment A

**Guidance on Reporting Information Security 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**

|  |  |
| --- | --- |
| **IT Security Incident:**  IT Security Incident refers to an adverse event in an information system, network, and/or device, or the threat of the occurrence of such an event. | **IT Security Event:**  An event is *any* observable occurrence in an IT system, network, and/or device. Although natural disasters and other non-security related disasters (power outages) are also called events, these reporting requirements are for IT security related events only. IT Security events can indicate that an IT Security incident is occurring. |

**What to Report**

An IT security incident should be reported if it resulted in either:

* + Exposure of legally protected data in Commonwealth databases, such as financial information protected by GLBA, health information protected by HIPAA.  
      
    AND/OR
  + 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. An IT security incident includes, but is not limited to the following events regardless of platform or computer environment:

1. When damage is done
2. Loss occurs
3. Malicious code is implanted
4. Evidence of tampering with data
5. Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources)
6. Threat or harassment via electronic medium (internal or external)
7. Access is achieved by the intruder
8. Web pages are defaced
9. When you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks)
10. Denial of service attack on the agency
11. Virus attacks which adversely affect servers or multiple workstations
12. Other information technology security 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 an IT Security Incident**

The following are clues that an IT 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 IT Security Event is a legitimate event or may be part of an IT 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*)

### Attachment B

**Information SECURITY INCIDENT REPORTING FORM**

**Use this form to report security incidents to the Chief Information Officer of the Commonwealth. If additional information is required, you will be contacted via phone or email. To assist with our initial assessment and investigation, please provide as much information as possible.**

**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/Data Owner  Human Resources

General Counsel  Law Enforcement (who & when) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Other (Please Specify) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**IMPACT OF INCIDENT**

Loss/Compromise of Data  System Downtime

Damage to Systems  Other Organizations’ Systems Affected

Financial Loss (estimated amount: $\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Damage to the Integrity or Delivery of Critical Goods, Services or Information

**SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS OR INFRASTRUCTURE**

High (defaced websites)  Medium (Trojan detected)  Low (Small virus outbreak)

Unknown

**SENSITIVITY OF DATA**

High (Privacy Act violation)  Medium (local administration)  Low (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

Log files examined (saved and secured)  Physically secured computer

Other (specify) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Attachment C

**Reporting IT Security Incidents via a secured webpage**

Reporting IT Security Incidents via the secured webpage is the preferred method for agencies to utilize when reporting an IT Security Incident to the Virginia Information Technologies Agency (VITA). Agencies can access the web based incident form on VITA’s Web Site ([www.vita.virginia.gov](http://www.vita.virginia.gov)) by clicking on the “[Information Technology Security Incident Reporting](http://www.vita.virginia.gov/security/default.aspx?id=317)” link. This form may be filled out online and then submitted by clicking the “Submit” button at the end of the form. The form will then be transmitted to “YOUR AGENCY NAME” Commonwealth Security and Risk Management.

**Reporting Incidents via telephone**

Agencies may also utilize reporting security incidents via the telephone. When submitting a report via telephone, agencies may contact the VITA Customer Care Center (VCCC) by dialing toll free **1-866-637-8482**. An operator will take down the caller’s contact information so that a member of VITA Security Services can contact them regarding the details of the incident.