Information Security Incident Response Procedure

PURPOSE
To document the response procedure for potential information technology (IT) security incidents that threatens the VITAIT systems and services.

SCOPE
All VITA employees (classified, hourly, or business partners).

ACRONYMS
CIO:	Chief Information Officer
CIRT:	Computer 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
SEC530:	Information Security Standard 530
VITA:	Virginia Information Technologies Agency

DEFINITIONS
See COV ITRM Glossary

BACKGROUND
The Information Security Incident Response Procedure at VITA 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 SEC530 and security best practices.

ROLES & RESPONSIBILITY
This section will provide a 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	Agency Contacts
Tasks			
COORDINATE ALL ASPECTS OF THE INCIDENT HANDLING PROCESS	A	R	R

STATEMENT OF PROCEDURE

The CIRT (Computer Incident Response Team) will act as the incident coordinator for all reported IT security incidents. The incident coordinator, under the direction of the ISO, and with the assistance of the affected agency contacts, will be responsible for coordinating all aspects of the incident handling process and the incident response process. All persons involved in the incident response and clean-up are responsible for providing all requested information to the incident coordinator. VITA and contracted staff must coordinate with the CIRT prior to initiating any actions during the investigation or in response to information security incidents. All communications regarding IT security incidents must be conducted through channels that are known to be unaffected by the IT security incident under investigation.

A. COMPUTER INCIDENT RESPONSE TEAM

1. The CIRT consists of:

    a. The Information Security Officer (ISO); and

    b. The VITA Commonwealth Security and Risk Management (CSRM) Incident Management (IM) staff.

B. INCIDENT HANDLING PROCESS

1. An incident report is received by the CIRT via the (ISO) or the Incident Reporting System.

2. The CIRT reviews each incident report to confirm a security incident has occurred.

    a. If a confirmed incident, the appropriate parties will be contacted as stipulated in the VITA Information Security Incident Reporting Procedure.

b. If not a confirmed incident, the information is passed on to the appropriate parties for resolution.

3. The CIRT, agency management and the (ISO) will determine if the incident requires immediate response**.**

    a. If so, the CIRT will activate and begin to coordinate response activities.

    b. If not, the agency management and (ISO) will coordinate appropriate response activities.

4. The CIRT, agency management and the (ISO) will determine if the incident will require an investigation.

    a. If so, investigative efforts are initiated.

    b. If not, recovery efforts are initiated.

5. In cases where multiple incidents are occurring simultaneously, the CIRT will classify the incidents according to their immediate and potential adverse effects and prioritize recovery and investigation activities according to these effects.

6. Initiation of Recovery and Investigation.

    a. Attachment A, Initial Response Checklist, provides a response checklist for CIRT members to log initial details and activity.

    b. All pertinent live forensic data should be recovered from the system before disconnection from network or powering down.

    c. Attachment B, Windows Forensic Checklist, details steps for Windows based platforms.

    d. Attachment C, Unix Forensic Command Log sheet, provides a form for CIRT members to log commands used on UNIX based platforms. Due to the variety of commands necessary on UNIX based platforms, specific commands are not provided.

    e. Additional network traces performed with open standards based network packet capture tools may also be required.

7. Preservation of evidence if an investigation is required.

    a. In cases of investigations where physical evidence is collected from the scene, CIRT members will fill out a Description of Evidence Form (Attachment D).

    b. In cases where criminal charges may be an outcome, CIRT members will also use a Chain of Custody Form (Attachment E).

    c. CIRT members are to make forensic drive images of incident related hardware and store the originals in clearly marked containers in a locked area. All forensic drive images should be recorded in an open standard format (dd based)

to allow the use of the widest variety of forensic tools. Proprietary image formats such as those generated by the EnCase tool set should not be used.

8. Identification of Problem.

    a. CIRT members should identify the root cause of the incident and the most likely vectors of attack. If recoverable malicious binaries can be removed from the system(s), they should be put on safe media and forwarded to the appropriate anti-virus vendor contacts.

9. Containment and Recovery.

    a. CIRT members will take appropriate immediate actions to contain and control the incident. This may require removal of infected machines or entire network segments from the larger agency network. It may also require blocking agency networks from access to the Internet or other Commonwealth resources. CIRT members should also develop an action plan for recovery of systems harmed in an incident with assistance from agency management and the (ISO) to be carried out by appropriate VITA and contracted staff. All staff will cooperate with the directives of the CIRT in a timely manner to minimize exposure time and vulnerability.

10. Restoration of Functionality.

    a. After an incident has been contained and all affected systems have returned to normal operations mode, the CIRT will finish the incident response by verification of proper systems behavior.

11. Follow-up analysis.

    a. Once an incident has been resolved and all systems are restored to a normal mode of operation, a follow-up postmortem analysis will be performed. All involved VITA and agency parties will meet and discuss actions taken and the lessons learned. Pertinent procedures should be evaluated and modified, if necessary. If applicable, a set of recommendations should be presented to the appropriate management levels.

ASSOCIATED PROCEDURE

VITAIT Incident Response Policy
VITA CUST Customer Service Alert Reporting and Notification Policy & Procedure
VITA Information Incident Reporting Procedure

AUTHORITY REFERENCE

Code of Virginia, §2.2-2005 et seq.
(Powers and duties of the Chief Information Officer "CIO" ""YOUR AGENCY"")

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)

ITRM Information Security Standard (SEC530)

ATTACHMENTS

(A) Initial Response Checklist.doc
(B) Windows Forensic Checklist.doc
(C) Unix Forensic Command Log sheet.doc
(D) Description of Evidence Form.doc
(E) Chain of Custody Form.doc

Version History ***This document will be reviewed and updated on an annual basis or more frequently as needed.***		
Version	Date	Change Summary
1	01/13/2004	Original Document
2	11/15/2005	Minor modifications to procedure and attachments
3	06/18/2007	Major rewriting and restructuring of procedure and attachments to include the roles and responsibilities of the CIRT and the CISIAO
4	10/01/2007	Minor modifications to improve alignment with COV ITRM SEC501-01 and to make parallel with other CSRM Policies and Procedures.
5	02/01/2013	Administrative Changes
6	07/01/2014	Formatting changes and role matrix added.
7	09/18/2020	Administrative change: Changed font
8	07/08/2022	Annual review and update
9	10/01/2024	Updated language to reflect SEC530 which superseded SEC501.

ATTACHMENT A
Initial Response Checklist

Incident #: _____ Date: _____

Contact Information

Your Contact Information

Name:	
Department:	
Telephone:	
Other Telephone:	
Email:	

Individual Reporting Incident

Name:	
Department:	
Telephone:	
Other Telephone:	
Email:	

Incident Detection

Type of Incident:	☐ Denial of Service ☐ Unauthorized Access ☐ Virus ☐ Unauthorized Use of Resources ☐ Hoax ☐ Theft of Intellectual Property ☐ Other:_____ _____ _____ _____
Location of Incident:	Address: Building: Room Number:

Describe the Physical Security at the Site: 1. Are there locks? 2. Alarm systems? 3. Who is charge of Physical Security at the site?	
How the incident was detected:	
Is the information concerning the incident stored in a protected, tamper-proof manner?	

System Details

System Information:	
Make/Model of System:	
Operating System:	
Primary System User:	
System Admin:	
IP Address:	
Network Name:	
Modem Connection(Y/N)	
What Critical Information is contained on the system:	

Incident Containment

Is the incident still in progress or ongoing?	
Are you performing network Surveillance?	
Is the system still connected on network? If so, why is it still online? If not, who authorized removal? When will it be placed back online?	

Incident #:_____ Date:_____

Are there backups of the system?	
Who has accessed/ touched system(s) affected since the onset of the incident?	
Who has had physical access to the system since the incident?	
Who currently knows about the incident?	
Is there a need to keep knowledge of the incident on a "need to know" basis?	

Have network devices (routers, firewalls) been configured to provide additional defense against the incident?	

Preliminary Investigation

What is the Source IP of the attack?	
What investigative actions have been taken?	
Does a forensic dupe need to be made?	
Does a logical backup need to be made?	
Who needs to be contacted?	

Incident #:_____ Date:_____

Comments:

ATTACHMENT B
Windows Forensics Checklist

Incident #: _____ Date: _____
Investigator_____

1. Execute trusted cmd.exe _____

2. Record system time and date _____
   date > date.txt
   time >> date.txt

3. Determine logged on users _____
   psloggedon

4. Record MCA times of all files _____
   dir /t:a /a /s /o:d c:\

5. Record open ports _____
   netstat –an

6. Associate Applications with open ports _____
   fport

7. Grab process listing _____
   pslist

8. List current and recent connections _____
   netstat, arp, nbtstat

9. Record system time and data again _____

10. Document commands used during initial response _____
    doskey /history

Comments:
_____
_____
_____
_____
_____
_____

ATTACHMENT C
Unix Forensic Command Log

Start Time	Command Line	Trusted	Un	MD5 Sum	Comments

ATTACHMENT D
Description of Evidence Form

Case Information

Date:

Case:

Location:

CPU Information

Make/Model:

Memory:

Serial Number:

Processor:

Asset Tag Number:

Remarks:

Hard Drives/Removable Media

Drive 0:

Type:

Serial Number:

Capacity:

Remarks:

Drive 1:

Type:

Serial Number:

Capacity:

Remarks:

Drive 2:

Type:

Serial Number:

Capacity:

Remarks:

Drive 3:

Type:

Serial Number:

Capacity:

Remarks:

Additional Notes

ATTACHMENT E
Chain of Custody Form

Date: Case Number:

Consent Required: Y N Signature of Consenting Person:

Tag Number:

Description:

Person Receiving Evidence: Signature:

From:	Date:	Reason:	To:
From:	Date:	Reason:	To:
From:	Date:	Reason:	To: