U.S. DEPARTMENT OF VETERANS AFFAIRS



VAEC AWS GovCloud - High

VISTA ADAPTIVE MAINTENANCE VAEC (VAM)

Incident Response Plan

Version 1.0

04/03/2019

SYSTEM SECURITY ARTIFACT  
ASSESSMENT AND AUTHORIZATION

**We, the undersigned, approve the content of this Incident Response Plan for the VA Enterprise Cloud AWS GovCloud High (VAEC) located in AWS GovCloud’s two Availability Zones within their Region.**

*A valid PKI can be used to sign in lieu of a handwritten signature.*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Signature Date**

**Christopher Brown**

**System Owner**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Signature Date**

**Bobbie Begay**

**Information Security Officer**

[Organization 2 name/acronym] signatory authorities

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Plan Approver Name>

<Job Title>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Plan Approver Name>

<Job Title>

**Record of Changes/Revisions**

This record shall be maintained throughout the life of the document. Each published update shall be recorded. Revisions are a complete re-issue of the entire document. Increment the version number’s decimal (minor) portion here, on the cover page, and in the headers for each revision. The version number’s integer (major) portion will be updated at each time a full Authorization and Accreditation (A&A) is performed.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Date** | **Version** | **Pages Affected** | **Description** | **Author** |
| 6/30/2017 | 1.0 | All | Initial Draft | Peter Davies, CSRA/MPG |
| 11/14/2017 | 1.1 | All | Various updates | Daniel Beaver/ Wilbert Francis,  CSRA/MPG |
| 11/14/2017 | 1.2 | All | Review | Peter Davies,  CSRA/MPG |
| 10/11/2018 | 1.3 | All | Template Update & Review | IMC/Unisys |
| 04/03/2019 | 1.4 | All | General transition and updates from previous IRP | AbleVets/ David Faulkner |
|  |  |  |  |  |

Provide organization Author name and System Acronym in the document change control record table.

Entries in Green are instructions

Entries in RED are to be completed

Entries in BLACK are not to be changed, they are boiler plate

[Organization2] is the organization joining VAEC AWS

All colored texts are to be removed

[Organization2] is the organization joining VAEC AZURE

All colored texts are to be removed

Table of Contents

[1 PURPOSE 1](#_Toc527022237)

[2 POLICY AND AUTHORITY 2](#_Toc527022238)

[3 SYSTEM INFORMATION 3](#_Toc527022239)

[3.1 System Description 3](#_Toc527022240)

[3.1.1 System Name 3](#_Toc527022241)

[3.1.2 System Description 3](#_Toc527022242)

[3.1.3 System Categorization 4](#_Toc527022243)

[3.2 System Contacts 5](#_Toc527022244)

[3.2.1 System Owner 5](#_Toc527022245)

[3.2.2 System/Facility Chief Information Officer 5](#_Toc527022246)

[3.2.3 System/Facility Information Security Officer 5](#_Toc527022247)

[3.2.4 System/Facility Privacy Officer 5](#_Toc527022248)

[3.3 System Location 5](#_Toc527022249)

[4 SYSTEM INTERCONNECTIONS 7](#_Toc527022250)

[5 ROLES AND RESPONSIBILITIES 8](#_Toc527022251)

[5.1 System Owner 8](#_Toc527022252)

[5.2 Facility CIO 10](#_Toc527022253)

[5.3 Facility ISO 11](#_Toc527022254)

[5.4 Facility Privacy Officer 12](#_Toc527022255)

[6 SYSTEM SPECIFIC INCIDENT HANDLING PROCEDURES 14](#_Toc527022256)

[7. CONTACT INFORMATION 17](#_Toc527022257)

[8 REFERENCES 17](#_Toc527022258)

[8.1 Acronyms 17](#_Toc527022259)

[8.2 Definitions 18](#_Toc527022260)

[Appendix A – 800-53 CONTROL FAMILY Incident Response (IR) 19](#_Toc527022261)

[Appendix B – Incident Response and Management Resources 26](#_Toc527022262)

[Appendix C – Policy and Document References 29](#_Toc527022263)

# PURPOSE

An Incident Response Plan must be formulated for every information system (IS) at the U.S. Department of Veterans Affairs. The Incident Response Plan (IRP) is a required document that must be included in the Security Artifacts package. The purpose of an incident response plan is the establishment of procedures and protocol for the reporting and handling of information security incidents as required by the policies and laws of the U.S. Federal Government and the U.S. Department of Veterans Affairs.

The guidelines contained herein include fundamental information about responding to security incidents and provides a practical source of guidance and incident response. A structured, systematic incident response program will assist VA personnel to:

* Quick and efficient recovery through proven response measures
* Minimal loss or theft of information or disruption of critical computing services
* Systematic response by outlining the recommended response times
* Protection of IS and data through quick detection and recovery
* Protection of personnel through sound incident response practices
* Efficient use of resources through quick resolution of incidents

# POLICY AND AUTHORITY

This section shows the Federal laws, regulatory guidance, and directives that drive Department of Veterans Affairs Information Security Programs including the formation of an Incident Response Plan.

• Federal Information Security Management Act (FISMA) of 2002

• Health Insurance Portability and Accountability Act of 1996 (HIPAA)

• Computer Fraud and Abuse Act of 1986, as amended

• OMB Circular No. A 130, Appendix III “Security of Federal Automated Information Resources”

• Federal Information Processing Standard - 199 “Standards for Security Categorization of Federal Information and Information Systems” February 2004.

• Federal Information Processing Standard – 200 “Minimum Security Requirements for Federal Information and Information Systems” March 2006.

• NIST SP 800-12 - An Introduction to Computer Security: The NIST Handbook, Oct 1995

• NIST SP 800-18 Rev. 1 - Guide for Developing Security Plans for Federal Information Systems, February 2006

• NIST SP 800-37 Rev. 1 – Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Feb 2010

• NIST SP 800-53 Rev. 4 – Security and Privacy Controls for Federal Information Systems and Organizations, Apr 2013

• NIST SP 800-53A Rev. 4 - Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, Dec 2014

• NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide, Aug 2012

• VA Directive 6500, Managing Information Security Risk: VA Information Security Program

• VA Handbook 6500, Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program

• VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI)

• VA Handbook 6500.5, Incorporating Security and Privacy into the System Development Life Cycle

# SYSTEM INFORMATION

This section describes information defining and relating to the VAEC AWS GovCloud High and Vista Adaptative Maintenance VAEC (VAM)

## System Description

### System Name

System Name: VAEC AWS GovCloud High

System Acronym: VAEC

Unique Identifier: VAEC AWS GovCloud High

System Name: Vista Adaptative Maintenance VAEC (VAM)

System Acronym: VAM

Unique Identifier: 029-555555302

### System Description

The VA Enterprise Cloud AWS GovCloud High (VAEC) is a General Support System that provides a secure application and hosting environment for VA applications, content, and utilities that are used to deliver content and applications to an audience made up of employees, veterans, contractors, and partners across all VA medical centers and component facilities and the Federal government, veterans and the general public. Content and applications are provided by Veterans Benefits Administration (VBA), Veterans Health Administration (VHA), National Cemetery Administration (NCA) and Support Offices. VAEC provides the following services: Content delivery, Application Hosting and Management Services.

The VAEC infrastructure is hosted by AWS GovCloud, a cloud service provider. The AWS GovCloud platform is used to provide a variety of hosting environments to suit a variety of needs. AWS GovCloud can support applications categorized up to High as rated in accordance with Federal Information Processing Standard (FIPS) 199. VA applications available to the public are hosted in AWS GovCloud.

A dedicated private data link (AWS Direct Connect) provides all connectivity for VA resources communicating to the environment. Virtual Private Clouds (VPCs) wrap the applications within AWS GovCloud to encapsulate network access. Access from the applications to VA internal resources such as Identity, Credential, and Access Management (ICAM) and Active Directory (AD) Services are conducted over the encrypted private data link to the VA Network.

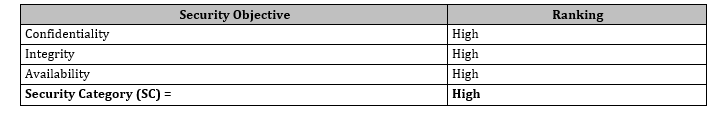
VAEC is located in one AWS GovCloud Region with two Availability Zones (AZs) designed to allow U.S. government agencies, contractors and customers to move sensitive workloads into the cloud for addressing specific regulatory and compliance requirements. AWS GovCloud does not manage logical access controls within the VAEC system boundary. VAEC offers the same level of security as other VA physical technology centers and supports existing VA security controls and certification requirements such as FISMA, HIPAA, HITECH, SAS-70, ISO 27001, FIPS 140-2 compliant end points, and PCI DSS.

**VistA Adaptive Maintenance – VA Enterprise Cloud (VAM VAEC)** Security provides a complete audit, analysis, and translation of the entire VistA RPC interface into a modern machine-processable form. VAM VAEC, is operational and scaled for the production enterprise’s use on the VAEC CloudWatch monitoring tool in order to provide a comprehensive cloud-based VistA RPC Interface monitoring and security for all VistA systems migrated to the VAEC.

As the VA continues to strengthen its cybersecurity profile, VAM provides a quadruple initiative of reducing the cost and complexity of maintenance for VistA systems by resolving severe security vulnerabilities within all VistA systems that migrated to VAEC, while taking full advantage of the features and scaling of VA’s new commercial cloud capabilities, and ensuring the safe, secure, and seamless continuity of veteran care and services as VistA systems are migrated to the VAEC.

### System Categorization

Overall categorization for VAM: HIGH



[Organization 2] System Categorization

[LOW/MEDIUM/HIGH]

System Categorization is derived in the System Security Plan. Indicate the overall system sensitivity level by using exact level calculated in the SSP.

## System Contacts

### System Owner

**Title:** System Owner

**Name:** Christopher Brown

**Email:** Christopher.brown1@va.gov

**Phone:** 202-270-1432

**Mobile:** XXX

### System/Facility Chief Information Officer

**Title:**

**Name:**

**Email:** @va.gov

**Phone:**

**Mobile:** XXX

### System/Facility Information Security Officer

**Title:** ISO

**Name:** Bobbi Begay

**Email:** bobbi.begay@va.gov

**Phone:** 303-331-7837

**Mobile:** XXX

### System/Facility Privacy Officer

**Title:**

**Name:**

**Email:** @va.gov

**Phone:**

**Mobile:** XXX

**Discussion:** Enter the name of the system/facility Privacy Officer as defined in the systems Security Plan (SSP).

## System Location

**3.3.1** **Geographical Location of the Physical System**

The VAEC AWS GovCloud High (VAEC) is located in one AWS GovCloud region with two Availability Zones. AWS does not disclose the physical address of its data centers.

**3.3.2** **Logical Location of the Management System**

The VAEC AWS GovCloud High (VAEC) is located in one AWS GovCloud region with two Availability Zones.

VAM is located in one AWS GovCloud region with two Availability Zones.

**3.3.3** **Location of System Backups**

The VAEC AWS GovCloud High (VAEC) is located in one AWS GovCloud region with two Availability Zones.

VAM is located in one VAEC AWS GovCloud High regions with two Availability Zones.

# SYSTEM INTERCONNECTIONS

The VAEC system is VA’s enterprise cloud-based provider for applications hosted in AWS clouds. The VAEC utilizes internal system interconnections with:

• VA AD Service: Identification, Authentication, and Authorization services for application servers and the cloud infrastructure

• VA NSOC: Auditing, Monitoring, and Incident Response

• VA NSOC: Trusted Internet Connection to the CSP.

• VA NSOC: Network termination and firewall management

### VAM is installed and only located in the VAEC environment

# ROLES AND RESPONSIBILITIES

## System Owner

Christopher Brown

1. **Incident Preparation:**
2. Make training available as is appropriate and necessary to the facility incident response personnel.
3. Ensure that all users of VA information and information systems under their responsibility take annual security awareness and privacy training.
4. Ensure that all users of VA information and information systems under their responsibility take ownership/responsibility for the data at their disposal.

The OI&T provides basic security awareness training to all users (including managers, senior executives, and contractors) of VA Information systems or VA information on an annual basis.

1. **Incident Prevention:** Adhere to VA configuration standards to ensure appropriate workstation and/or server setup by:
2. Hardware/software patch installation and maintenance
3. Anti-virus software and patch installation and maintenance
4. Appropriate configuration setup and maintenance
5. Ensure that users are aware of the reporting procedures and the policies in place to protect information systems, employees, and property.
6. Ensure regular review of user level permissions to network shares.
7. Ensure systems and subsystems affected by incidents are isolated as quickly as possible and, if necessary, are restored and/or rebuilt.

### This control is partially inherited from the VA NSOC. Additionally, Incident Response training is required for each new user as a component of the VA User Awareness Training. This training is done annually.

1. **Incident Detection:**
2. Implement enterprise tools in a timely fashion.
3. Provide consistent monitoring and automated alert implementation.

### **I**nherited from the VA NSOC.

1. **Incident Analysis**

Maintain pertinent information including, but not limited to, audit and event logs as well as user account information when appropriate.

### Inherited from the VA NSOC.

1. **Incident Documentation:**
2. Ensures staff provides updates to open incidents as directed.
3. Provide input as required in any documentation requested from top management, both inside and outside the facility
4. Safeguard data and sensitive information related to the incident
5. Ensure that access to the incident data is properly restricted.

### Inherited from the VA NSOC.

1. **Containment Strategy**

1. Coordinate and advice in the execution of the containment strategy and efforts at the regional and local levels.
2. Make decisions about containment actions.
3. Coordinate response actions until the incident are resolved.
4. Report to senior VA officials on the status of the incident.
5. Work with the OI&T staff to assure containment actions are performed in a timely and efficient manner.
6. Safeguard the integrity of involved hardware/software as appropriate.

### **I**nherited from the VA NSOC.

1. **Evidence Gathering and Management**
2. Preserve hardware/software as appropriate and requested.
3. Preserve audit and event logs as appropriate.

### **I**nherited from the VA NSOC.

1. **Corrective/Mitigation Action**
2. Balance mission needs with recommended risk mitigation.
3. Own the restoration plan.
4. Coordinate with Veterans Integrated Service Network (VISN) CIO, FCIO, Network ISOs, PO, and staff to implement eradication and remediation actions.
5. Assure response actions are carried out by Local IT Operations Staff
6. Implement recommendations as appropriate.

### **I**nherited from the VA NSOC.

1. **Lessons Learned**
2. Ensure facility incident response staff conducts a post mortem review of all documentation surrounding the incident/suspected incident.
3. Implement “best practices” as appropriate based on the review

### **I**nherited from the VA NSOC.

## Facility CIO

1. **Incident Preparation:**
2. Maintain current facility incident response contact information.
3. Make training available as is appropriate and necessary to the facility incident response personnel.
4. Ensure that all users of VA information and information systems under their responsibility take annual privacy training.
5. Work closely with the facility ISO to maintain continuity of service.
6. Ensure that all users of VA information and information systems under their responsibility take ownership/responsibility for the data at their disposal.

### Enter your organization incident preparation here.

**b. Incident Prevention:** Adhere to VA configuration standards to ensure appropriate workstation and/or server setup by:

1. Hardware/software patch installation and maintenance
2. Anti-virus software and patch installation and maintenance
3. Appropriate configuration setup and maintenance
4. Ensure the appropriate user awareness and training programs on privacy procedures are available.
5. Ensure that users are aware of the reporting procedures and the policies in place to protect information systems, employees, and property.
6. Conduct regular review of user level permissions to network shares.
7. Maintain a strong working relationship with the facility ISO and PO.
8. Ensure systems and subsystems affected by incidents are isolated as quickly as possible and, if necessary, are restored and/or rebuilt.

### Enter your organization incident prevention here.

**c. Incident Detection:**

1. Implement enterprise tools in a timely fashion.
2. Provide consistent monitoring and automated alert implementation.
3. Maintain a strong working relationship with staff to encourage reporting of incidents/suspected incidents.

### Enter your organization incident detection here.

**d. Incident Analysis**

Maintain pertinent information including, but not limited to, audit and event logs as well as user account information when appropriate.

### Enter your organization incident analysis here.

**e. Incident Documentation:**

1. Provide updates to open incidents as directed.
2. Provide input as required in any documentation requested from top management both inside and outside the facility.
3. Safeguard data and sensitive information related to the incident.
4. Ensure that access to incident data is properly restricted

### Enter your organization incident documentation here.

**f. Containment Strategy**

1. Coordinate and advice in the execution of the containment strategy and efforts at the regional and local levels.
2. Make decisions about containment actions.
3. Coordinate response actions until the incident are resolved.
4. Report to senior VA officials on the status of the incident.
5. Work with the OI&T staff to assure containment actions are performed in a timely and efficient manner.
6. Safeguard the integrity of involved hardware/software as appropriate.

### Enter your organization containment strategy here.

**g. Evidence Gathering and Management**

1. Preserve hardware/software as appropriate and requested.
2. Preserve audit and event logs as appropriate.

### Enter your organization evidence gathering and management here.

**h. Corrective/Mitigation Action**

1. Balance mission needs with recommended risk mitigation.
2. Own the restoration plan.
3. Coordinate with Network ISOs, PO, and staff to implement eradication and remediation actions.
4. Assure response actions are carried out by Local Area Network/Wide Area Network (LAN/WAN) managers.
5. Implement recommendations as appropriate.
6. Maintain a record of costs associated with repair, restoration, business disruption, and labor.

### Enter your organization corrective/mitigative action here.

**i. Lessons Learned**

1. Participate with the facility incident response staff in a post mortem review of all documentation surrounding the incident/suspected incident.
2. Implement “best practices” as appropriate based on the review.

### Enter your organization learned here.

## Facility ISO

Bobbi Begay

**a. Incident Preparation**

(1) Obtain and maintain PSETS user accounts and obtain training in Remedy and Risk Assessment.

(2) Complete appropriate privacy and security training.

(3) Be aware of the security laws, regulations, and policies that apply to the organization.

(4) ensure that individuals within the organization know who their ISOs are.

(5) Ensure that facility incident response personnel have appropriate incident response mechanisms, such as phone numbers, email addresses, and tools available to report suspected incidents.

(6) Be familiar with and establish a working relationship with the PO, FCIO, and OI&T staff for the organization.

(7) Ensure that an after-action report process is in place to look at root causes and future prevention mechanisms.

(8) Provide local organization policy and procedures for reporting and managing incidents.

### **I**nherited from the VA NSOC.

**b. Incident Prevention**

(1) Advise users on proper security protocols to prevent incidents.

(2) Provide training to staff on their roles in preventing, reporting, and managing security incidents.

(3) Ensure systems and subsystems affected by incidents are isolated as quickly as possible and, if necessary, are restored and/or rebuilt.

(4) Provide local organization policy and procedures for reporting and managing incidents.

(5) Verify that all users complete the VA Privacy and Security Awareness and Rules of Behavior (ROB) training annually.

(6) Verify that all users sign the VA National ROB annually.

### Inherited from the VA NSOC.

**c. Incident Detection**

(1) Initiate protective measures when an incident or vulnerability is discovered.

(2) Ensure that incidents are properly reported, responses are coordinated, and incident updates are provided as required.

(3) Coordinate with the PO to determine if a detected or reported security incident is also a privacy incident.

Inherited from the VA NSOC.

**d. Incident Analysis**

(1) Enter all reported incidents into the PSETS within one (1) hour of receiving or identifying an incident.

(2) Complete a risk evaluation at the time of reporting the incident and update information on each incident accordingly.

### Inherited from the VA NSOC.

**e. Incident Documentation**

(1) Enter incident updates in PSETS for any incident with a status of “Open”.

(2) Incidents should be reviewed and updated according to the rating assigned to the incident.

High Every 24 hours

Medium Every 48 hours

Low Every 72 hours

ISOs and POs will also receive an email alert from PSETS reminding them to provide an update. If the ticket is in “pending” status, then an update is required after one week.

1. Track the progress of response activity in PSETS, if the event is determined to be a breach, and performing all necessary documentation of incident progress

Inherited from the VA NSOC.

**f. Incident Notification**

Notify and keep local management and support staff apprised of the incident.

### Inherited from the VA NSOC.

**g. Containment Strategy**

(1) Participate in initiating containment actions.

(2) Suggest alternate containment actions, as necessary

.

Inherited from the VA NSOC.

**h. Evidence Gathering and Management**

(1) Execute direction provided by the Data Breach Response Service, VA NSOC, law enforcement, or the OIG.

(2) Consult with law enforcement or the OIG as necessary.

(3) Log all comments and details of their investigation into the PSETS or the system designated for the reporting of privacy complaints and incidents.

Inherited from the VA NSOC.

1. **Lessons Learned**

(1) Log resolution of incident.

(2) Raise user awareness through lessons learned

### Inherited from the VA NSOC.

## Facility Privacy Officer

Rita Grewal

[Organization 2 name/acronym] facility privacy officer.

### Enter your organization facility privacy officer full name here.

**a. Incident Preparation**

(1) Take appropriate privacy and security training.

(2) Obtain and maintain a PSETS account and develop familiarity with the system.

(3) Review VA Handbook 6502.1, Privacy Event Tracking.

(4) Review PSETS Basic User’s Handbook.

(5) Maintain awareness of the privacy laws, regulations, and policies that affect their organizations.

(6) Ensure that individuals within their organizations know who their POs are.

(7) Acquire template of Incident Notification/Credit Monitoring letter.

(8) Establish a working relationship with the ISO(s) for their organizations.

(9) Ensure that facility privacy personnel have appropriate incident response mechanisms, such as phone numbers, email addresses, and tools available to report suspected privacy incidents.

(10) Ensure an after-action report process in place to look at root causes and future prevention mechanisms.

### **I**nherited from the VA NSOC.

**b. Incident Prevention**

(1) Implement Departmental and appropriate Administration privacy policies and procedures.

(2) Establish an internal privacy audit or compliance monitoring and audit program.

(3) Monitor and report that individuals in their organizations complete the appropriate annual Privacy training(s).

(4) Ensure that privacy issues and concerns are communicated to and coordinated with appropriate parties.

(5) Be aware of the systems in their organizations that collect and/or maintain PHI and/or PII.

(6) Participate in the preparation and updating of Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA) for systems within the purview of their organizations.

(7) Understand what constitutes a Privacy Act system of records (SOR), and ensure that all PII that is retrieved by individuals’ names or other unique identifiers are maintained in an official SOR published in the Federal Register.

(8) Promote activities to foster privacy awareness (e.g., Privacy Day or Information Protection Awareness Week).

Inherited from the VA NSOC.

**c. Incident Detection**

(1) Receive complaints from Veterans or anyone within their organization who believes an incident has occurred.

(2) Enter all complaints received into the system allotted for the reporting of incidents within one (1) hour of discovery.

(3) Follow guidance provided by the VA Privacy Service in order to record all incidents in PSETS.

(4) Monitor all incidents that they have entered into PSETS.

(5) Provide updates to PSETS, as appropriate.

Inherited from the VA NSOC.

**d. Incident Documentation**

(1) Enter incident updates in PSETS for any incident with a status of “Open”.

(2) Incidents should be reviewed and updated according to the rating assigned to the incident.

High Every 24 hours

Medium Every 48 hours

Low Every 72 hours

ISOs and POs will also receive an email alert from PSETS reminding them to provide an update. If the ticket is in “pending” status, then an update is required after one week.

Inherited from the VA NSOC.

**e. Incident Notification**

(1) Notify and keep local management and support staff apprised of the incident.

(2) Prepare Incident Notification/Credit Monitoring Letters for signature

(3) Obtain Promo Codes for Credit Monitoring Letters when applicable

### Inherited from the VA NSOC.

**f. Containment Strategy**

(1) Participate in initiating containment actions.

(2) Suggest alternate containment actions, as necessary

.

Inherited from the VA NSOC.

**g. Restoration**

Ensure timely closure of incidents and complaints.

Inherited from the VA NSOC.

**h. Evidence Gathering and Management**

(1) Execute direction provided by the Data Breach Response Service, VA-NSOC, law enforcement, and the OIG.

(2) Begin fact-finding investigation once initial complaint is logged into PSETS.

(3) Consult with law enforcement or the OIG as necessary.

(4) Log all comments and details of their investigation into PSETS or the subsequent system designated for the reporting of privacy complaints and incidents.

### **I**nherited from the VA NSOC.

**i**. **Lessons Learned**

Inherited from the VA NSOC.

# SYSTEM SPECIFIC INCIDENT HANDLING PROCEDURES

VAEC relies on the VA NSOC for all incident response activities.

1. Any incident or suspected violation of information security policy must be reported immediately to the employee’s supervisor and the ISO or PO for incidents involving PHI/PII. For weekend and after hours reporting of incidents, users must notify their supervisor or the Medical Administrative Assistant (MAA) on duty at the time who will then notify the ISO/PO. If the ISO/PO cannot be reached during off tours, the MAA will contact VA-NSOC directly at 800-877-4328 to report the incident. When reporting, the user should provide as much information as possible, including the “who, what, where, when, and how” of the event.

The ISO and PO will report the incident to the VA NSOC by entering the incident into the Privacy Security Events Tracking Systems (PSETS) within one hour of initial notification. The VA Data Breach Response Service (DBRS) Privacy and Security Event Tracking System User’s Manual, Version 2, will be followed when entering the incident.

Following initial notification the individual reporting the incident is required to submit an incident report to the ISO or PO which should provide as much information as possible, including:

* Who was involved in the event (include your own contact information)
* What exactly occurred? What information and equipment were involved?
* Where the event took place. Was it in a VA protected environment?
* When the event was discovered and by whom (date, time, time zone, and contact information).
* How many individuals may be potentially negatively impacted by the event?

The ISO will notify the appropriate management staff of all incidents. Those requiring to be notified **may include** the Director and applicable executive management, Police, Privacy Officer, CIO, Network CIO, Network ISO, Regional ISO, and the local Incident Response Team. The incident report should include date, time, description, and scope of the incident and reference positions rather than include identifying information of individuals involved in the incident.

VA Police and/or VA Office of Inspector General (VA-OIG) must be notified if the incident warrants a criminal investigation. Such incidents include, but are not limited to: theft of computer equipment or software; destruction of, or tampering with, government equipment; illegal Internet activity; electronic mail that poses a threat to veterans or staff; and falsifying or stealing information contained in VA systems.

The ISO will update the incident ticket according to the schedule below until the incident is resolved.

Categories:

High, update every 24 hours

Medium, update every 48 hours

Low, update every 72 hours

If the incident involves a medical device the procedures in HISD Medical Device Incident Response SOP dated July 25, 2016 will be followed. If the incident involves a Special Purpose System the procedures in Special Purpose Systems Incident Response SOP dated November 8, 2016, version 1.0 will be followed

Inherited from the VA NSOC.

1. Incidents reported by the NSOC.

The VA-NSOC will enter the incident into PSETS and will notify the appropriate ISO. The ISO will follow the procedures above and the instructions provided by the VA-NSOC.

For suspected and confirmed infected devices the remediation actions below will be followed.

|  |  |  |
| --- | --- | --- |
| Remediation Action | Timeframe | Notes |
| Remove suspected and confirmed infected devices off of the network | Immediately upon direction from the NSOC | The computer should not be shut down unless authorized by the VA-NSOC  The device should be disconnected from the network upon request/direction of the authorized NSOC Incident Management government personnel |
| Focused Operations (FO)/Advanced Persistent Threat (APT) Identified incidents | Remove the device(s) immediately upon direction of VA-NSOC |  |
| On Demand Scan (ODS) Logs are requested from the field for remediation | Within 48 hours of notification/direction from the VA-NSOC |  |
| Reimage of a computer is required | Reimage the machine within 72 hours of notification/direction from the VA-NSOC | The facility staff will ensure the passwords for any users of the affected device are changed, in the event the Malware has key logger capabilities.  Reimage the device.  Before placing the device back on the network, the facility OIT staff will ensure all of the latest patches and updates have been applied (McAfee, Java, Adobe, MS Office, MS Windows, etc.). |

### Enter your organization incident reported by NSOC in the table below.

For suspected and confirmed infected devices the remediation actions below will be followed.

[Organization 2 name/acronym]

|  |  |  |
| --- | --- | --- |
| Remediation Action | Timeframe | Notes |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 7. CONTACT INFORMATION



Vista Adaptive Maintenance VAEC (VAM)

|  |  |
| --- | --- |
| **Key Personnel** | **Contact Information** |
| System Owner | Work #: 202-270-1432 |
| Name: Christopher Brown | VA Cellular #: 202-270-1432 |
| Title: | VA E-mail: Christopher.brown1@va.gov |
| Facility CIO | Work #: 703-291-4478 |
| Name: Tom Willcox | VA Cellular #: 703-291-4478 |
| Title: AbleVets CIO | VA E-mail: galen.willcox2@va.gov |
| Facility ISO | Work #: 303-331-7837 |
| Name: Bobbi Begay | VA Cellular #: 303-331-7837 |
| Title: | VA E-mail: bobbi.begay@va.gov |
| Facility Privacy Officer | Work #: |
| Name: | VA Cellular #: |
| Title: | VA E-mail: |

# REFERENCES

## Acronyms

|  |  |
| --- | --- |
| **Term / Abbreviation** | **Description** |
| (VAEC) | VA Enterprise Cloud |
| (IR) | Incident Response |
| (IS) | Information System |
| (IRP) | Incident Response Plan |
| (FISMA) | Federal Information Security Management Act |
| (HIPAA) | Health Insurance Portability and Accountability Act of 1996 |
| (VBA) | Veterans Benefits Administration |
| (VHA) | Veterans Health Administration |
| (NCA) | National Cemetery Administration |
| (FIPS) | Federal Information Processing Standard |
| (VPC) | Virtual Private Cloud |
| (ICAM) | Identity, Credential, and Access Management |
| (AD) | Active Directory |
| (AZ) | Availability Zone |
| (LAN) | Local Area Network |
| (WAN) | Wide Area Network |
| (ROB) | Rules of Behavior |
| (PTA) | Privacy Threshold Assessment |
| (PIA) | Privacy Impact Analysis |
| (SOR) | System of Records |
| (AV) | Antivirus |
| (US-CERT) | United States Computer Emergency Readiness Team |
| (OIG) | Office of Inspector General |
| (E II) | Echelon II |
| (TSO) | Technical Security Officer |
| (VA NSOC) | VA Network and Security Operation Center |

## Definitions

**Potential Add -JH**

# Appendix A – 800-53 CONTROL FAMILY Incident Response (IR)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IR-1**  (L), (M), (H) | | **Incident Response Policy and Procedures:**  The organization: a. Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy [Assignment: organization-defined frequency]; and 2. Incident response procedures [Assignment: organization-defined frequency]. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-2**  (L), (M), (H) | | **Incident Response Training:**  The organization provides incident response training to information system users consistent with assigned roles and responsibilities: a. Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility; b. When required by information system changes; and c. [Assignment: organization-defined frequency] thereafter. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-2 (1)**  (H) | | **Incident Response Training:**  The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-2 (2)**  (H) | | **Incident Response Training:**  The organization employs automated mechanisms to provide a more thorough and realistic incident response training environment. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-3**  (M), (H) | | **Incident Response Testing:**  The organization tests the incident response capability for the information system [Assignment: organization-defined frequency] using [Assignment: organization-defined tests] to determine the incident response effectiveness and documents the results. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-3 (2)**  (M), (H) | | **Incident Response Testing:**  The organization coordinates incident response testing with organizational elements responsible for related plans. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-4**  (L), (M), (H) | | **Incident Handling:**  The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-4 (1)**  (M), (H) | | **Incident Handling:**  The organization employs automated mechanisms to support the incident handling process. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-4 (4)**  (H) | | **Incident Handling:**  The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-5**  (L), (M), (H) | | **Incident Monitoring:**  The organization tracks and documents information system security incidents. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-5 (1)**  (H) | | **Incident Monitoring:**  The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-6**  (L), (M), (H) | **Incident Reporting:**  The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [Assignment: organization-defined time-period]; and b. Reports security incident information to [Assignment: organization-defined authorities]. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | | |
|  | | | | |
| **IR-6 (1)**  (M), (H) | **Incident Reporting:**  The organization employs automated mechanisms to assist in the reporting of security incidents. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | | |
|  | | | | |
| IR-7  (L), (M), (H) | | **Incident Response Assistance:**  The organization provides an incident response support resource, integral to the organizational incident response capability that offers advice and assistance to users of the information system for the handling and reporting of security incidents. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-7 (1)**  (M), (H) | | **Incident Response Assistance:**  The organization employs automated mechanisms to increase the availability of incident response-related information and support. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |
| **IR-8**  (L), (M), (H) | | **Incident Response Plan:**  The organization: a. Develops an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c. Reviews the incident response plan [Assignment: organization-defined frequency]; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicates incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protects the incident response plan from unauthorized disclosure and modification. | | |  |  |  |  | | --- | --- | --- | --- | | Status | | Type | | | In Place |  | Common | x | | Planned |  | Hybrid |  | | In Place and Planned |  | System Specific |  | | Not Applicable |  |  | | |
|  | | | | |

# Appendix B – Incident Response and Management Resources

Federal Agency Incident Categories

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Name | Description | Reporting Timeframe |
| CAT 0 | Exercise/Network Defense Testing | This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses. | Not Applicable; this category is for each agency's internal use during exercises. |
| CAT 1 | \*Unauthorized Access | In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource | Within one (1) hour of discovery/detection. |
| CAT 2 | \*Denial of Service (DoS) | An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS. | Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity. |
| CAT 3 | \*Malicious Code | *Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software. | Daily Note: Within one (1) hour of discovery/detection if widespread across agency. |
| CAT 4 | \*Improper Usage | A person violates acceptable computing use policies. | Weekly |
| CAT 5 | Scans/Probes/Attempted Access | This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. | Monthly Note: If system is classified, report within one (1) hour of discovery. |
| CAT 6 | Investigation | *Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. | Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated. |

VA Incident Roles and Responsibilities

|  |  |
| --- | --- |
| **VA Role Title** | **Responsibilities** |
| **VA-NSOC Team Lead** | Approve incident severity assignments. Approve and direct all IM efforts based on standard security practices or as directed by VA OI&T or United States Computer Emergency Readiness Team (US­CERT). |
| **VA-NSOC** | * Provide central coordination and IM functions for all cyber security events and incidents affecting the VA. * Identify, validate and direct all IM efforts. * Coordinate with outside agencies such as US-CERT. * Work directly with the Office of Inspector General (OIG) to support any activity necessary. * Track the progress of response activity via a Security Event Trouble Ticket and perform all necessary documentation of incident progress. * Generate a Situation Report, Final Incident Report and a Lessons Learned briefing for major incidents. * Assist law enforcement with the collection of forensic data in accordance with Federal and local law. * Under special circumstances, as determined by the IPS Director, deploy an Emergency Response Team to affected locations to direct and help in IM efforts * Monitor VA network for potential threats and malicious activity |
| **CIO** | * Responsible for the portion of the enterprise under their charge. * Ensure mission continuity and the assurance of the confidentiality, integrity and availability of VA resources during cyber security situations. * Decide for all recommended actions proposed by VA-NSOC. * Balance mission needs with recommended risk mitigations. |
| **ISO** | * Coordinate incidents under their jurisdiction * Act as the first line of defense when events or incidents occur, and operate as the field counterpart to the VA-NSOC * Assure that all affected field personnel such as the affected CIOs, Echelon II (E-II) ISOs and technical staff (Local Area Network (LAN)/Wide Area Network (WAN), system administrators, etc.) are aware of IM activity and direction during a cyber security situation. |

Incident Management Responsibilities Matrix

|  |  |  |
| --- | --- | --- |
| **TASK** | **CIO** | **ISO/Technical Security Officer (TSO)** |
| **Security Event/Incident Reporting** |  | Assure a ticket is created for a newly discovered event, when applicable. Update ticket.  Notify VA-NSOC when there is a change in the status of an event. |
| **Incident Validation** |  | Assure that accurate information is provided Provide accurate information to VA-NSOC in timely manner. |
| **Severity Assignments/ Incident Confirmation** |  |  |
| **Notification** | Make appropriate notifications and escalations | Notify local organizational structure and support staff in a timely manner.  Notify the WAN Manager as appropriate |
| **Incident Management** |  | Assist VA-NSOC in directing response actions  Notify VISN CIO, WAN Managers and local IT staff, as necessary |
| **Containment** | Make decisions about containment actions Initiates containment actions.  Suggests alternate containment actions as necessary | Work with the WAN Manager, Facility ISO and facility personnel to assure containment actions are performed in a timely and efficient manner |
| **Remediation / Response Actions** | Balance mission needs with recommended risk mitigation.  Coordinate with Facility ISOs to implement eradication and  remediation actions | Provide VA-NSOC with all related information.  Assure response actions are carried out by LAN/WAN managers.  Coordinate with CIO and VA-NSOC on response actions and mitigation strategies  Assure that remediation actions are performed in a timely and efficient manner.  Coordinate with field on eradication and remediation actions |
| **Incident Documentation**  **and Lessons Learned** |  | Report recovery actions to the VA-NSOC.  Communicate information from VA-NSOC to the field. |

# Appendix C – Policy and Document References

VA Directive 6500, “Managing Information Security Risk: VA Information Security Program”

VA Handbook 6500, “Risk Management Framework for VA Information Systems - Tier 3: VA Information Security Program”

VA Handbook 6500.2 “Management of Breaches Involving Sensitive Personal Information”

NIST SP 800-12 Rev. 1, “An Introduction to Computer Security: The NIST Handbook”

NIST SP 800-37 Rev. 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach”

NIST SP 800-53 Rev. 4, “Security and Privacy Controls for Federal Information Systems and Organizations”

NIST SP 800-53A Rev. 4 “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans”

NIST SP 800-61 Rev. 2, “Computer Security Incident Handling Guide”