U.S. DEPARTMENT OF VETERANS AFFAIRS



VISTA ADAPTIVE MAINTENANCE (VAM)

Incident Response Plan

Version 1.0

09/07/2018

SYSTEM SECURITY ARTIFACT  
ASSESSMENT AND AUTHORIZATION

We, the undersigned, approve the content of this Incident Response Plan for Vista Adaptive Maintenance (VAM) located in the VAEC AWS GovCloud High.



**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** |
| *09/07/2018* | *1.0* | *All* | *Initial document* | *AbleVets* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1 PURPOSE 1](#_Toc524082865)

[2 POLICY AND AUTHORITY 2](#_Toc524082866)

[3 SYSTEM INFORMATION 3](#_Toc524082867)

[3.1 System Description 3](#_Toc524082868)

[3.1.1 System Name 3](#_Toc524082869)

[3.1.2 System Description 3](#_Toc524082870)

[3.1.3 System Categorization 3](#_Toc524082871)

[3.2 System Contacts 4](#_Toc524082872)

[3.2.1 System Owner 4](#_Toc524082873)

[3.2.2 System/Facility Information Security Officer 4](#_Toc524082874)

[3.2.3 System/Facility Privacy Officer 4](#_Toc524082875)

[3.3 System Location 4](#_Toc524082876)

[3.3.1 Geographical Location of the Physical System 4](#_Toc524082877)

[3.3.2 Logical Location of the Management System 4](#_Toc524082878)

[3.3.3 Location of System Backups 4](#_Toc524082879)

[4 SYSTEM INTERCONNECTIONS 5](#_Toc524082880)

[5 ROLES AND RESPONSIBILITIES 6](#_Toc524082881)

[5.1 System Owner 6](#_Toc524082882)

[5.2 Facility CIO 8](#_Toc524082883)

[5.3 Facility ISO 10](#_Toc524082884)

[5.4 Facility Privacy Officer 12](#_Toc524082885)

[6 SYSTEM SPECIFIC INCIDENT HANDLING PROCEDURES 15](#_Toc524082886)

[7. CONTACT INFORMATION 18](#_Toc524082887)

[8 REFERENCES 19](#_Toc524082888)

[8.1 Acronyms 19](#_Toc524082889)

[Appendix A – 800-53 CONTROL FAMILY Incident Response (IR) 21](#_Toc524082890)

[Appendix B – Incident Response and Management Resources 28](#_Toc524082891)

[Appendix C – Policy and Document References 31](#_Toc524082892)

# 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 VAM.

## System Description

VISTA Adaptive Maintenance (VAM) provides a cloud-based roadmap and software for maintaining continuity of the Veterans Information Systems Technology Architecture (VISTA) and the VA workflows it supports using straightforward off-the-shelf commercial cloud services and microservices during the multi-year EHR modernization (EHRM) program. VAM will be deployed within the VA’s Enterprise Cloud using Amazon Web Services (AWS) and Amazon CloudWatch.

### System Name

System Name: VISTA ADAPTIVE MAINTANANCE  
System Acronym: VAM  
Unique Identifier: VAM

### System Description

The VAM Project will provide adaptive sustainment services to enable VA to migrate Veterans Information Systems and Technology Architecture (VistA) off of its Massachusetts General Hospital Utility Multi-Programming System (MUMPS) infrastructure to provide backwards and forwards compatibility for VistA domains and use cases including Patient Data Entry and Pharmacy Computerized Physician Order Entry (CPOE)

### System Categorization

**HIGH**

## System Contacts

### System Owner

**Title:** System Owner

**Name:** Dick Rickard

**Email:** Dick.Rickard@va.gov

**Phone:** 503-884-6178

### System/Facility Information Security Officer

**Title:** Information Systems Officer

**Name:** Bobbi Begay

**Email:** Bobbi.Begay@va.gov

**Phone:** 303-331-7837

### System/Facility Privacy Officer

**Title:** Privacy Officer

**Name:** Rita Grewal

**Email:** Rita.Grewal@va.gov

**Phone:** 202-632-7861

## System Location

### Geographical Location of the Physical System

VAM is located in one AWS GovCloud region with two Availability Zones. AWS does not disclose the physical address of its data centers.

### Logical Location of the Management System

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

### Location of System Backups

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

# ROLES AND RESPONSIBILITIES

## System Owner Dick Rickard

Per NIST SP 800-100 The information system owner is the agency official responsible for the overall procurement, development, integration, modification, and operation and maintenance of the information system.

The information system owner is responsible for ensuring that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior) and assisting in the identification, implementation, and assessment of the common security controls.

## Facility ISO

**Bobbi Begay**

Per VA Handbook 6500.2:

1. Obtain and maintain PSETS user accounts and obtain training in Remedy and Risk Assessment.
2. Complete appropriate privacy and security training.
3. Become 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. Become familiar with and establish a working relationship with the PO, CIO, 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.
9. Advise users on proper security protocols to prevent incidents.
10. Provide training to staff on their roles in preventing, reporting, and managing security incidents.
11. Ensure systems and subsystems affected by incidents are isolated as quickly as possible and, if necessary, are restored and/or rebuilt.
12. Provide local organization policy and procedures for reporting and managing incidents.
13. Verify that all users complete the VA Privacy and Security Awareness and Rules of Behavior (ROB) training annually.
14. Verify that all users sign the VA National ROB annually.
15. Initiate protective measures when an incident or vulnerability is discovered.
16. Ensure that incidents are properly reported, responses are coordinated, and incident updates are provided as required.
17. Coordinate with the PO to determine if a detected or reported security incident is also a privacy incident.
18. Enter all reported incidents into the PSETS within one (1) hour of receiving or identifying an incident.
19. Complete a risk evaluation at the time of reporting the incident and update information on each incident accordingly.
20. Enter updates to the system allotted for the reporting of privacy/security complaints or violations, as necessary, for any incident with a status of “Open”.
21. ISOs and POs will also receive an email alert from the reporting tools reminding them to provide an update. If the ticket is in “pending” status, then an update is required after one week.
22. Tickets should be reviewed at least every 72 hours. The ISOs and POs should immediately update the risk assessment with new information about the incident as soon as it becomes available.
23. Track the progress of response activity via a PSETS ticket, if the event is determined to be a breach, and performing all necessary documentation of incident progress
24. Notify and keep local management and support staff apprised of the incident.
25. Participate in initiating containment actions.
26. Suggest alternate containment actions, as necessary.
27. Execute direction provided by the Data Breach Response Service, VA NSOC, law enforcement, or the OIG.
28. Consult with law enforcement or the OIG as necessary.
29. Log all comments and details of their investigation into the PSETS or the system designated for the reporting of privacy complaints and incidents.
30. Log resolution of incident.
31. Raise user awareness through lessons learned.

## Facility Privacy Officer

**Rita Grewal**

Per VA Handbook 6500.2:

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.
4. Maintain awareness of the privacy laws, regulations, and policies that affect their organizations.
5. Ensure that individuals within their organizations know who their POs are.
6. Acquire template of Incident Notification/Credit Monitoring letter.
7. Establish a working relationship with the ISO(s) for their organizations.
8. Ensure that facility privacy personnel have appropriate incident response mechanisms, such as phone numbers, email addresses, and tools available to report suspected privacy incidents.
9. Ensure an after-action report process in place to look at root causes and future prevention mechanisms.
10. Implement Departmental and appropriate Administration privacy policies and procedures.
11. Establish an internal privacy audit or compliance monitoring and audit program.
12. Monitor and report that individuals in their organizations complete the appropriate annual Privacy training(s).
13. Ensure that privacy issues and concerns are communicated to and coordinated with appropriate parties.
14. Become aware of the systems in their organizations that collect and/or maintain PHI and/or PII.
15. Participate in the preparation and updating of Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA) for systems within the purview of their organizations.
16. 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.
17. Promote activities to foster privacy awareness (e.g., Privacy Day or Information Protection Awareness Week).
18. Receive complaints from Veterans or anyone within their organization who believes an incident has occurred.
19. Enter all complaints received into the system allotted for the reporting of incidents within one (1) hour of discovery.
20. Follow guidance provided by the VA Privacy Service in order to record all incidents in PSETS.
21. Monitor all incidents that they have entered into PSETS.
22. Provide updates to PSETS, as appropriate. 24. Enter updates to PSETS, as necessary, for any incident with a status of “Open”.
23. Track the progress of response activity via a PSETS ticket, if the event is determined to be a breach, and perform all necessary documentation of progress.
24. Enter updates into the reporting tools when prompted by reminders. If the ticket is in

“pending” status, then an update is required after one week.

1. Review tickets at least every 72 hours for updates.
2. Immediately update the risk assessment with new information about the incident as soon as it becomes available.
3. Notify and keep local management and support staff apprised of the incident.
4. Prepare Incident Notification/Credit Monitoring Letters for signature 31. Obtain Promo Codes for Credit Monitoring Letters when applicable
5. Participate in initiating containment actions.
6. Suggest alternate containment actions, as necessary.
7. Ensure timely closure of incidents and complaints.
8. Execute direction provided by the Data Breach Response Service, VA-NSOC, law enforcement, and the OIG.
9. Begin fact-finding investigation once initial complaint is logged into PSETS.
10. Consult with law enforcement or the OIG as necessary.
11. Log all comments and details of their investigation into PSETS or the subsequent system designated for the reporting of privacy complaints and incidents.
12. Log resolution of incident.
13. Raise user awareness through lessons learned.

# SYSTEM SPECIFIC INCIDENT HANDLING PROCEDURES



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

# 7. CONTACT INFORMATION

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Position | Work Phone | Cell Phone | Email |
| National Service Desk | EO Incident  Coordinator | 855-673-4357 |  | NSD.  IncidentManagement@  va.gov |
| NSOC | VA Incident Coordinator | 800-877-4328 |  | vasoc@va.gov |
| Benito Urbina | ITOPS Technical Security  Service Line Manager, | (512) 326-6014 (W) | (512) 470-7736 | Benito.Urbina@va.gov |
| Christopher Cardella | AWS Manager, Cloud Infrastructure | 512-590-9414 |  | Christopher.Cardella@va.gov |
| Bill James | AWS Facility CIO | 202-632-7390 |  | Bill.James@va.gov |
| Dick Rickard | VAM System Owner | 503-884-6178 |  | Dick.Rickard@va.gov |
| Bobbi Begay | VAM  Information Security Officer | 303-331-7837 |  | Bobbi.Begay@va.gov |
| Rita Grewal | VAM Privacy Officer | 202-632-7861 |  | Rita.Grewal@va.gov |

# 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 |

# 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 |  | | 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 |  | | 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 |  | | 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 |  | | 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 |  | | 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 |  | | 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 |  | | 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 |  | | 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 |  | | 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 |  | | 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 |  | | 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 |  | | 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”