**Incident Response Policy Template**

# PURPOSE

The purpose of this policy is to create a prescriptive set of process and procedures, aligned with applicable COV IT security policy and standards, to ensure that “YOUR AGENCY NAME” develops, disseminates, and updates the IT Incident Response Policy. This policy and procedure establishes the minimum requirements for the IT Incident Response Policy.

This policy is intended to meet the control requirements outlined in SEC501, Section 8.8 Incident Response Family, Controls IR-1 through IR-8, to include specific requirements for the Commonwealth of Virginia

# SCOPE

All “YOUR AGENCY NAME” employees (classified, hourly, or business partners) as well as all “YOUR AGENCY NAME” systems

# ACRONYMS

CIO: Chief Information Officer

COV: Commonwealth of Virginia

CSRM: Commonwealth Security and Risk Management

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

ISO: Information Security Officer

IT: Information Technology

ITRM: Information Technology Resource Management

PII: Personally Identifiable Information

SEC501: Information Security Standard 501

“YOUR AGENCY NAME”: “YOUR AGENCY NAME”

# DEFINITIONS

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

# BACKGROUND

The IT Incident Response Policy at “YOUR AGENCY NAME” is intended to facilitate the effective implementation of the processes necessary meet the incident response requirements as stipulated by the COV ITRM Security Standard SEC501 and security best practices. This policy directs that “YOUR AGENCY NAME” meet these requirements for all IT systems.

# ROLES & RESPONSIBILITY

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

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Roles** | Incident Response Team | Data Owner | System Owner | System Admin | Information Security Officer |
| **Tasks** |  |  |  |  |  |
| Require service provider to document and implement threat detection practices |  |  | I |  | A/R |
| Require service provider to document and implement monitoring and logging |  |  | I |  | A/R |
| Document incident handling practices | R |  | I |  | A |
| Incident response training | R |  | I |  | A |
| Incident response testing | R |  | I |  | A |
| Implement an incident handling capability | R |  | I |  | A |
| Identify and document all locations containing personal and medical information | I | R |  | R | A |
| Redact personal and medical information | I | R |  | R | A |
| Provide appropriate notice to affected individuals upon the unauthorized release of personal or medical information | I | R |  |  | A |
| Incident reporting | I |  |  | R | A |
| Incident response assistance | R |  |  |  | A |
| Develop and incident response plan | R |  |  |  | A |
| Review and revise incident response plan | R |  |  |  | A |

# STATEMENT OF POLICY

In accordance with SEC501, IR-1 through IR-8, “YOUR AGENCY NAME” shall create an incident response program with procedures and training to handle security incidents.

1. **INCIDENT RESPONSE POLICY AND PROCEDURES** 
   1. The ISO or designee requires that the agency or its service provider document and implement threat detection practices that at a minimum include the following:
      1. Designates an individual responsible for “YOUR AGENCY NAME”’s threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance;
      2. Implements Intrusion Detection System (IDS) and Intrusion Prevention System (IPS);
      3. Conducts IDS and IPS log reviews to detect new attack patterns as quickly as possible; and
      4. Develops and implements required mitigation measures based on the results of IDS and IPS log reviews.
   2. The ISO or designee requires that the agency or its service provider document and implement information security monitoring and logging practices that include the following components, at a minimum:
      1. Designates individuals responsible for the development and implementation of information security logging capabilities, as well as detailed procedures for reviewing and administering the logs;
      2. Documents standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place;
      3. Prohibits the installation or use of unauthorized monitoring devices; and
      4. Prohibits the use of keystroke logging, except when required for security investigations and a documented business case outlining the need and residual risk has been approved in writing by the Agency Head.
   3. The ISO or designee shall document information security incident handling practices and where appropriate “YOUR AGENCY NAME” shall incorporate its service provider’s procedures for incident handling practices that include the following at a minimum:
      1. Designates an Information Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber-attacks;
      2. Identifies controls to deter and defend against cyber-attacks to best minimize loss or theft of information and disruption of services;
      3. Implements proactive measures based on cyber-attacks to defend against new forms of cyber-attacks and zero-day exploits; and
      4. Establishes information security incident categorization and prioritization based on the immediate and potential adverse effect of the information security incident and the sensitivity of affected IT systems and data.
2. **INCIDENT RESPONSE TRAINING**
   1. The ISO requires specific training that includes:
      1. Personnel are trained in their incident response roles and responsibilities with respect to the information system, including identification and reporting of suspicious activities;
      2. Refresher training is provided at least once a year or whenever the Incident Response procedures are modified; and
      3. Simulated events are incorporated into incident response training to facilitate effective response by personnel in crisis situations.
3. **INCIDENT RESPONSE TESTING AND EXERCISES** 
   1. The ISO or designee shall test and/or exercise the incident response capability for the agency at least once a year using the existing incident response procedures to determine the incident response effectiveness and documents the results.
4. **INCIDENT HANDLING**
   1. The ISO or designee shall:
      1. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;
      2. Coordinate incident handling activities with contingency planning activities;
      3. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly;
      4. Obtain incident-related information from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports;
      5. Identify classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions;
         1. Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks.
         2. Incident response actions that may be appropriate include, for example, graceful degradation, information system shutdown, fall back to manual mode or alternative technology whereby the system operates differently, employing deceptive measures (e.g., false data flows, false status measures), alternate information flows, or operating in a mode that is reserved solely for when a system is under attack.
      6. Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response;
      7. Identify immediate mitigation procedures, including specific instructions, based on information security incident categorization level, on whether or not to shut down or disconnect affected IT systems; and
      8. Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.
   2. Where electronic records or IT infrastructure are involved, the Data Owner shall adhere to the following requirements. Where non-electronic records are involved or implied, the following are advisory in nature, but are strongly recommended:
      1. Identify and document all “YOUR AGENCY NAME” systems, processes, and logical or physical data storage locations (whether held by “YOUR AGENCY NAME” or a third party) that contain personal information or medical information.
         1. Personal information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:
            1. Social security number;
            2. Driver’s license number or state identification card number issued in lieu of a driver’s license number;
            3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident’s financial accounts; or
            4. Other personal identifying information, such as date of birth.
         2. Medical information means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:
            1. Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
            2. An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.
      2. “Redact” for personal information means alteration or truncation of data such that no more than the following are accessible as part of the personal information:
         1. Five digits of a social security number; or
         2. The last four digits of a driver’s license number, state identification card number, or account number.
      3. “Redact” for medical information means alteration or truncation of data such that no information regarding the following are accessible as part of the medical information:
         1. An individual’s medical history;
         2. Mental or physical condition;
         3. Medical treatment or diagnosis;
         4. No more than four digits of a health insurance policy number, subscriber number; or
         5. Other unique identifier.
      4. Include provisions in any third party contracts requiring that the third party and third party subcontractors:
         1. Provide immediate notification to “YOUR AGENCY NAME” of suspected breaches; and
         2. Allow “YOUR AGENCY NAME” to both participate in the investigation of incidents and exercise control over decisions regarding external reporting.
      5. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted personal information or medical information by any mechanism, including, but not limited to:
         1. Theft or loss of digital media including laptops, desktops, tablets, CDs, DVDs, tapes, USB drives, SD cards, etc.;
         2. Theft or loss of physical hardcopy; and
         3. Security compromise of any system containing personal or medical information (i.e., social security numbers, credit card numbers, medical records, insurance policy numbers, laboratory findings, pharmaceutical regimens, medical or mental diagnosis, medical claims history, medical appeals records, etc.).
      6. “YOUR AGENCY NAME” shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.
      7. If a Data Custodian is the entity involved in the data breach, they must alert the Data Owner so that the Data Owner can notify the affected individuals.
      8. In the case of a computer (i.e., public kiosk, individually owned, or COV resource) found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules. “YOUR AGENCY NAME” shall notify the CISO when notification of affected individuals has been completed.
      9. Provide notification that consists of:
         1. A general description of what occurred and when;
         2. The type of Personal Information (PII) that was involved;
         3. What actions have been taken to protect the individual’s Personal Information from further unauthorized access;
         4. A telephone number that the person may call for further information and assistance, if one exists; and
         5. What actions “YOUR AGENCY NAME” recommends that the individual take. The actions recommended should include monitoring their credit report and reviewing their account statements (i.e., credit report, medical insurance Explanation of Benefits (EOB), etc.).
      10. Provide this notification by one or more of the following methodologies, listed in order of preference:
          1. Written notice to the last known postal address in the records of the individual or entity;
          2. Telephone Notice;
          3. Electronic notice; or
          4. Substitute Notice - if the individual or the entity required under law to provide notice demonstrates that the cost of providing such notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following:
             1. Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
             2. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and
             3. Notice to major statewide media, including newspaper, radio, and television.
      11. “YOUR AGENCY NAME” shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated below.
      12. Hold the release of notification immediately following verification of unauthorized data disclosure only:
          1. If law enforcement is notified and the law enforcement agency determines and advises “YOUR AGENCY NAME” that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.
          2. Where CISO or designee determines that it would interfere with the scope of the data breach or the investigation of root cause.
5. **INCIDENT MONITORING**
   1. The ISO or designee shall require that system security incidents are tracked and documented including, but not limited to, the following information:
      1. Maintaining records about each incident,
      2. The status of the incident,
      3. Pertinent information necessary for forensics, and
      4. Evaluating incident details, trends, and handling.
   2. The ISO requires IT system event logs are monitored in real time, information is correlated with other automated tools, suspicious activities are identified, and alert notifications are provided.
6. **INCIDENT REPORTING**
   1. The ISO or designee shall:
      1. Require personnel to report suspected security incidents to the CISO within 24 hours from when “YOUR AGENCY NAME” discovered or should have discovered their occurrence.
      2. Report security incident information to designated authorities.
         1. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable laws, directives, policies, regulations, standards, and guidance.
      3. Report information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.
      4. Provide quarterly summary reports of IDS and IPS events to Commonwealth Security.
      5. Establish a process for reporting IT security incidents to the CISO. All “YOUR AGENCY NAME” customers and partners are encouraged to report security incidents; however, Executive Branch agencies must establish a reporting process for IT security incidents in accordance with §2.2-603(F) of the Code of Virginia so as to report “to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence,”… “all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities.”
      6. Report information security incidents only through channels that have not been compromised.
7. **INCIDENT RESPONSE ASSISTANCE**
   1. The ISO or designee shall provide an incident response support resource, integral to the organizational incident response capability, which offers advice and assistance to users of the information system for the handling and reporting of security incidents.
   2. The ISO or designee shall:
      1. Establish a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and
         1. External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.
      2. Identify organizational incident response team members to the external providers.
8. **INCIDENT RESPONSE PLAN**
   1. The ISO or designee shall:
      1. Develop an incident response plan that:
         1. Provides “YOUR AGENCY NAME” with a roadmap for implementing its incident response capability;
         2. Describes the structure and organization of the incident response capability;
            1. The “YOUR AGENCY NAME” mission, strategies, and goals for incident response help determine the structure of its 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 designated officials within “YOUR AGENCY NAME”.
      2. Distribute copies of the incident response plan to the organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements;
      3. Review the incident response plan at least once a year;
      4. Revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and
      5. Communicate incident response plan changes to the organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements.

# ASSOCIATED

**PROCEDURE** “YOUR AGENCY NAME” Information Security Program Policy

[IT Security Threat Management Guideline (SEC506-01)](http://www.vita.virginia.gov/uploadedFiles/Library/SEC510-00ThreatManagementGuideline.pdf)

**AUTHORITY**

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

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

**OTHER**

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

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

| Version History | | |
| --- | --- | --- |
| Version | Date | Change Summary |
| 1 | 07/01/2014 | Supersedes “YOUR AGENCY NAME” CSRM Data Breach Notification Policy and Procedure |
| 2 | 11/16/2021 | Formatting changes |