# Policy and Procedure 9-8
# Information Security: Incident Response

| | | | |
|---|---|---|---|
| **Issued By:** | Robert W. Farrell, State Forester | DocuSigned by: Robert W. Farrell 2115C3D38FCF4E7... | 7/1/2024 |
| **Effective Date:** | June 10, 2024 | | |
| **Codes/Mandates:** | Code of Virginia, §2.2-2005 Creation of Agency; appointment of Chief Information Officer<br>Code of Virginia: §2.2-2007 Powers of the CIO | | |
| **References:** | Commonwealth Information Technology Resource Management (ITRM) Information Security Policy SEC 519-00<br>Commonwealth ITRM Standard SEC502: Audit Security Standard<br>Commonwealth ITRM Standard SEC530: Information Security Standard | | |
| **Forms:** | See Attachments | | |

## CONTENTS



## PURPOSE

The purpose of this policy and procedure is to document the response procedure for potential information technology (IT) security incidents that threatens the Department of Forestry IT systems and services.

## SCOPE

All Department of Forestry employees (classified, hourly, or business partners) as well as DOF systems.

# DEFINITIONS and ACRONYMS

**"Agency"** and **"DOF"** means the Virginia Department of Forestry.

**"Chief Information Security Officer" or "CISO"** means The senior management official designated by the CIO of the Commonwealth to develop Information Security policies, procedures, and standards to protect the confidentiality, integrity, and availability of information systems and data.

**"Data custodian" means** an individual or organization in physical or logical possession of data for Data Owners. Data Custodians are responsible for protecting the data in their possession from unauthorized access, alteration, destruction, or usage and for providing and administering general controls, such as back-up and recovery systems.

**"Data owner"** means the agency manager or supervisor, designated by the state forester, who defines, manages and controls the use of data and ensures compliance with adopted standards.

**"Information security officer"** and **"ISO"** means the agency employee who is designated by the state forester to develop and manage the agency's information security program, as required in the Commonwealth's Information Security Standard, SEC530.

**"System administrator"** means the agency employee who implements, manages, and/or operates a system at the direction of the system owner or data owner.

**"System owner"** means the agency manager or supervisor who is responsible for the operation and oversight of any given agency business system.

**ACRONYMS**

| | |
|---|---|
| CIO: | Chief Information Officer |
| CIRT: | Computer Incident Response Team |
| COV: | Commonwealth of Virginia |
| CSRM: | Commonwealth Security and Risk Management |
| DOF: | Department of Forestry |
| DRP: | Disaster Recovery Plan |
| IDS: | Intrusion Detection System |
| IPS: | Intrusion Prevention System |
| ISO: | Information Security Officer |
| IT: | Information Technology |
| PII: | Personally Identifiable Information |
| ITRM: | Information Technology Resource Management |
| SEC530: | Information Security Standard 530 |
| VCCC: | VITA Customer Care Center |
| VITA: | Virginia Information Technology Agency |

# BACKGROUND

The Information Security Incident Response Policy and Procedure at Department of Forestry is intended to facilitate the effective implementation of the processes necessary to meet the IT Incident Response requirements as stipulated by the COV ITRM Security Standard SEC530, Section 8.8 Incident Response, IR-1 through IR-8, and security best practices.

# ROLES & RESPONSIBILITY

This section will provide summary of the roles and responsibility as described in the Statement of Process section. The following Roles and Responsibility Matrix describes 4 role specific activities:

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

| | 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 |
| Conduct incident response training. | R | | I | | A |
| Conduct 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 |
| Complete incident reporting. | I | | | R | A |
| Provide incident response assistance. | R | | | | A |
| Develop and incident response plan. | R | | | | A |
| Review and revise incident response plan. | R | | | | A |
| Coordinate all aspects of the incident handling process. | A | | | | R |

# STATEMENT OF POLICY

In accordance with SEC530, Section 8.8 Incident Response, IR-1 through IR-8, DOF shall create an incident response program with procedures and training to handle security incidents.

## Policy and Procedures (IR-1)

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:
    a. Designates an individual responsible for Department of Forestry's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.
    b. Implements Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).
    c. Conducts IDS and IPS log reviews to detect new attack patterns as quickly as possible.
    d. 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:
    a. Designates individuals responsible for the development and implementation of information security logging capabilities, as well as detailed procedures for reviewing and administering the logs.

b. Documents standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place.

c. Prohibits the installation or use of unauthorized monitoring devices.

d. 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 shall incorporate its service provider's procedures for incident handling practices that include the following at a minimum:

a. Designates an Information Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber-attacks.

b. Identifies controls to deter and defend against cyber-attacks to best minimize loss or theft of information and disruption of services.

c. Implements proactive measures based on cyber-attacks to defend against new forms of cyber-attacks and zero-day exploits.

d. 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.

## Incident Response Training (IR-2)

1. The ISO requires specific training that includes:

a. Personnel are trained in their incident response roles and responsibilities with respect to the information system, including identification and reporting of suspicious activities.

i. Training is provided within 30 days of assuming an incident response role or responsibility or acquiring new system access.

ii. Refresher training is provided at least once a year or whenever the Incident Response procedures or system changes occur.

iii. Simulated events are incorporated into incident response training to facilitate effective response by personnel in crisis situations.

iv. Training on how to identify and respond to a breach is included, including the organization's process for reporting a breach.

b. Incident response training content is reviewed on an annual basis and following environmental change or security incident.

## Incident Response Testing And Exercises (IR-3)

1. The ISO or designee shall:

a. 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.

b. Coordinate incident response testing with organizational elements responsible for related plans such as the business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, crisis communications plans, critical infrastructure plans, and occupant emergency plans.

c. Use qualitative and quantitative data from testing to:

i. Determine the effectiveness of incident response processes.

ii. Continuously improve incident response processes.

iii. Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

## Incident Handling (IR-4)

1. The ISO or designee shall:
    a. Implement an incident handling capability for security incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication and recovery.
    b. Coordinate incident handling activities with contingency planning activities.
    c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.
    d. Ensure the rigor, intensity, scope and results of incident handling activities are comparable and predictable across the organization.
    e. Support the incident handling process using organization-defined automated mechanisms such as online incident management systems and tools that support the collection of live-response data, full network packet capture and forensic analysis.
    f. Identify classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions.
        i. Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks and untargeted malicious attacks.
        ii. 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.
    g. Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.
    h. Implement a configurable capability to automatically disable the system if organization-defined security violations are detected.
    i. Implement an incident handling capability for incidents involving insider threats, including coordination with intra and external organizations as appropriate.
    j. Coordinate with the appropriate external organizations to correlate and share incident information to achieve a cross-organization perspective on incident awareness and more effective incident responses.
    k. Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.
    l. Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization within eight hours.
        i. Deployment can be virtual or physical.
    m. Analyze malicious code and/or other residual artifacts remaining in the system after the incident,
    n. Analyze anomalous or suspected adversarial behavior in or related to organization environments and resources.
    o. Establish and maintain a security operations center (SOC).
    p. Manage public relations associated with an incident including employing measures to repair the reputation of the organization.
    q. 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.
    r. 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:

    a. Identify and document all DOF systems, processes, and logical or physical data storage locations (whether held by DOF or a third party) that contain personal information or medical information.

        i. 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:

            - Social security number.
            - Driver's license number or state identification card number issued in lieu of a driver's license number.
            - 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
            - Other personal identifying information, such as date of birth.

        ii. 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:

            - 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
            - 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.

    b. "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:

        i. Five digits of a social security number or

        ii. The last four digits of a driver's license number, state identification card number or account number.

    c. "Redact" for medical information means alteration or truncation of data such that no information regarding the following is accessible as part of the medical information:

        i. An individual's medical history.

        ii. Mental or physical condition.

        iii. Medical treatment or diagnosis.

        iv. No more than four digits of a health insurance policy number, subscriber number or

        v. Other unique identifier.

    d. Include provisions in any third-party contracts requiring that the third-party and third-party subcontractors:

        i. Provide immediate notification to Department of Forestry of suspected breaches; and

        ii. Allow Department of Forestry to both participate in the investigation of incidents and exercise control over decisions regarding external reporting.

    e. 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:

        i. Theft or loss of digital media including laptops, desktops, tablets, CDs, DVDs, tapes, USB drives, SD cards, etc..

        ii. Theft or loss of physical hardcopy,

iii. 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.).

f. DOF 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.

g. 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.

h. 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. Department of Forestry shall notify the chief information security officer (CISO) when notification of affected individuals has been completed.

i. Provide notification that consists of:

   i. A general description of what occurred and when.

   ii. The type of Personal Information (PII) that was involved.

   iii. What actions have been taken to protect the individual's Personal Information from further unauthorized access.

   iv. A telephone number that the person may call for further information and assistance, if one exists.

   v. What actions DOF 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.).

j. Provide this notification by one or more of the following methodologies, listed in order of preference:

   i. Written notice to the last known postal address in the records of the individual or entity.

   ii. Telephone notice.

   iii. Electronic notice.

   iv. 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.

      3. Notice to major statewide media, including newspaper, radio, and television.

k. Department of Forestry shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated below.

l. Hold the release of notification immediately following verification of unauthorized data disclosure only:

   i. If law enforcement is notified and the law enforcement agency determines and advises DOF 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.

   ii. Where CISO or designee determines that it would interfere with the scope of the data breach or the investigation of root cause.

## Incident Monitoring (IR-5)

1. The ISO or designee shall require that system security incidents are tracked and documented including, but not limited to, the following information:
    a. Maintaining records about each incident.
    b. Status of the incident.
    c. Pertinent information necessary for forensics.
    d. Evaluating incident details, trends, and handling.
2. The ISO requires IT system track incidents and collect and analyze incident information using Commonwealth Security and Risk Management approved and integrated tools.

## Incident Reporting (IR-6)

1. The ISO or designee shall:
    a. Require personnel to report suspected security incidents to the CISO within 24 hours from when DOF discovered or should have discovered their occurrence.
    b. Report security incident information to designated authorities.
        i. 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.
        ii. Report incidents using the Commonwealth Incident Reporting Form.
    c. Report information system vulnerabilities associated with reported security incidents to CISO.
    d. Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.
    e. Provide quarterly summary reports of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) events to Commonwealth Security.
    f. Establish a process for reporting IT security incidents that complies to the Code of Virginia § 2.2-5514 and verify that the IT security incident has been recorded into the Commonwealth Security and Risk Management approved system within 24 hours;
    g. Report information security incidents only through channels that have not been compromised.
    h. Provide Commonwealth Security and Risk Management at least on an annual basis or when personnel changes occur the emergency contact information for agency personnel that should be contacted for security incidents that occur outside of normal working hours.

## Incident Response Assistance (IR-7)

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:
    a. Increase the availability of incident response related information and support using organization-defined automated mechanisms.
    b. Establish a direct, cooperative relationship between its incident response capability and external providers of information system protection capability.
        i. 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.

c. Identify organizational incident response team members to the external providers.

## Incident Response Plan (IR-8)

3. The ISO or designee shall:
   a. Develop an incident response plan that:
      i. Provides a roadmap for implementing its incident response capability.
      ii. Describes the structure and organization of the incident response capability.
         1. The Department of Forestry mission, strategies, and goals for incident response help determine the structure of its incident response capability.
      iii. Provides a high-level approach for how the incident response capability fits into the overall organization.
      iv. Meets the unique requirements of the organization, which relate to mission, size, structure and functions.
      v. Defines reportable incidents.
      vi. Provides metrics for measuring the incident response capability within the organization..Defines the resources and management support needed to effectively maintain and mature an incident response capability.
      vii. Addresses the sharing of incident information.
      viii. Is reviewed and approved by designated officials within Department of Forestry.
      ix. Explicitly designates responsibility for incident response to the ISO and designees.
   b. 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.
   c. Review the incident response plan at least once a year.
   d. Update the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
   e. Communicate incident response plan changes to the organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements.
   f. Protect the incident response plan from unauthorized disclosure and modification.
   g. Include the following in the Incident Response Plan for breaches involving personally identifiable information:
      i. A process to determine if notice to individuals or other organizations, including oversight organizations, is needed.
      ii. An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
      iii. Identification of applicable privacy requirements.

# STATEMENT OF PROCEDURE

The Computer Incident Response Team (CIRT) will act as the incident coordinator for all reported IT security incidents. The incident coordinator, under the direction of the ISO, and with the assistance of the affected agency contacts, will be responsible for coordinating all aspects of the incident handling process and the incident response process. All persons involved in the incident response and clean-up are responsible for providing all requested information to the incident coordinator. Department of Forestry and contracted staff must coordinate with the CIRT prior to initiating any actions

during the investigation or in response to information security incidents. All communications regarding IT security incidents must be conducted through channels that are known to be unaffected by the IT security incident under investigation.

## Computer Incident Response Team

1. The CIRT consists of:
    a. The Information Security Officer (ISO); and
    b. The VITA Commonwealth Security and Risk Management (CSRM) Incident Management (IM) staff.

## Incident Handling Process

1. An incident report is received by the CIRT via the ISO or the Incident Reporting System.
2. The CIRT reviews each incident report to confirm a security incident has occurred.
    a. If a confirmed incident, the appropriate parties will be contacted as stipulated in the Information Security Incident Reporting (IR-6) in this policy and procedure.
    b. If not a confirmed incident, the information is passed on to the appropriate parties for resolution.
3. The CIRT, agency management and the ISO will determine if the incident requires immediate response.
    a. If so, the CIRT will activate and begin to coordinate response activities.
    b. If not, the agency management and ISO will coordinate appropriate response activities.
4. The CIRT, agency management and the ISO will determine if the incident will require an investigation.
    a. If so, investigative efforts are initiated.
    b. If not, recovery efforts are initiated.
5. In cases where multiple incidents are occurring simultaneously, the CIRT will classify the incidents according to their immediate and potential adverse effects and prioritize recovery and investigation activities according to these effects.
6. Initiation of Recovery and Investigation.
    a. Initial Response Checklist (Attachment A) provides a response checklist for CIRT members to log initial details and activity.
    b. All pertinent live forensic data should be recovered from the system before disconnection from network or powering down.
    c. Windows Forensic Checklist (Attachment B), details steps for Windows based platforms.
    d. Unix Forensic Command Log Sheet (Attachment C) provides a form for CIRT members to log commands used on UNIX based platforms. Due to the variety of commands necessary on UNIX based platforms, specific commands are not provided.
    e. Additional network traces performed with open standards-based network packet capture tools may also be required.
7. Preservation of evidence if an investigation is required.
    a. In cases of investigations where physical evidence is collected from the scene, CIRT members will fill out a Description of Evidence Form (Attachment D).
    b. In cases where criminal charges may be an outcome, CIRT members will also use a Chain of Custody Form (Attachment E).
    c. CIRT members are to make forensic drive images of incident related hardware and store the originals in clearly marked containers in a locked area. All forensic drive images should be recorded in an open standard

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

8. Identification of Problem.
    a. CIRT members should identify the root cause of the incident and the most likely vectors of attack. If recoverable malicious binaries can be removed from the system(s), they should be put on safe media and forwarded to the appropriate anti-virus vendor contacts.
9. Containment and Recovery.
    a. CIRT members will take appropriate immediate actions to contain and control the incident. This may require removal of infected machines or entire network segments from the larger agency network. It may also require blocking agency networks from access to the Internet or other Commonwealth resources. CIRT members should also develop an action plan for recovery of systems harmed in an incident with assistance from agency management and the (ISO) to be carried out by appropriate DOF and contracted staff. All staff will cooperate with the directives of the CIRT in a timely manner to minimize exposure time and vulnerability.
10. Restoration of Functionality.
    a. After an incident has been contained and all affected systems have returned to normal operations mode, the CIRT will finish the incident response by verification of proper systems behavior.
11. Follow-up analysis.
    a. Once an incident has been resolved and all systems are restored to a normal mode of operation, a follow-up postmortem analysis will be performed. All involved DOF and agency parties will meet and discuss actions taken and the lessons learned. Pertinent procedures should be evaluated and modified, if necessary. If applicable, a set of recommendations should be presented to the appropriate management levels.

## AUTHORITY

This policy and procedure is issued by the Virginia state forester.

## INTERPRETATION

The director of information technology and the chief of administration are responsible for the interpretation of this policy and procedure.

## APPROVAL

I certify that this policy and procedure is approved and ready for publication.

| | | |
|---|---|---|
| Parik Patel | DocuSigned by: Parik Patel 3448F7C5388F457... | 6/10/2024 |
| Director of Information Technology Name (Print) | Director of Information Technology Signature | |
| Amanda Davis | DocuSigned by: amanda davis C2CCAB60F85A4A6... | 6/27/2024 |
| Chief of Administration Name (Print) | Chief of Administration Signature | |

## Version History

| Version History | | | |
|---|---|---|---|
| **Date** | **Version** | **Details** | **Author/Contributors** |
| June 10, 2024 | 1 | Original – CSRM template and updated with SEC530 | Catherine Shefski, ISO |

## Attachment A

**Initial Response Checklist**

Incident #: _____ Date: _____

**Contact Information**

Your Contact Information

| | |
|---|---|
| Name: | |
| Department: | |
| Telephone: | |
| Other Telephone: | |
| Email: | |

Individual Reporting Incident

| | |
|---|---|
| Name: | |
| Department: | |
| Telephone: | |
| Other Telephone: | |
| Email: | |

**Incident Detection**

| | |
|---|---|
| Type of Incident: | □ Denial of Service □ Unauthorized Access<br>□ Virus □ Unauthorized Use of Resources<br>□ Hoax □ Theft of Intellectual Property<br>□<br>Other:_____<br>_____<br>_____<br>_____ |
| Location of Incident: | Address:<br><br>Building:<br><br>Room Number: |
| Describe the Physical Security at the Site:<br>1. Are there locks?<br>2. Alarm systems?<br>3. Who is charge of Physical Security at the site? | |

| | |
|---|---|
| How the incident was detected: | |
| Is the information concerning the incident stored in a protected, tamper-proof manner? | |

**System Details**

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

**Incident Containment**

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

Incident #:_____ Date:_____

| | |
|---|---|
| Are there backups of the system? | |
| Who has accessed/ touched system(s) affected since the onset of the incident? | |
| Who has had physical access to the system since the incident? | |
| Who currently knows about the incident? | |
| Is there a need to keep knowledge of the incident on a "need to know" basis? | |
| Have network devices (routers, firewalls) been configured to provide additional defense against the incident? | |

**Preliminary Investigation**

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

Incident #:_____ Date:_____

Comments:

## Attachment B

**Windows Forensics Checklist**

Incident #: _____ Date: _____
Investigator_____

1. Execute trusted cmd.exe ____

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

3. Determine logged on users ____
   psloggedon

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

5. Record open ports ____
   netstat –an

6. Associate Applications with open ports ____
   fport

7. Grab process listing ____
   pslist

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

9. Record system time and data again ____

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

Comments:
_____
_____
_____
_____

## Attachment C

**Unix Forensic Command Log**

| Start Time | Command Line | Trusted | Un | MD5 Sum | Comments |
|---|---|---|---|---|---|
| | | | | | |

## Attachment D

**Description of Evidence Form**

Case Information

Date:

Case:

Location:

CPU Information

Make/Model: Memory:

Serial Number: Processor:

Asset Tag Number:

Remarks:

Hard Drives/Removable Media

Drive 0:

Type:

Serial Number:

Capacity:

Remarks:

Drive 1:

Type:

Serial Number:

Capacity:

Remarks:

Drive 2:

Type:

Serial Number:

Capacity:

Remarks:

Drive 3:

Type:

Serial Number:

Capacity:

Remarks:

Additional Notes

## Attachment E

**Chain of Custody Form**

Date: Case Number:

Consent Required: Y N Signature of Consenting Person:

Tag Number:

Description:

Person Receiving Evidence: Signature:

| From: | Date: | Reason: | To: |
|---|---|---|---|
| From: | Date: | Reason: | To: |
| From: | Date: | Reason: | To: |