SYSTEM SECURITY PLAN

**A picture containing drawing

Description automatically generated**

**[INSERT\_COMPANY\_LOGO]**

TABLE OF CONTENTS

[1. SYSTEM POINTS OF CONTACT 3](#_Toc37245207)

[2. SYSTEM IDENTIFICATION 4](#_Toc37245208)

[2.1. System Name 4](#_Toc37245209)

[2.2. System Categorization 4](#_Toc37245210)

[2.3. General Description/Purpose of System 4](#_Toc37245211)

[2.4. General Description of Information 4](#_Toc37245212)

[3. SYSTEM ENVIRONMENT 5](#_Toc37245213)

[3.1. Hardware and Software Inventory 5](#_Toc37245214)

[3.2. Hardware and Software Maintenance and Ownership 5](#_Toc37245215)

[4. LAWS, REGULATIONS, AND POLICIES AFFECTING THE SYSTEM 6](#_Toc37245216)

[5. SECURITY CONTROL SELECTION 7](#_Toc37245217)

[5.1. Access Control 7](#_Toc37245218)

[5.2. Awareness and Training 10](#_Toc37245219)

[5.3. Audit and Accountability 10](#_Toc37245220)

[5.4. Configuration Management 12](#_Toc37245221)

[5.5. Identification and Authentication 13](#_Toc37245222)

[5.6. Incident Response 15](#_Toc37245223)

[5.7. Maintenance 15](#_Toc37245224)

[5.8. Media Protection 16](#_Toc37245225)

[5.9. Personnel Security 17](#_Toc37245226)

[5.10. Physical Protection 18](#_Toc37245227)

[5.11. Risk Assessment 19](#_Toc37245228)

[5.12. Security Assessment 19](#_Toc37245229)

[5.13. System and Communications Protection 20](#_Toc37245230)

[5.14. System and Information Integrity 22](#_Toc37245231)

[6. INCIDENT RESPONSE PLAN 24](#_Toc37245232)

[6.1. Incident Phases 24](#_Toc37245233)

[**6.1.1.** **Prepare** 24](#_Toc37245234)

[**6.1.2.** **Detection and Analysis** 25](#_Toc37245235)

[**6.1.3.** **Containment, Eradication, And Recovery** 27](#_Toc37245236)

[**6.1.4.** **Post-Incident Activity** 28](#_Toc37245237)

[6.2. Incident Handling Checklist 29](#_Toc37245238)

[7. APPENDIX A - INVENTORY 34](#_Toc37245239)

[8. APPENDIX B - REFERENCES 35](#_Toc37245240)

[9. APPENDIX C - RECORD OF CHANGES 36](#_Toc37245241)

# **SYSTEM POINTS OF CONTACT**

* 1. **Responsible Organization:**

|  |  |
| --- | --- |
| Name: |  |
| Address: |  |
| Phone: |  |

**Information Owner [Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal]**

|  |  |
| --- | --- |
| Name: |  |
| Title: |  |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

* + - 1. **System Owner [assignment of security responsibility]**

|  |  |
| --- | --- |
| Name: |  |
| Title: |  |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

* + - 1. **System Security Officer [research, develop, implement, test and review an organization's information security in order to protect information and prevent unauthorized access.]**

|  |  |
| --- | --- |
| Name: |  |
| Title: |  |
| Office Address: |  |
| Work Phone: |  |
| e-Mail Address: |  |

# **SYSTEM IDENTIFICATION**

* 1. System Name**: [State the name of the system. Spell out acronyms.]**
  2. System Categorization**:** **[Systems Impact level used to select a baseline of security controls for the information system from NIST SP 800-53. The potential impact is low if—The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. The potential impact is moderate if—The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The potential impact is high if—The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.]**
  3. General Description/Purpose of System**:**  What is the function/purpose of the system? **[Provide a short, high-level description of the function/purpose of the system.]** 
     1. Number of end users and privileged users: **[In the table below, provide the approximate number of users and administrators of the system. Include all those with privileged access such as system administrators, database administrators, application administrators, etc. Add rows to define different roles as needed.]**

Roles of Users and Number of Each Type:

|  |  |
| --- | --- |
| **Number of Users** | **Number of Administrators/**  **Privileged Users** |
|  |  |

* 1. General Description of Information**: [Document the information types processed, stored, or transmitted by the system below]**

# **SYSTEM ENVIRONMENT**

Include a detailed topology narrative and graphic that clearly depicts the system boundaries, system interconnections, and key devices. (Note**:** this does not require depicting every workstation or desktop, but include an instance for each operating system in use, an instance for portable components (if applicable), all virtual and physical servers (e.g., file, print, web, database, application), as well as any networked workstations (e.g., Unix, Windows, Mac, Linux), firewalls, routers, switches, copiers, printers, lab equipment, handhelds). If components of other systems that interconnect/interface with this system need to be shown on the diagram, denote the system boundaries by referencing the security plans or names and owners of the other system(s) in the diagram.

**[Insert a system topology graphic. Provide a narrative consistent with the graphic that clearly lists and describes each system component.]**

* 1. Hardware and Software Inventory - Include or reference a **complete and accurate** listing of all hardware (a reference to the organizational component inventory database is acceptable) and software (system software and application software) components, including make/OEM, model, version, service packs, and person or role responsible for the component. See Appendix A **[Insert the reference/URL or note that the hardware component inventory is attached.]**
  2. Hardware and Software Maintenance and Ownership - Is all hardware and software maintained and owned by the organization? **[Yes/No - If no, explain and include maintenance agreements or contracts:]**

# **LAWS, REGULATIONS, AND POLICIES AFFECTING THE SYSTEM**

List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of the system and information retained by, transmitted by, or processed by the system. General agency security requirements need not be listed since they mandate security for all systems. Each agency should decide on the level of laws, regulations, and policies to include in the system security plan. Examples might include the Privacy Act of 1974 or a specific statute or regulation concerning the information processed (e.g., tax or census information). If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities.

# **SECURITY CONTROL SELECTION**

**(Note: The source of the requirements is NIST Special Publication 800-171, dated December 2016)**

Provide a thorough description of how all of the security requirements are being implemented or planned to be implemented. The description for each security requirement contains: 1) the security requirement number and description; 2) how the security requirement is being implemented or planned to be implemented; and 3) any scoping guidance that has been applied (e.g., compensating mitigations(s) in place due to implementation constraints in lieu of the stated requirement). If the requirement is not applicable to the system, provide rationale.

## Access Control

* + 1. Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Limit system access to the types of transactions and functions that authorized users are permitted to execute.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Control the flow of CUI in accordance with approved authorizations.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Employ the principle of least privilege, including for specific security functions and privileged accounts.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Use non-privileged accounts or roles when accessing nonsecurity functions.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Limit unsuccessful logon attempts.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Provide privacy and security notices consistent with applicable CUI rules.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Terminate (automatically) a user session after a defined condition.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Monitor and control remote access sessions.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Route remote access via managed access control points.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Authorize remote execution of privileged commands and remote access to security-relevant information.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Authorize wireless access prior to allowing such connections.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Protect wireless access using authentication and encryption.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Control connection of mobile devices.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Encrypt CUI on mobile devices and mobile computing platforms.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Verify and control/limit connections to and use of external systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Limit use of organizational portable storage devices on external systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Control CUI posted or processed on publicly accessible systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Awareness and Training

* + 1. Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Provide security awareness training on recognizing and reporting potential indicators of insider threat.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Audit and Accountability

* + 1. Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Review and update logged events.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Alert in the event of an audit logging process failure.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Provide audit record reduction and report generation to support on-demand analysis and reporting.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Limit management of audit logging functionality to a subset of privileged users.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Configuration Management

* + 1. Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Establish and enforce security configuration settings for information technology products employed in organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Track, review, approve or disapprove, and log changes to organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Analyze the security impact of changes prior to implementation.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Control and monitor user-installed software.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Identification and Authentication

* + 1. Identify system users, processes acting on behalf of users, and devices.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Prevent reuse of identifiers for a defined period.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Disable identifiers after a defined period of inactivity.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Enforce a minimum password complexity and change of characters when new passwords are created.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Prohibit password reuse for a specified number of generations.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Allow temporary password use for system logons with an immediate change to a permanent password.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Store and transmit only cryptographically-protected passwords.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Obscure feedback of authentication information.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Incident Response

* + 1. Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Test the organizational incident response capability

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Maintenance

* + 1. Perform maintenance on organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Ensure equipment removed for off-site maintenance is sanitized of any CUI.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Supervise the maintenance activities of maintenance personnel without required access authorization.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Media Protection

* + 1. Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Limit access to CUI on system media to authorized users.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Sanitize or destroy system media containing CUI before disposal or release for reuse.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Mark media with necessary CUI markings and distribution limitations.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Control the use of removable media on system components.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Prohibit the use of portable storage devices when such devices have no identifiable owner.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Protect the confidentiality of backup CUI at storage locations.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Personnel Security

* + 1. Screen individuals prior to authorizing access to organizational systems containing CUI.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Physical Protection

* + 1. Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Protect and monitor the physical facility and support infrastructure for organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Escort visitors and monitor visitor activity.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Maintain audit logs of physical access.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Control and manage physical access devices.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Enforce safeguarding measures for CUI at alternate work sites.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Risk Assessment

* + 1. Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Remediate vulnerabilities in accordance with risk assessments.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## Security Assessment

* + 1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## System and Communications Protection

* + 1. Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Separate user functionality from system management functionality.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Prevent unauthorized and unintended information transfer via shared system resources.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Establish and manage cryptographic keys for cryptography employed in organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Prohibit remote activationof collaborative computing devices and provide indication of devices in use to users present at the device.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Control and monitor the use of mobile code.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Protect the authenticity of communications sessions.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Protect the confidentiality of CUI at rest.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

## System and Information Integrity

* + 1. Identify, report, and correct system flaws in a timely manner.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Provide protection from malicious code at designated locations within organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Monitor system security alerts and advisories and take action in response.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Update malicious code protection mechanisms when new releases are available.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

* + 1. Identify unauthorized use of organizational systems.

|  |  |  |
| --- | --- | --- |
| Implemented | Planned to be Implemented | Not Applicable |
| **Current implementation or planned implementation details. If “Not Applicable,” provide rationale.** | | |

# **INCIDENT RESPONSE PLAN**

## Incident Phases

The incident response process has several phases. The initial phase involves establishing and training an incident response team, and acquiring the necessary tools and resources. During preparation, the organization also attempts to limit the number of incidents that will occur by selecting and implementing a set of controls based on the results of risk assessments. However, residual risk will inevitably persist after controls are implemented. Detection of security breaches is thus necessary to alert the organization whenever incidents occur. In keeping with the severity of the incident, the organization can mitigate the impact of the incident by containing it and ultimately recovering from it. During this phase, activity often cycles back to detection and analysis—for example, to see if additional hosts are infected by malware while eradicating a malware incident. After the incident is adequately handled, the organization issues a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents.

### **Prepare**

Preparation includes those activities that enable [COMPANY\_NAME] to respond to an incident. These include a variety of policies, procedures, tools, as well as governance and communications plans.

* + - * 1. **Communication**

Initial communication to affected stakeholders should occur as expeditiously as possible upon the identification of the incident. In some cases, this may include an initial communication (letter, email, phone call) that simply states that [COMPANY\_NAME] is aware of the issue and is addressing it, with the promise of a follow up.

Should the unauthorized release of customer data occur, [COMPANY\_NAME] shall notify the customer affected by the release in the most expedient way possible.

Updated communications will come from the Incident Response Manager. As staff receive requests from districts for information, they should pass those requests along to the Incident Response Manager.

Staff should be clearly informed by the [DESIGNATED\_POC] what information is public and what is internal/confidential. However, company leadership should be aware that any material or information communicated to staff can and likely will be shared with the public, including the news media.

Communication with news media will be initiated by [DESIGNATED\_POC] and/or designee. Incoming news media calls and requests for information will be directed through Incident Response Team Communication Specialist. A communication response plan (talking points, interview refusal statement, etc.) will be formulated as needed, with information coming from [DESIGNATED\_POC] or designee.

* **Incident Response Manager**

|  |  |
| --- | --- |
| Name: |  |
| Work Phone: |  |
| Mobile Phone: |  |
| e-Mail Address: |  |

* **Technical Contacts**

|  |  |
| --- | --- |
| Name: |  |
| Work Phone: |  |
| Mobile Phone: |  |
| e-Mail Address: |  |

* **Legal Counsel**

|  |  |
| --- | --- |
| Name: |  |
| Work Phone: |  |
| Mobile Phone: |  |
| e-Mail Address: |  |

* **Communications Specialist**

|  |  |
| --- | --- |
| Name: |  |
| Work Phone: |  |
| Mobile Phone: |  |
| e-Mail Address: |  |

* + - * 1. **Incident Tipping Mechanisms**

All [COMPANY\_NAME] staff have a responsibility to remain vigilant and protect the data stored within the systems we support. Any event that threatens the confidentiality, integrity or availability of the information resources we support or utilize internally should immediately be reported to a supervisor or the Incident Response Manager if a supervisor is unavailable. Supervisors should immediately bring the incident to the attention of the Incident Response Manager.

### **Detection and Analysis**

* + - * 1. **Detection**

Detection is the discovery of an event with security tools or through notification by an inside or outside party about a suspected incident. The detection of an incident requires the immediate activation of the IRT as listed in paragraph 6.1.1.1. The determination of a security incident can arise from one or several circumstances simultaneously. Means by which detection could occur include:

* Trained personnel reviewing collected event data for evidence of compromise.
* Software applications analyzing events, trends, and patterns of behavior.
* Intrusion Protection/Intrusion Detection devices alerting to unusual network or port traffic.
* The observation of suspicious or anomalous activity within a [COMPANY\_NAME] facility or on a computer system.

It is critical in this phase:

* To detect whether a security incident has occurred.
* To determine the method of attack.
* To determine the impact of the incident to the mission, systems, and personnel involved in the incident.
* To obtain or create intelligence products regarding attack modes and methods.
  + - * 1. **Analysis**

Analysis of the incident indicators will be performed in a manner consistent with the type of incident. In the event of a physical incident, appropriate steps will be taken to determine weaknesses in either the physical security of the facility, its monitoring tools, or its training programs to assess areas for process improvement or change. For an electronic incident, [COMPANY\_NAME] will utilize [DEFINE WHO IS REQUIRED] to perform static and dynamic analysis of malicious code, a review of information system boundary protections, determination of source code if applicable, the depth and breadth of the attack, if the attack has migrated to other systems on or off the network, and any other tasks appropriate to the type of incident experienced. These analyses can be performed either manually or utilizing automated tools dependent upon the situation, timeliness, and availability of resources.

* + - * 1. **Categorization**

An incident will be categorized as one of four severity levels. These severity levels are based on the impact to [COMPANY\_NAME] and can be expressed in terms of financial impact, impact to services and/or performance of our mission functions, impact to [COMPANY\_NAME] image, or impact to trust by [COMPANY\_NAME] customers etc. The below table provides a listing of the severity levels and a definition of each severity level.

|  |  |
| --- | --- |
| Severity Level | Description |
| Low | Incident where the impact is minimal. Examples may be e-mail SPAM,  isolated virus infections, etc. |
| Medium | Incident where the impact is significant. Examples may be a delayed or  limited ability to provide services, meet [COMPANY\_NAME]  mission, delayed delivery of critical electronic mail or data transfers, etc. |
| High | Incident where the impact is severe. Examples may be a disruption to the  services and/or performance of our mission functions. [COMPANY\_NAME] proprietary or confidential information has been  compromised, a virus or worm has become widespread and is affecting  over 1 percent of employees, Pubic Safety systems are unavailable, or [COMPANY\_NAME] Executive management has been notified. |
| Extreme | Incident where the impact is catastrophic. Examples may be a shutdown of  all [COMPANY\_NAME] network services. [COMPANY\_NAME] proprietary or confidential information has been  compromised and published in/on a public venue or site. Public safety  systems are unavailable. Executive management must make a public  statement. |

* + - * 1. **Reporting**

In the event of a cybersecurity incident, [COMPANY\_NAME] must report the incident to the DoD within 72 hours via <https://dibnet.dod.mil/>

Upon receipt of a cyber incident report

* DoD Cyber Crime Center (DC3) sends the report to the contracting officer(s)
* The contracting officer(s) provides the report to the requiring activities
* DC3 analyzes report to identify cyber threat vectors and adversary trends
* DCS contacts the reporting company if the report is incomplete

In the event that a subcontractor experiences a cybersecurity incident, they must report it to you, or to the next highest tier of subcontractor, and present the evidence as required. As the prime contractor, you’re then required to report the incident to the DoD and submit the evidence, as detailed above.

### **Containment, Eradication, And Recovery**

[INSERT NAME, TITLE, AND CONTACT INFORMATION] is responsible for containment and will document all containment activities during an incident.

Containment activities for security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. This requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

* + - 1. **Eradication**

[INSERT NAME, TITLE, AND CONTACT INFORMATION] is responsible for eradication and will document all eradication activities during an incident.

Eradication efforts for a security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

* + - 1. **Recovery**

[INSERT NAME, TITLE, AND CONTACT INFORMATION] is responsible for recovery and will document all recovery activities during an incident.

Recovery efforts for incidents will involve the restoration of affected systems to normal operation. This is dependent upon the type of incident experienced but may include actions such as restoring systems from backups, rebuilding systems from an agency approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

### **Post-Incident Activity**

[INSERT NAME, TITLE, AND CONTACT INFORMATION] is responsible for documenting and communicating post-incident activity.

Post-incident activities will occur after the detection, analysis, containment, eradication, and recovery from a security incident. One of the most important phases of incident response, post -incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Important items to be reviewed and considered for documentation are:

• Exactly what happened, and at what times?

• How well did staff and management perform in dealing with the incident?

• What information was needed sooner?

• Were any steps or actions taken that might have inhibited the recovery?

• What should be done differently the next time a similar incident occurs?

• How could information sharing with other organizations have been improved?

• What corrective actions can prevent similar actions in the future?

• What precursors or indicators should be watched for in the future to detect similar incidents?

• What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Post-incident activities will be incorporated into future training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

## Incident Handling Checklist

1. The person who discovers the incident will [enter action to be performed]. List possible sources of those who may discover the incident. The known sources should be provided with a contact procedure and contact list. Sources requiring contact information may be:
   1. Helpdesk.
   2. IT Manager.
   3. [OTHER CONTACTS AS DETERMINED TO BE APPROPRIATE FOR YOUR AGENCY]

List all sources and check off whether they have contact information and procedures. Usually each source would contact one 24/7 reachable entity such as a grounds security office. Those in the IT department may have different contact procedures than those outside the IT department.

1. If the person discovering the incident is a member of the IT department or affected department, they will proceed to step four.
2. The Helpdesk/manager/IT Staff will refer to the IT emergency contact list or effected department contact list and call the designated numbers in order on the list. The Helpdesk will log:
   * 1. The name of the caller.
     2. Time of the call.
     3. Contact information about the caller.
     4. The nature of the incident.
     5. When the event was first noticed, supporting the idea that the incident occurred.
3. The IT staff member or affected department staff member who receives the call (or discovered the incident) will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The staff member will call those designated on the list. The staff member will contact the incident response manager using both email and phone messages. The staff member will log the information received in the same format as the security office in the previous step. The staff member could possibly add the following:
   * 1. Is the system affected business critical?
     2. What is the severity of the potential impact?
     3. Name of system being targeted, along with operating system, Internet Protocol (IP) address, and location.
     4. IP address and any information about the origin of the attack.
4. Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.
   * 1. Is the incident real or perceived?
     2. Is the incident still in progress?
     3. What data or property is threatened and how critical is it?
     4. What is the impact on the business should the attack succeed? Minimal, serious, or critical?
     5. What system or systems are targeted, where are they located physically and on the network?
     6. Is the incident inside the trusted network?
     7. Is the response urgent?
     8. Can the incident be quickly contained?
     9. Will the response alert the attacker and do we care?
     10. What type of incident is this? Example: virus, worm, intrusion, abuse, damage.
5. An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:
   * 1. Category one - A threat to public safety or life.
     2. Category two - A threat to sensitive data.
     3. Category three - A threat to computer systems.
     4. Category four - A disruption of services.
6. Team members will establish and follow one of the following procedures basing their response on the incident assessment:
   * 1. Worm response procedure.
     2. Virus response procedure.
     3. System failure procedure.
     4. Active intrusion response procedure - Is critical or sensitive data (Personally Identifiable Information (PII), CJI, etc.) at risk?
     5. Inactive Intrusion response procedure.
     6. System abuse procedure.
     7. Property theft response procedure.
     8. Website denial of service response procedure.
     9. Database or file denial of service response procedure.
     10. Spyware response procedure.

The team may create additional procedures which are not foreseen in this document. If there is no applicable procedure in place, the team must document what was done and later establish a procedure for the incident.

1. Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.
2. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.
3. Upon management approval, the changes will be implemented.
4. Team members will restore the affected system(s) to the uninfected state. They may do any or more of the following:
   * 1. Reinstall the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
     2. Make users change passwords if passwords may have been sniffed.
     3. Be sure the system has been hardened by turning off or uninstalling unused services.
     4. Be sure the system is fully patched.
     5. Be sure real time virus protection and intrusion detection is running.
     6. Be sure the system is logging the correct events and to the proper level.
5. Documentation—the following shall be documented:
   * 1. How the incident was discovered.
     2. The category of the incident.
     3. How the incident occurred, whether through email, firewall, etc.
     4. Where the attack came from, such as IP addresses and other related information about the attacker.
     5. What the response plan was.
     6. What was done in response?
     7. Whether the response was effective.
6. Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond, in case of an appeal.
7. Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible. List the agencies and contact numbers here.
8. In the event of a loss or suspected loss of criminal justice information, contact [LAW\_ENFORCEMENT\_CONTACT]
9. Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
10. Review response and update policies—plan and take preventative steps so the intrusion can't happen again.
    * 1. Consider whether an additional policy could have prevented the intrusion.
      2. Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
      3. Was the incident response appropriate? How could it be improved?
      4. Was every appropriate party informed in a timely manner?
      5. Were the incident response procedures detailed, and did they cover the entire situation? How can they be improved?
      6. Have changes been made to prevent a reinfection? Have all systems been patched, systems locked down, passwords changed, antivirus updated, email policies set, etc.?
      7. Have changes been made to prevent a new and similar infection?
      8. Should any security policies be updated?
      9. What lessons have been learned from this experience?

# **APPENDIX A - INVENTORY**



# **APPENDIX B - REFERENCES**

NIST 800-61 – Computer Security Incident Handling Guide

NIST 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations

NIST 800-171 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

DFARs Clause 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting

# **APPENDIX C - RECORD OF CHANGES**

|  |  |  |
| --- | --- | --- |
| **Date** | **Description** | **Made By:** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |