**Server Configuration Procedure**

**COMPANY NAME**

**Version #**

**Last Revision Date:**

Document Classification

**Table of Contents**

[1.0 - System Identification 3](#_Toc46816869)

[1.1 - System Name 3](#_Toc46816870)

[1.2 - System Categorization 3](#_Toc46816871)

[1.3 – Responsible Organization 3](#_Toc46816872)

[1.4 – System Roles & Responsibilities 3](#_Toc46816873)

[1.5 - Contracts Containing CUI 4](#_Toc46816874)

[2.0 - System Environment & Boundaries 4](#_Toc46816875)

[2.1 - General Description / Purpose of System 4](#_Toc46816876)

[2.2 - Operating / Hosting Model 4](#_Toc46816877)

[2.3 - System Environment Overview 5](#_Toc46816878)

[2.4 - System Components (Hardware / Software) 5](#_Toc46816879)

[2.5 - System / Network Boundaries 5](#_Toc46816880)

[2.6 - High-Level System Architecture Diagram 5](#_Toc46816881)

[2.7 - System Life Cycle (SDLC) 5](#_Toc46816882)

[3.0 - Security Requirements 6](#_Toc46816883)

[3.1 – Security Requirements 6](#_Toc46816884)

**Procedure Information**

|  |  |
| --- | --- |
| **Prepared By** | |
| **Name:** |  |
| **Department / Title:** |  |
| **Email Address:** |  |
| **Phone #:** |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Description** | **Pages Affected** |
| 1.0 | [DATE] | Initial version of procedure | All |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Policy Requirement Reference

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Description / Requirement** | **NIST 800-53** |
| **3.3.1** | Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. | AU-2 AU-3 AU-3(1) Au-6 AU-12 |
| **3.3.9** | Limit management of audit functionality to a subset of privileged users. | AU-9(4) |
| **3.4.1** | Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. | CM-2 CM-6 CM-8 CM-8(1) |
| **3.4.2** | Establish and enforce security configuration settings for information technology products employed in organizational information systems. | CM-2 CM-6 |
| **3.4.3** | Track, review, approve/disapprove, and audit changes to information systems. | CM-3 |
| **3.4.4** | Analyze the security impact of changes prior to implementation. | CM-4 |
| **3.4.6** | Employ the principle of least functionality by configuring the information system to provide only essential capabilities. | CM-7 |
| **3.4.7** | Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services. | CM-7(1) CM-7(2) |
| **3.4.9** | Control and monitor user-installed software. | CM-11 |
| **3.5.10** | Store and transmit only cryptographically-protected passwords. | IA-5(1) |
| **3.8.7** | Control the use of removable media on information system components. | MP-7 |
| **3.13.13** | Control and monitor the use of mobile code. | SC-18 |
| **3.13.15** | Protect the authenticity of communications sessions. | SC-23 |
| **3.13.16** | Protect the confidentiality of CUI at rest. | SC-28 |

Procedure

Reference: [NIST 800-128](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf)

The system administrator:

1. Uses vendor recommended settings and industry-recognized secure practices to ensure baseline system hardening configuration for all servers comply with applicable legal, statutory, and regulatory compliance
2. Where technically feasible, technology platforms algin with industry-recommended hardening recommendations including Defense Information Systems Agency (DISA) Secure Technical Implementation Guides (STIGs) or Original Equipment Manufacturer (OEM) security configuration guides.
3. Ensures that system hardening includes but is not limited to:
   1. Enforcing least functionality, which includes but is not limited to:
      1. Allowing only necessary and secure services, protocols, and daemons;
      2. Removing all unnecessary functionality, which includes but is not limited to:
         1. Scripts;
         2. Drivers;
         3. Features;
         4. Subsystems;
         5. File systems; and
         6. Unnecessary web servers.
   2. Configuring and documenting only the necessary ports, protocols, and services to meet business needs;
   3. Implementing security features for any required services, protocols or daemons that are considered to be insecure, which includes but is not limited to using secured technologies such as Secure Shell (SSH), Secure File Transfer Protocol (S‐FTP), Transport Layer Security (TLS), or IPSec VPN to protect insecure services such as NetBIOS, file‐sharing, Telnet, and FTP;
   4. Storing and transmitting only cryptographically-protected passwords;
   5. Installing and configuring appropriate technical controls, such as:
      1. Antimalware;
      2. Software firewall;
      3. Event logging; and
      4. File Integrity Monitoring (FIM), as required; and
   6. Enforce least privileges, in particular limit the management of logging to a small subset of privileged users
   7. Protect the confidentiality of data at rest if the data is CUI;
   8. Limit the use of removable media; and
   9. As applicable, implementing only one primary function per server to prevent functions that require different security levels from co‐existing on the same server (e.g., web servers, database servers, and DNS should be implemented on separate servers).
4. Documents and validates security parameters are configured to prevent misuse
5. Follows documented change control that includes the following:
   1. A review and approval of proposed changes with explicit consideration for the security impact, end-user impact, and associated business reason;
   2. Documentation of configuration change decisions
   3. Documentation of test plans, test results, and associated approvals for all required testing
   4. Clear segregation of duties between development and production environments, with developers having no access to production resources.
6. In the case of an emergency, change requests, testing artifacts, and all approvals must be documented after-the-fact and maintained, including a formal post-implementation review.
7. Validates and refreshes configurations on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors. Unless a technical or business reason exists, standardized images are used to represent hardened versions of the underlying operating system and the applications installed on the system.
8. On at least an annual basis, during the 2nd quarter of the calendar year, reviews the process for non‐conforming instances.
9. As needed, revises processes to address necessary changes and evolving conditions. Whenever the process is updated:
   1. Distributes copies of the change to key personnel; and
   2. Communicates the changes and updates to key personnel.
10. If necessary, requests corrective action to address identified deficiencies.
11. If necessary, validates corrective action occurred to appropriately remediate deficiencies.
12. If necessary, documents the results of corrective action and notes findings.
13. If necessary, requests additional corrective action to address un-remediated deficiencies.