[Company Name] Configuration Management Plan

Official Policy Title:	
Responsible Party:	
Approval Party:	
Effective Date:	
Last Update:	
Version Number:	
Policy Framework:	**Developed in accordance with NIST Special Publication (SP) 800 Series - https://csrc.nist.gov/publications/sp800 (NIST SP 800-53, rev. 5)**
Mapping	**(1). NIST SP 800-53, rev. 5 [NIST CM-9]**

Introduction

The Configuration Management Plan referenced within this document defines the security measures to be implemented by [company name] that strive to ensure the Confidentiality, Integrity, and Availability (CIA) of information systems. Additionally, the Configuration Management Plan is to be developed by personnel with the appropriate knowledge and skill sets, documented accordingly with all necessary policy and procedural statements, and disseminated to all in-scope personnel within the organization. The Configuration Management Plan is to be reviewed and updated [annually, or other designated time frame] by a responsible party at [company name].

Purpose

The purpose of the Configuration Management Plan is to outline the organization's objectives relating to implementing, establishing, maintaining, recording, and effectively monitoring secure configurations to an organization's overall information system's landscape, including, but not limited to the following information systems: network devices, operating systems, applications, internally developed software and systems, and other relevant hardware and software platforms.

Scope

This policy document encompasses information systems that store, process, and transmit information for [company name]. Please note, for purposes of this document, an "information system" is defined as the following: *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.* Additionally, a "user" is defined as the following: *Individual or (system) process authorized to access an information system.*

Policy

The following policy statements, rules, and assertions have been formally adopted by [company name]. Additionally, for any procedural requirements, they are to be documented as necessary within this policy, or within a separate set of standard operating procedures (SOP), as needed.

CONFIGURATION MANAGEMENT PLANNING

Scope Considerations
[company name] defines configuration management as practices utilized for ***implementing, establishing, maintaining, recording, and effectively monitoring*** secure configurations to the organization's overall information system's landscape. Specifically, this includes all network devices, operating systems, applications, internally developed software and systems, and other relevant hardware and software platforms. If any specific systems, because of size or complexity challenges, ultimately require their own independent configuration management program, they are to be developed accordingly by authorized personnel, and must abide by the practices as stated herein.

As such, [company name] is to develop, document, and implement a configuration management plan that consists of the following:

- Addresses roles, responsibilities, and configuration management processes and procedures.
- Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items.
- Defines the configuration items for the information system and places the configuration items under configuration management.
- Protects the configuration management plan from unauthorized disclosure and modification.

Roles and Responsibilities
The following roles and responsibilities are to be developed and subsequently assigned to authorized personnel within [company name] regarding configuration management practices:

- **Chief Technology Officer (CTO) | Chief Information Officer (CIO) | Chief Information Security Officer (CISO):** Responsibilities include providing overall direction, guidance, leadership, and support for the entire information systems configuration management program, while also assisting other applicable personnel in their day-to-day operations. The CTO | CIO | CISO is to report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture, which includes configuration management.

- **Director of Information Technology | Senior Information Security Officer**: Responsibilities include researching and developing information security configuration standards for all in-scope information systems. This will require extensive identification of industry benchmarks, standards, and frameworks that can be effectively utilized by [company name] for provisioning, hardening, securing, and locking-down such resources. After the research of such standards, the senior security officer is to then develop and establish a series of baseline configuration standards to include, but not limited to, the following information systems: network devices, operating systems, applications, internally developed software and systems, and other relevant hardware and software platforms. Because baseline configuration can and will change, this authorized individual is to also update the applicable configurations, documenting all modifications and enhancements as required.

- **Network Engineer | Systems Administrator:** Responsibilities include implementing the baseline configuration standards for all in-scope information systems. This requires obtaining a current and accurate asset inventory of all such systems, assessing their initial posture with the stated baseline, and then undertaking the necessary configurations. Because of the complexities and depth often involved with such activities, numerous personnel designated as Network Engineers | System Administrators are often involved in such activities.

  Furthermore, these individuals are also responsible for monitoring compliance with the stated baseline configuration standards, reporting to senior authorities' instances of non-compliance and efforts undertaken to correct such issues. Additionally, because these individuals are to undertake the majority of the operational and technical procedures for [company name]'s information configuration management plan, it is critical to highlight other relevant CM duties, such as the following:

  - Assessing and analyzing baseline configuration standards for ensuring they meet the intent and rigor of [company name]'s intent for the safety and security (both logically and physically) of critical information systems.
  - Ensuring the asset inventory for all in-scope information systems is in fact kept current and accurate.
  - Ensuring that network topology documents are also kept current and accurate.
  - Facilitating requests for validation of [company name]'s baseline configurations for purposes of regulatory compliance assessments and audits – such as those for PCI compliance, AICPA SOC reporting, HIPAA, FISMA, GLBA, etc.
  - Continuous training and certification accreditation for the purpose of maintaining an acceptable level of information security expertise necessary for configuration management.

- **Software Developers | Coders:** Responsibilities include developing secure systems by implementing the required baseline configuration standards into all systems and software development lifecycle activities. Coding for security, not functionality, is a core theme for which all [company name] software developers/coders are to adhere to. They are to also identify any other necessary baseline configuration standards when warranted. Ultimately, this requires removing, disabling, and not implementing insecure services, protocols, or ports that – while may be conducive for purposes of ease-of-use – ultimately compromise the applicable systems being developed.

Additionally, these personnel are also responsible for following a structured project management framework, one that includes utilizing a documented SDLC process, complete with well-defined change management policies, procedures, and processes. The [company name] change management policy and procedure document outlines critical practices regarding such changes, for which software developers/coders are to adhere to at all times. Moreover, these personnel are to support and coordinate all required requests for validation of the baseline configurations within their systems being developed for purposes of regulatory compliance and/or internal audit assessments.

- **Change Management | Change Control Personnel:** Responsibilities include reviewing, approving, and/or denying all changes to critical information systems and specifically for purposes of any changes to the various baseline configuration standards. While changes are often associated with user functionality, many times the issue of vulnerability, patch, and configuration management are brought to light with change requests. In such cases, authorized change management/change control personnel are to extensively analyze and assess these issues for ensuring the safety and security of [company name] information systems.

- **End Users:** Responsibilities include adhering to the baseline configuration standards and not undertaking any measures to alter such standards on any such [company name] information systems. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impact the safety and security of [company name] information systems and are to also report such instances immediately to senior authorities.

- **Vendors, Contractors, Other Third-Party Entities:** Responsibilities for such individuals and organizations are much like those stated for end users: adhering to the baseline configuration standards, not undertaking any measures to alter such standards on any such [company name] information systems, while also reporting instances of non-compliance.

Training Requirements

Configuration Management is a vast, complex, and challenging task, one that requires thoughtful decision making, necessary skills, along with a sincere commitment for ensuring the confidentiality, integrity, and availability (CIA) of [company name]'s information systems landscape. As such, all employees, and relevant users of [company name] information systems are to receive the required and necessary training for undertaking their roles and responsibilities for configuration management. Training varies by personnel but is to include all measures for ensuring employees and users stay abreast of significant issues affecting configuration management.

For technical personnel, such as Network Engineers, System Administrators, Software Developers, and coders, this means continuous professional training, such as continuing education for existing I.T. certifications, along with goals of obtaining additional certifications and/or designations. Moreover, it also means subscribing to industry leading security bulletins online, hard copy publications, etc.

For end users, vendors, contractors, and other third parties, this means acknowledging [company name]'s acceptable use policies regarding systems resources. Additionally, it also entails not altering any systems for which access has been granted.

Automated Tools and Software Usage

Authorized personnel are to identify, assess, and select specific software tools and related utilities for aiding and facilitating all aspects of [company name]'s configuration management plan. This entails extensive research into all possible configuration management tools for ensuring interoperability and compatibility with all in-scope information systems, while also ensuring such tools always have appropriate end-user technical and operational support. The use of automated tools for configuration management is a necessity as the size, complexity, and scale of [company name] information systems continue to grow and expand. Additionally, the tools utilized by [company name] should also be evaluated for the following:

- The ability to effectively obtain data from a vast amount of various information systems, from the network level to the host level.
- Using standard specifications for aiding and facilitating the configuration of information systems.
- The ability to meet and/or exceed mandates and requirements with any applicable regulatory compliance provisions.
- Comprehensive reporting features, such as system settings on applicable information systems, reporting of violations/non-compliance, and other feature-rich reporting.

Additionally, because many of these automated tools are software applications, the following measures are to be in place regarding software utilized by [company name]:

- The software and its associated documentation is to be used in accordance with contract agreements and copyright laws.
- The use of software and its associated documentation is to be tracked accordingly for ensuring its protection regarding copying and distribution, whereby no unauthorized distribution, display, performance, or reproduction of the software itself is undertaken.
- Additional detail can be found within [company name]'s software usage policy and procedures.

Lastly, if users have been provided the privilege of installing software, then they are to adhere to the stated software usage policy and procedures as documented by [company name].

Configuration Management Tool	Description and Purpose of Tool
Puppet Configuration Management Tool - http://bit.ly/2ikcfFw	Configuration management tool for providing as-needed updates to all information systems on a scheduled basis.

Security Posture
Security posture is the establishment of a minimum acceptable level of security for [company name]'s information systems landscape and all critical information systems. This requires authorized I.T. personnel to determine a variety of factors, most importantly the following: The minimum agreed upon security settings for ensuring a risk level as low as possible, yet one that still allows the organization to function in an efficient and effective manner, from an operational perspective.

Baseline Configuration Standards
Authorized I.T. personnel are to identify baseline configuration standards for information systems, which is available from a number of well-known benchmarks, frameworks, associations, along with vendor specific guides. Developed by experienced and competent information security specialists, baseline configuration standards enforce the provisions set forth in [company name]'s security posture – the minimum acceptable level of security necessary for ensuring the confidentiality, integrity, and availability (CIA) of critical information systems. As such, [company name] is to utilize specific hardening guidelines, including, but not limited to, the following:

- SANS
- NIST SP 800 Publications
- United States Computer Emergency Readiness Team (US-CERT)
- National Security Agency (NSA) hardening documents.
- CIS Security Benchmarks Division
- OWASP
- Vendor specific hardening guidelines
- MITRE community driven information security consortiums

Configuration Standards Source	Description of Source Document	Scope of Information Systems
Palo Alto Firewall Admin Guide at http://bit.ly/2ikdUeu	Used for applying baseline configuration standards to Palo Alto Firewalls.	Palo Alto Firewalls in production environment
?	?	?
?	?	?

The provisioning and hardening guidelines are to allow [company name] to establish, at a minimum, the following baseline configuration standards for information systems:

- Secure services – those that are operating system (O/S) and application specific to all major operating systems (Windows, UNIX, Linux) and applications (i.e., web server applications, database applications, internally developed applications)
- Secure protocols, such as SSL, SSH, VPN, etc.

- Secure ports, such as 443, 22, etc.
- User access principles, such as Role Based Access Controls (RBAC), etc.
- Username and password parameters, such as unique user ID's, password complexity rules, password aging rules, account lockout thresholds, etc.
- Encryption
- Event monitoring
- Configuration and change monitoring
- Performance and utilization monitoring
- Logging and reporting

Insecure Services, Ports, Protocols
All security posture assessment and baseline configuration standards are to not allow the passing of usernames and passwords, along with sensitive data, over a network unencrypted.

Specifically, the use of FTP, Telnet, HTTP is to be disabled for such systems that store, process, and/or transmit usernames, passwords, and other types of sensitive or confidential information. For all in-scope information systems, insecure service, ports, and protocols are to be readily identified by authorized I.T. personnel, which means having a strong technical understanding of all relevant network devices (i.e., firewalls, routers, switches, load balancers, etc.), operating systems (i.e., Windows, UNIX, Linux), and applications (i.e., web server applications, database applications), etc.

By implementing baseline configuration standards – the practices used for ensuring proper provisioning and hardening initiatives are in place – [Company name] is also adhering to the concept of "Least Functionality" for information systems. While "Least Functionality" is often referenced in terms of access control and access rights – for which Role Based Access Control (RBAC) is utilized, it also applies to removing unnecessary, insecure, and default accounts, ports, protocols, and services for [company name] information systems.

Review and Update of Baseline Configurations
Authorized personnel within [company name] are to review and update baseline configurations of information systems [monthly, quarterly, every six-months, annually], and when specifically required to do so because of mandated compliance mandates, information security best practices, management directives, and when undertaking installs and upgrades to information systems.

Automated Mechanisms for Baseline Configurations
[Company name] is to employ automated mechanisms for aiding and facilitating baseline configurations to information systems. Such automated mechanisms are to include, but are not limited to, the following:

- Hardware and software inventory tools
- Configuration management tools
- Network management tools

Retention of Previous Baseline Configurations
[Company name] is to retain previous versions of baseline configurations of the information system to support rollback, if necessary. Network attacks, natural disasters, and many other unforeseen hazards

could ultimately result in the physical destruction of the information system and all supporting systems, thus the need for maintaining previous baseline configurations is essential. Such configurations should be stored in a different physical location than that of the core production environment for purposes of contingency planning.

Baseline Configurations for High-Risk Areas

If, at any time, employees, contractors, or any other in-scope personnel will be physically located in an area deemed "High Risk", then additional security precautions are to be applied for ensuring the safety and security of such individuals, along with their relevant information systems for which they have in their possession. Specifically, any location for which a lack of physical security controls exists to adequately protect individuals and their information systems will thus result in the area identified as "High Risk." The following baseline configurations are to be applied to information systems that may enter an area identified as "High Risk."

Type of Information System	Possible Threat	Baseline Configurations for High Risk
Laptops, Tablets	Unauthorized access and theft of device	Full disk encryption and the use of enhanced username and password complexity rules.
Cellular Phones		
?		
?		

Least Functionality

[Company name] information systems are to be configured for providing only essential capabilities, while removing all unnecessary services, ports, and protocols. Baseline configuration standards provided by various sources are to provide additional guidance and recommendations on how to implement "least functionality" for all systems.

Periodic Review

[Company name] is to review the information system [defined frequency] for purposes of identifying any unnecessary and/or non-secure functions, ports, protocols, and services, and disabling such services as necessary. The review process is to be conducted by authorized I.T. personnel, with the results of the review formally documented.

Prevention of Program Execution

The information system is to prevent program execution in accordance with [company name] policies and procedures regarding the use of software.

Authorized Software and Whitelisting

[Company name] is to identify software programs authorized to execute on the information system, employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system, and to review and update the list of authorized software programs on a [define the frequency] basis.

Asset Inventory

The success of one's configuration management initiatives is highly dependent on identifying all in-scope information systems, which ultimately entails having a comprehensive asset inventory list in place.

Additionally, the asset inventory list is to be updated when components are installed and removed, as this helps ensure the overall accuracy of the list. While tools may be used to help automate the process of maintaining the asset inventory list, authorized personnel must strive to keep the list accurate to the extent feasible, which is to also include manual processes.

Moreover, the asset inventory list is to also include the names of individuals who are responsible and accountable for each component. Lastly, authorized personnel within [company name] are to verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories. Therefore, [company name] is to identify all applicable unique identifiers and necessary data elements for successfully tracking and managing such inventory.

Unauthorized Component Detection
[Company name] is to employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware within the information system, and to then take appropriate action when unauthorized components are detected. The following automated mechanisms are used: [Discuss what tools are used]. Additionally, the following response procedures are to be enacted when such unauthorized components are found on the network: [Discuss what steps to take].

Access Control for Changes
Access control is a vital element of one's configuration management practices, and it requires that only authorized individuals within [company name] have appropriate access to the actual systems being configured, along with the tools being utilized for configuration management itself. While end-users are provisioned and de-provisioned according to [company name]'s access control policies and procedures, additional emphasis is to be placed on the following personnel responsible for administering, maintaining, and monitoring the entire configuration management program itself:

- Network engineers, systems administrators, and other related personnel
- Software developers, coders, and other related personnel
- Change management and change control personnel, and other related personnel.

Moreover, because many of the software tools for configuration management provide rich reporting capabilities, often detailing sensitive and highly confidential information, such reporting metrics and deliverables are to be highly restricted.

Additionally, physical access to information systems that control the ability to make configuration changes are to be limited to authorized personnel only. As such, internal computer rooms, third—party data centers, co-location entities, and other facilities are only to be accessed by authorized personnel – no exceptions.

Access Enforcement
Access to information systems that support configuration management – and to the facilities where such information systems are located – is to be enforced with all necessary identification and authentication procedures utilizing necessary access protocols, such as Role Based Access Control (RBAC) within directory services that enforce access restrictions and support auditing of the enforcement actions themselves.

Reviewing System Changes
[Company name] is to review information system changes as needed to determine whether unauthorized changes have occurred.

Signed Components
[Company name] is to ensure that the information system prevents the installation of software and firmware without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.