1. Purpose
<Organization Name> <Insert Organization Mission Here>. This policy establishes the Enterprise Configuration Management Policy, for managing risks from system changes impacting baseline configuration settings, system configuration and security. The configuration management program helps <Organization Name> document, authorize, manage and control system changes impacting Information Systems.

2. Scope
The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by <Organization Name>. Any information, not specifically identified as the property of other parties, that is transmitted or stored on <Organization Name> IT resources (including e-mail, messages and files) is the property of <Organization Name>. All users (<Organization Name> employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3. Intent
The <Organization Name> Information Security policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a configuration management capability throughout <Organization Name> and its business units for documenting, authorizing, managing, and controlling configuration changes which may occur across the enterprise environment.

4. Policy
<Organization Name> has chosen to adopt the Configuration Management principles established in NIST SP 800-53 “Configuration Management” Control Family guidelines, as the official policy for this domain. The following subsections outline the Configuration Management standards that constitute <Organization Name> policy. Each <Organization Name> Business System is then bound to this policy, and must develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- CM-1 Configuration Management Policy and Procedures: All <Organization Name> Business Systems must develop, adopt or adhere to a formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- CM-2 Baseline Configuration: All <Organization Name> Business Systems must develop, document, and maintain a current baseline configuration of their Information Systems. The baseline configuration must be reviewed and updated based on environment changes.
<table>
<thead>
<tr>
<th>Department Name</th>
<th>Policy #</th>
<th>Issue Date: September 13, 2013</th>
</tr>
</thead>
</table>

- **CM-3 Configuration Change Control:** All <Organization Name> Business Systems must perform change control for key Information Systems. This includes:
  - Determining the type of changes to the information asset that are configuration controlled.
  - Approving configuration-controlled changes to the system with explicit consideration for security impact analysis.
  - Documenting approved configuration-controlled changes to the system.
  - Retaining and reviewing records of configuration-controlled changes to the system.
  - Auditing activities associated with configuration-controlled changes to the system.
  - Coordinating and providing oversight for configuration change control activities through Change Control Board (CCB) that convenes **weekly**.

- **CM-4 Security Impact Analysis:** All <Organization Name> Business Systems must analyze changes to the Information Systems to determine potential security impacts prior to change implementation.

- **CM-5 Access Restrictions for Change:** All <Organization Name> Business Systems must define, document, approve, and enforce physical and logical access restrictions with changes to the information asset.

- **CM-6 Configuration Settings:** All <Organization Name> Business Systems must establish, document, implement and monitor mandatory configuration settings for information technology products employed within the information asset using a security configuration checklist that reflects the most restrictive mode consistent with operational requirements. In addition, any exceptions to the mandatory configuration settings within the information asset must be identified, documented, and approved prior to ongoing use.

- **CM-7 Least Functionality:** All <Organization Name> Business Systems must configure the information asset to provide only essential capabilities and specifically prohibit or restrict the use of the following functions, ports, protocols, and/or services.

- **CM-8 Information System Component Inventory:** All <Organization Name> Business Systems must develop, document, and maintain an inventory of the information asset components that exist within their area. Inventory detail must be maintained at a sufficient level for purposes of tracking and reporting.

- **CM-9 Configuration Management Plan:** All <Organization Name> Business Systems must develop, document, and implement a configuration management plan for the information asset that:
Addresses roles, responsibilities, and configuration management processes and procedures.

Defines the configuration items for the information asset and when in the system development life cycle the configuration items are placed under configuration management.

Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.
Appendix A – References

The following references illustrate public laws which have been issued on the subject of cyber security and should be used to demonstrate <Organization Name> responsibilities associated with protection of its cyber assets.


