Salisbury University

Configuration Management Policy

1. PURPOSE

Configuration management is critical to establishing an initial baseline of hardware, software, and firmware components of Enterprise information systems and subsequently controlling and maintaining an accurate inventory of any changes to those systems. The Salisbury University Information Technology (SUIT) department is committed to managing the confidentiality, integrity, and availability of their information technology (IT) networks, systems, and applications (IT Systems) by establishing and enforcing standard baselines within the Enterprise. This allows SUIT to document, authorize, manage, and control system changes while preventing deviation from the established accepted risk.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication

3. SCOPE

This policy is applicable to all information technology assets managed and supported by SUIT. Information technology assets within the purview of configuration management include systems and applications with network and enterprise configurations that manage and maintain the reliable operations and security of the device and the information processed on that device.

4. BASE POLICY AND COMPLIANCE REFERENCES

SUIT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other organizations. This policy serves as SU's authoritative adaptation of these policies with specific amendments to meet the business and operational needs of the University.

Policy References

- State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy-List.aspx

- USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

5. POLICY

Salisbury University Information Technology (SUIT) is responsible for coordinating technology asset configuration management. SUIT will establish, maintain, manage and track baseline configurations of applicable IT assets. This will assist in the protection and support of IT assets and confidential information.

5.1 Baseline Configurations

SUIT should develop, document and maintain baseline configurations for servers, endpoints and network switches/routers. Each type of asset has different requirements and relevant configuration data that should be maintained in their respective management applications in order to ensure that as new devices are installed they start with a uniform set of security settings, patches, and configuration options wherever possible. It is the responsibility of the SUIT Administrators of those systems to maintain this data in a format for each type of system that is reproducible for consistent deployments.

5.2 Configuration Management Process

SUIT is responsible for coordinating and approving changes to SUIT managed systems. Each managed system change is approved by the respective SUIT Director responsible for the system that the change will primarily affecting. If there will be significant campus impact the CIO may also be required to approve the change and the impact is communicated to the campus via email whenever possible at least one day before the change when part of a scheduled downtime.

Individual systems may define more detailed processes for change approval as necessary for the upkeep and maintenance of that particular system or where approvals outside of IT are required to authorize changes such as for PeopleSoft.

5.3 Analyze Security Impact of Configuration Changes

SUIT where possible will evaluate the security impact of significant planned configuration changes. This should consider the impact of the change as well as the associated system risk of the affected system in order to maintain existing security posture to protect confidential data. SUIT Directors can accept the associated risk of changes after considering this impact.

5.4 Restrict Access for Implementing Changes

The relevant SUIT system administrator or owner of each system should limit the ability to affect configuration changes to only those personnel who require it for their job duties. This helps ensure that only qualified individuals who are responsible for managing a system will be able to initiate significant changes within the system that would either impact availability or the security of that system.

5.5 Standardize Security-Related Configuration Settings

Security-related settings include but are not limited to: rulesets, settings for ports and protocols, directory settings, access controls and group policy objects. Where possible, SUIT will standardize the processes and procedures around the configuration of security-related settings to establish best practices and baseline configurations. These baselines should be stored in any applicable management tool used to administer the corresponding systems if available or documented as a process per section 5.1.

5.6 Manage Hardware and Software Lifecycles

Another aspect of configuration management is coordinating and establishing an asset lifecycle process. Lifecycle management addresses the issues of maintaining an asset over its estimated "shelf life" in the organization. In alignment with the mission of Salisbury University, these refresh cycles allow for long term planning and budgeting to ensure that the needs of faculty, students and staff are met.

Lifecycle management is important beyond ensuring the availability and efficiency of a system. In order to protect the data assets from degradation, data loss, failing hardware, and evolving security threats, systems must be refreshed on regular intervals. The rate of change for modern threats evolves at such a pace that the security landscape can be drastically altered over a relatively short period of years. Lifecycle management helps ensure that IT systems are replaced and maintained with updated security features to meet new and evolving security standards to protect SU assets and stakeholders. Each IT system wherever possible should have a defined refresh lifecycle to determine the budget year for replacement or retirement. SUIT is responsible for developing and maintaining the lifecycle plans for each category of system or individual system.

6. EXEMPTIONS

If an exemption from this policy is required, an SUIT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted.

7. DEFINITIONS

Term	Definition
Baseline Configuration	A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

8. ENFORCEMENT

SUIT is responsible for managing security assessments for the University according to established requirements authorized in the SUIT Security Program Policy. Any systems under the policy authority of SUIT with requirements that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.