CONFIGURATION MANAGEMENT POLICY

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: February 10, 2021
Updated: February 10, 2021

NextGen CGI, LLC Configuration Management Policy							
Effective Date:				**Document Owner:**			
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0	02/10/2021	Policy	AF	CC	02/10/2021	SGH	02/10/2021

1. Overview 2
2. Purpose 2
3. Scope 2
4. Policy 2
4.1 2
4.2 2
4.3 2
4.4 3
4.5 3
4.6 3
4.7 3
4.8 3
4.9 3
5. Audit Controls and Management 3
6. Enforcement 4
7. Distribution 4
8. Related Standards, Policies, and Processes 4
9. Related Sub controls 4
10. Definitions and Terms 4

1. Overview

Configuration management maintains the integrity of computer systems by controlling all processes that initialize, change, or monitor system configurations. Configuration management entails:

- Determining and documenting appropriate configuration settings for a system
- Conducting security impact analyses
- Managing any changes to configuration settings through a change control board

2. Purpose

This policy provides procedures and protocols supporting an effective management of configurations for all company devices and systems.

3. Scope

This policy applies to all company officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that initialize, change, or monitor any system configuration settings. It is the responsibility of all the above to familiarize themselves with this policy and ensure adequate compliance with it.

4. Policy

4.1

It is the responsibility of NextGen CGI to establish and maintain baseline configurations and inventories of organizational systems throughout their system development lifecycles.

Baseline Configuration and System Inventory should each encompass:

- Hardware
- Software
- Firmware
- Documentation

4.2

NextGen CGI should establish and enforce security configuration settings for any technology employed on NextGen CGI organizational systems.

4.3

Changes to NextGen CGI's organizational systems must be:

- Tracked
- Reviewed

- Approved/Disapproved
- Logged

4.4

NextGen CGI is responsible for analyzing the security impact of changes prior to implementation.

4.5

Any physical and logical access restrictions associated with changes to the system must be:

- Defined
- Documented
- Approved
- Enforced

4.6

NextGen CGI follows the *Least Functionality Principal*. All organizational systems are configured to provide only essential capabilities.

4.7

NextGen CGI should either restrict, disable, or prevent the use of nonessential:

- Programs
- Functions
- Ports
- Protocols
- Services

4.8

Either:

NextGen CGI maintains a whitelisting policy to allow the execution of authorized software

4.9

NextGen CGI will control and monitor user installed software.

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy. Satisfactory examples of evidence and compliance are outlined in the Audit and Accountability Policy.

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all staff.

8. Related Standards, Policies, and Processes

- Documented Software Installation Protocol
- Baseline Configuration Standards
- Formal Change Control Procedures
- Technical and Non-Technical Review After Changes Protocol
- Policy Addressing the Implementation of one Primary Function per Server (Evidence Artifact)
- Enable Only Necessary Services, Protocols, and Daemons (Evidence Artifact)
- Policy Addressing Session Timeout
- Policy Addressing Access Restrictions for Changes to Information Systems
- Session Termination Protocol
- Documentation Outlining Mobile Code Controls
- Documented Network Disconnect Procedure

9. Related Sub controls

Control Code	Control
3.4.1	Asset Inventory and Baseline Configuration
3.4.2	Security Configuration Settings
3.4.3	Configuration Change Control
3.4.4	Security Impact Analysis
3.4.5	Access Restrictions for Changes
3.4.6	Least Functionality
3.4.7	Disable Unnecessary Components
3.4.8	Authorized Software Execution
3.4.9	User-Installed Software

10. Definitions and Terms

The following definitions are not all-inclusive and should be updated as new information is made available:

Term	Definition

Whitelisting	A process used to identify software programs that are authorized to execute on a system or authorized Universal Resource Locators (URL)/websites.
Blacklisting	A process used to identify software programs that are not authorized to execute on a system or prohibited Universal Resource Locators (URL)/websites.
Least Functionality Principle	The procedure of configuring all organizational systems to provide only essential capabilities.