SECURITY ASSESSMENT POLICY

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: 01/01/2021
Updated:

NextGen CGI, LLC Security Assessment Policy							
Effective Date:		01/01/2021		**Document Owner:**		NextGen CGI, LLC	
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0	01/01/2021	Policy	S. Hall	S. Hall	01/01/2021	S. Hall	01/01/2021

1. Overview

A security requirement assessment involves testing and/or evaluating:

- NextGen CGI, LLC management security requirements
- Operational security requirements
- Technical security requirements

These evaluations determine if requirements are:

- implemented correctly
- operating as intended

- producing the desired outcome

Additionally, a security assessment helps to determine if the implemented requirements are the best solution for the function they are intended to serve.

2. Purpose

This policy provides procedures and protocols supporting the effective management of NextGen CGI, LLC security assessments.

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

NextGen CGI periodically assesses the security controls in organizational systems to determine if the controls are effective in their application.

4.2

- RESTRICTED

4.3

System security plans that describe:

- System boundaries
- System environments of operation
- How security requirements are implemented
- The relationships/connections with/to other systems

Are periodically developed, documented, and updated. Relevant personnel should remain aware of any updates or changes.

4.4

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

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

- Policy that Outlines Contact with Special Interest Groups
- Mobile Device Policy and Procedures
- Secure System Engineering Standards
- Use of External Information Systems Procedures
- System Security Plan Diagram
- Backup Security Policy
- Personnel Security Policy

9. Related Sub controls

Control Code	Control
3.12.1	Periodic Security Assessments
3.12.2	Plan of Action and Milestones
3.12.3	Continuous Monitoring
3.12.4	System Security Plans

10. Definitions and Terms

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

Term	Definition
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in a system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.