AUDIT AND ACCOUNTABILITY POLICY

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: January 1, 2021
Updated:

NextGen CGI, LLC Audit and Accountability Control Policy							
Effective Date:				**Document Owner:**			
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

Maintaining detailed audit logs is critical to managing and tracking the chronological flow of data from sources to destinations. In instances of security and compliance, audit logs offer an official record that can provide valuable insights that are beneficial to NextGen CGI interests.

2. Purpose

This policy outlines the procedures and standards in place to ensure proper audit logs are maintained. Additionally, these logs will ensure accountability of processes and personnel by tracking privileged functions performed.

3. Scope

This policy applies to all company officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that possess, access, or manage information owned by the organization. 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 will create and retain system audit logs and records to the extent needed to enable:

- Monitoring
- Analysis
- Investigation
- Reporting

for unlawful or unauthorized system activity.

4.2

Actions of individual system users will be uniquely traced to such users to ensure they can be held accountable for their actions.

4.3

It is NextGen CGI's duty to review and update logged events. NextGen CGI will review each its log files on a daily basis, and critical errors reported by the log monitors will be immediately reviewed with the appropriate action to remediate. These will include:

A. Server and Website Security and Firewall

- LFD Log
- Messenger Log
- Web Access Log
- Web Error Log
- Modsecurity Log
- Iptables Log
- Login Log
- POP3/IMAP Log

- SMTP Auth Log
- Panel Log
- System Logs

B. Email Security and Firewall

- Message Log
- Filter Log
- Mail Log
- Reject Log
- POP3/IMAP Log
- SMTP Auth Log
- Action Log

4.4

In the event of an audit logging process failure, IT will be alerted.

- All logging process failures will require an alert to be generated.
- IT will investigate each log failure alert then cross-reference different events that may be happening at the same time across multiple hosts to find any processes that were not logged in the log where the failure occurred, in attempt to determine the most likely error(s) that caused the failure. These notations will then be placed in a log noting that the failure occurred and all associated cross-referenced log entries, to include the date and time the failure occurred.
- IT will mediate all log failures.

4.5

For the purpose of investigation and response to indications of suspicious activity, NextGen CGI will correlate data between:

- Audit record reviews
- Audit record analysis
- Audit record reporting process

4.6

NextGen CGI will provide audit record reduction and report generation to support on-demand analysis and reporting.

4.7

NextGen CGI will provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

4.8

NextGen CGI requires that audit information and audit logging tools are protected from unauthorized access, modification, and deletion.

4.9

Audit logging functionality is to be limited to a subset of privileged users.

5. Enforcement

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

6. Distribution

This policy is to be distributed to all staff.

7. Related Standards, Policies, and Processes

- Event Logging Requirement Standards
- Secure Audit Trail Standards
- Policy Addressing Audit Trails for Root or Administrative Accounts
- Network Time Synchronization Standard
- Event Log Aggregation and Reporting Standards
- Network Monitoring Policy
- Audit Log Review Policy
- Policy Addressing Logging of Initializing, Stopping, or Pausing of the Audit Logs
- General Network and System Event Monitoring Policy

8. Related Sub Controls

Control Code	Control
3.3.1	Auditable Event Generation
3.3.2	Unique User Identifier
3.3.3	Audit Event Review
3.3.4	Alert Audit Processing Failure
3.3.5	Automated Event Correlation
3.3.6	Audit Reduction and Report Generation
3.3.7	Time stamps and Synchronization
3.3.8	Protection of Audit Information
3.3.9	Authorized Access to Audit Functionality

9. Definitions and Terms

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

Term	Definition
Audit	An official inspection of an account, generally by an external party.
Authentication	The verification of a user or processes identity
Authorization	The specific access rights and privileges of a user or process
CUI (Controlled Unclassified Information)	Unclassified Information that should not be publicly disclosed