LOG & MONITORING POLICY

NextGen CGI, LLC

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

NextGen CGI, LLC Logging & Monitoring Standard							
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	Police	S. Hall	S. Hall	0101/2021	S. Hall	01/01/2021

1. Overview

Logging from critical systems, applications, and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

2. Purpose

The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with the enterprise's log management function.

3. Scope

This policy applies to all production systems on NextGen CGI's network.

4. Policy

4.1 General Logging Requirements

4.1.1 All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information that includes the following data attributes:

1. Activity performed
2. User that performed the activity
3. System the activity was performed on
4. Date and time the activity was performed
5. What tool(s) the activity was performed with
6. Status of the activity (success vs. failure), outcome, or result

4.2 Activities to be Logged

4.2.1 The logs shall be created whenever any of the following activities are requested to be performed by production systems on the network:

1. Create, read, update, or delete confidential information, including confidential authentication information such as passwords
2. Create, update, or delete information not covered in #1
3. Initiation of network connections
4. Accepted network connections
5. User authentication and authorization for activities covered in #1 and #2 such as user login and logout
6. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes
7. System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes
8. Application process startup, shutdown, or restart
9. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault
10. Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IPS/IDS), anti-virus system, or anti-spyware system.

4.3 Elements of the Log

4.3.1 Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.

1. Type of action – examples include authorize, create, read, update, delete, and accept network connection.
2. Subsystem performing the action – examples include process or transaction name, process or transaction identifier.
3. Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
4. Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
5. Before and after values when action involves updating a data element, if feasible.
6. Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
7. Whether the action was allowed or denied by access-control mechanisms.
8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4.4 Formatting and Storage

4.4.1 The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

4.4.1.1 Microsoft Windows Event Logs collected by a centralized log management system

4.4.1.2 Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system

4.4.1.3 Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document

4.4.1.4 Other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

5. Policy Compliance

5.1 Compliance Measurement

The Information Security Team will verify compliance to this policy through various methods, including but not limited to periodic walkthroughs, video monitoring, business tool reports (e.g. SIEM tools), internal and external audits, and feedback to the policy owner(s).

5.2 Exceptions

Any exception to the policy must be approved by the Information Security Team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies, and Processes

- Data Classification Policy
- Asset Management Policy
- Change Management Policy
- Configuration Management Policy
- Risk Assessment Policy
- Anti-Malware Policy

7. Definitions and Terms

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

Term	Definition
RESTRICTED	RESTRICTED