NATIONAL DATA
MANAGEMENT AUTHORITY

Security Logging Standard

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. This standard establishes controls securing system logs.
2. It was adapted from NIST Cybersecurity Framework Policy Template Guide and SANS Institute.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

Logs record data so that systems and networks can be appropriately monitored to maintain use for authorised purposes and an awareness of the operating environment, including detecting indications of security problems. This standard defines requirements for security log generation, management, storage, disposal, access, and use. Security logs are generated by many sources, including security software, such as antivirus software, firewalls, and intrusion detection and prevention systems; operating systems on servers, workstations, and networking equipment; databases and applications.

2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this standard. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This standard encompasses all systems, automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It addresses all information, regardless of the form or format, which is created or used in support of business activities. It is the user's responsibility to read and understand this standard and to conduct their activities in accordance with its terms.

4.0 Standard

Logs must be generated in information technology (IT) systems and networks. Because of the nature of the data contained in security logs (e.g., passwords and e-mail content), they are considered personally identifiable information (PII) and must be protected with the controls that maintain confidentiality and integrity.

4.1 Initial Log Generation

4.1.1 All hosts and networking equipment must perform security log generation for all components (e.g., OS, service, application).

4.1.2 All security events (*See Appendix A*) must be logged and must be set to capture significant levels of detail to indicate activity.

4.2 Log Administration

4.2.1 All hosts and networking equipment must issue alerts on security log processing failures, such as software/hardware errors, failures in the log capturing mechanisms, and log storage capacity being reached or exceeded. All alerts must be as close to real time as possible.

4.2.2 When non-revolving log storage reaches 90% capacity, a warning must be issued.

4.3 Log Consolidation

4.3.1 Security-related information from all systems, with the exception of individual workstations, must be transferred to a consolidated log infrastructure. Systems running workstation operating systems which are used for shared services, such as shared file storage or web services must also satisfy these requirements.

4.3.2 All workstations must have the ability to transfer logs to a consolidated log infrastructure, if needed

4.3.3 Log data must be transferred real-time from individual hosts to a consolidated log infrastructure. Where real-time transfer is not possible, data must be transferred from the individual hosts to a consolidated log infrastructure as quickly as the technology allows.

4.3.4 Organisations must establish processes for the establishment, operation and, as appropriate, integration of log management systems.

4.4 Log Storage and Disposal

4.4.1 Within the consolidated log infrastructure, logs must be maintained and readily available for a minimum of 90 days. Based on the organisation's requirements, including audit or legal needs, logs may need to be retained for a longer period of time.

4.4.2 Log data must be securely disposed of (at both the system and the infrastructure level) in compliance with the *Sanitisation/Secure Disposal Standard*.

4.4.3 Systems that collect logs, whether local or consolidated, must maintain sufficient storage space to meet the minimum requirements for both readily available and retained logs. Storage planning must account for log bursts or increases in storage requirements that could reasonably be expected to result from system issues, including security.

4.4.4 A process must be put in place to provide for log preservation requests, such as a legal requirement to prevent the alteration and destruction of particular log records (e.g., how the impacted logs must be marked, stored, and protected).

4.4.5 Log integrity for consolidated log infrastructure needs to be preserved, such as storing logs on write-once media or generating message digests for each log file.

4.5 Log Access and Use

4.5.1 Log data must be initially analysed as close to real time as possible.

4.5.2 Access to log management systems must be recorded and must be limited to individuals with a specific need for access to records. Access to log data must be limited to the specific sets of data appropriate for the business need.

4.5.3 Procedures must exist for managing unusual events. Response must be commensurate with system criticality, data sensitivity and regulatory requirements

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with the standard may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

6.0 Exceptions

Requests for exceptions to this standard shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein.

7.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this standard.

8.0 Definitions of Key Terms

Term	Definition
Host[1]	A host is any hardware device that has the capability of permitting access to a network via a user interface, specialized software, network address, protocol stack, or any other means. Some examples include, but are not limited to, computers, personal electronic devices, thin clients, and multi-functional devices.
Log[2]	A record of the events occurring within an organization's systems and networks.
PII[3]	Personally Identifiable Information; Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

[1] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center (CSRC) https://csrc.nist.gov/glossary/term/host
[2] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center (CSRC) https://csrc.nist.gov/glossary/term/log
[3] *Retrieved from*: NIST Information Technology Laboratory – Computer Security Resource Center (CSRC) - https://csrc.nist.gov/glossary/term/pii

Term	Definition
User[4]	Individual or (system) process authorized to access an information system.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

[4] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/user

Appendix A: Security Events to log

Security events that must be logged for all systems include but are not limited to:

Successful and unsuccessful authentication events to include but not limited to:

i) system logon/logoff;

ii) account or user-ID;

iii) change of password;

iv) the type of event;

v) an indication of success or failure of event;

vi) the date and time of event; and

vii) Identification of the source of event such as location, IP addresses terminal ID or other means of identification.

Unsuccessful resource access events will be logged to include at minimum:

i) account or user-ID;

ii) the type of event;

iii) an indication of the event;

iv) the date and time of event;

v) the resource; and

vi) identification of the source of event such as location, IP addresses terminal ID or other means of identification.

Successful and unsuccessful privileged operations including but not limited to:

i) use of system privileged accounts;

ii) system starts and stops;

iii) hardware attachments and detachments;

iv) system and network management alerts and errors messages; and

v) security events - account/group management and policy changes.

Successful and unsuccessful access to log files to include but not limited to:

i) account or user-ID;

ii) the type of event;

iii) an indication of success or failure of event;

iv) the date and time of event; and

v) identification of the source of event such as location, IP address, terminal ID or other means of identification.

Most web servers offer the option to store log files in either the common log format or an extended log format. The extended log format records more information than the common log file format. When technically feasible web servers must use extended log format. The extended log format adds valuable logging information to your log file so you can determine where messages are coming from, who is sending the message and adds information to the log file that would be necessary to trace an attack.

For systems identified as critical based on a risk assessment or systems that have not yet been classified, in addition to the above, successful resource access events will be logged to include at a minimum:

i) account or user-ID;

ii) the type of event;

iii) an indication of the event;

iv) the date and time of event;

v) the resource; and

vi) identification of the source of event such as location, IP addresses terminal ID or other means of identification.