NATIONAL DATA
MANAGEMENT AUTHORITY

Log Retention Policy

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 policy addresses the retention of information system logs.
2. This is a living document which will be updated annually or as required.
3. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose and Benefits

A security log is an essential information security control tool that is used to identify, respond and prevent operational problems, security incidents, and fraudulent activities. Log retention is the continued storage of an organisation's logs. These logs must be retained for compliance, forensic investigations, legal investigations and other business reasons. The purpose of this Policy is to establish guidelines on retaining security logs for Government of Guyana (GoG) Agencies/Ministries utilising the Government's Network (eGovNet), Internet, email, web hosting, data storage facilities; and microwave, VSAT, LTE, Fibre Optics and PLC technologies.

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 policy. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This policy applies to all Public Sector Ministries/Agencies in the Government of Guyana.

4.0 Policy

The goal of this policy is to ensure the appropriate retention of logs for compliance, forensic investigations and other business reasons. The Permanent Secretary is responsible for the implementation of this Policy. For further information regarding the foregoing, please contact the National Data Management Authority.

4.1 Each Ministry/Agency must establish and make available a systemic process for retaining logs in accordance with this policy.

4.2 All Government of Guyana Logs must be retained for the specified time as required in a Log Retention Schedule.

4.3 Each agency is required to log and retain network security events. Examples of the types of logs to retain:

4.3.1 IDS / IPS;
4.3.2 Endpoint Security (Antivirus, antimalware);
4.3.3 Data Loss Prevention;
4.3.4 VPN Concentrators;
4.3.5 Web filters;
4.3.6 Operating Systems;

4.3.7 Hypervisors;
4.3.8 Storage Devices;
4.3.9 Firewalls;
4.3.10 Routers;
4.3.11 Switches;
4.3.12 Domain Controllers;
4.3.13 Wireless Access Points;
4.3.14 Application Servers;
4.3.15 Databases;
4.3.16 Intranet Applications

4.4 All Agencies/Ministries are required to maintain logs in a format that allows them to be immediately available for thirty (30) days. After 30 days, logs will be archived or stored remotely with the ability to make them available within three (3) business days after a request is received. Logs older than one (1) year may be purged unless otherwise directed by an Order of Court or any legal directive order to be retained longer.

4.5 All Agencies/Ministries are required to backup logs daily and securely store them offline. Log backups and retentions must follow the Agencies' established documents and policies, procedures and legislation and all applicable National laws and Public Service rules and regulations.

4.6 All logs are required to be archived in a manner that makes them admissible as evidence in a Court of Law, satisfying **the requirements laid out in The Evidence Act, Chapter 5:03 Section 91[1], and the Electronic Communications and Transactions bill 2019 Section 16.[2]**

5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all organisational policies and standards. Failure to comply with the policy may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, 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 policy 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 should provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with

[1] *Retrieved from:* Laws of Guyana, Evidence Act, Cap 5:03 NO. 20 of 1893

[2] Retrieved from: Laws of Guyana, Electronic Communications and Transactions Bill 2019

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 policy.

8.0 Definition of Key Terms

Term	Definition
IDS[3]	Intrusion Detection System: A security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.
IPS[4]	Intrusion Prevention System: Software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.
Log files[5]	Files that are created automatically during system operation and contain entries about the events that happened in a system. They are vital for systems troubleshooting and analysis. For example, Web Servers automatically saves usage and activity information such as the date, time, IP address, HTTP status, user activity, bytes sent, and bytes received etc
Retention Schedule[6]	A retention schedule is a basic tool of a log management system. It lists how long each type of log is kept, what the final disposition of the logs will be when they are no longer needed for business purposes, and other special information about the logs.
Forensic [7]	The application of investigative and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

9.0 Contact Information

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

[3] Retrieved from: NIST Computer Security Resource Center: https://csrc.nist.gov/glossary/term/intrusion_detection_system
[4] Retrieved from: NIST Computer Security Resource Center: https://csrc.nist.gov/glossary/term/intrusion_prevention_system
[5] Retrieved from: NIST Computer Security Resource Center: https://csrc.nist.gov/glossary/term/log
[6] Retrieved from: https://archives.un.org/sites/archives.un.org/files/general/documents/guideline_retention_schedule_implementation.pdf
[7] Retrieved from NIST Computer Security Resource Center: https://csrc.nist.gov/glossary/term/forensics