NATIONAL DATA
MANAGEMENT AUTHORITY

Auditing And Accountability 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 established requirements for auditing IT resources for accountability.
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

To ensure that Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable laws, directives, regulations, policies, standards, and guidance.

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 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 Information Statement

Auditing and logging are necessary for detecting significant auditable events and those that are relevant to the security of information systems, organisation data, and the environment in which they operate.

5.0 Standard

5.1 Audit Events

The organisation shall design and assign a role to:

5.1.1 Determine that the information system is capable of auditing both system and user-level events in accordance with the requirements of the log retention policy.

5.1.2 Coordinate the security audit function with other organizational entities requiring audit.

5.1.3 Provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.

Determine which events are to be audited within the information system in accordance with the requirements of the log retention policy.

5.2 Reviews and Updates

The organisation shall design and assign a role to update the audited events as needed.

5.3 Content of Audit Records

5.3.1 The information system shall generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

5.3.2 The information system shall generate audit records containing additional information if required.

5.4 Audit Storage Capacity

5.4.1 The information owner shall ensure audit record storage capacity is allocated in accordance with the requirements of the log retention policy.

5.4.2 The information system shall provide a warning to assigned personnel, roles, and/or locations within seconds when allocated audit record storage volume reaches seventy-five percentage of repository maximum audit record storage capacity.

5.5 Transfer to Alternate Storage

5.5.1 The information system shall off-load audit records at an organisation defined frequency onto a different system or media than the system being audited.

5.6 Response to Audit Processing Failures

The organisation shall design and assign a role to:

5.6.1 Alert assigned personnel in the event of an audit.

5.6.2 Take defined actions to process failure; (e.g., shut down information system, overwrite oldest audit records, stop generating audit records).

5.7 Real-Time Alerts

5.7.1.1 The information system shall provide an alert immediately to defined personnel, roles, and/or locations when audit failure events occur in accordance with organisational defined audit failure events requiring real-time alerts.

5.8 Configurable Traffic Volume Thresholds

5.8.1 The information system shall enforce configurable network communications traffic volume thresholds reflecting limits on auditing capacity and rejects or delays network traffic above those thresholds.

5.9 Shutdown on Failure

5.9.1 The information system shall invoke defined actions [e.g. full system shutdown; partial system shutdown; degraded operational mode with limited mission/business functionality available] in the event of organisational defined audit failures unless an alternate audit capability exists.

5.10 Audit Review, Analysis, and Reporting

5.10.1 Review and analyse information system audit records daily for indications of organisational defined inappropriate or unusual activity.

5.10.2 Report findings to organisational defined personnel or roles.

5.11 Process Integration

5.11.1 The information system owners shall ensure automated mechanisms are employed to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

5.12 Audit Repositories

5.12.1 The information system owner shall ensure analysis and correlation of audit records across different repositories to gain situational awareness.

5.13 Audit Reduction and Report Generation

5.13.1 The information system shall provide an audit reduction and report generation capability that:

5.13.1.1 Supports on-demand audit review, analysis, and reporting requirements and after-the-fact.

5.13.1.2 Does not alter the original content or time ordering of audit records.

5.14 Automatic Processing

5.14.1 The information system shall provide the capability to process audit records for events of interest based on organisational defined audit fields within audit records.

5.15 Time Stamps

The information system shall:

5.15.1 Use internal system clocks to generate time stamps for audit records.

5.15.2 Record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and meets organisational defined granularity of time measurement.

5.16 Synchronization With Authoritative Time Source

The information system shall:

5.16.1 Compare the internal information system clocks' organisational defined frequency with the organisational defined authoritative time source.

5.16.2 Synchronize the internal system clocks to the authoritative time source when the time difference is greater than the default five-minutes.

5.17Protection of Audit Information

5.17.1 The information system shall protect audit information and audit tools from unauthorized access, modification, and deletion.

5.18Access by Subset of Privileged Users

5.18.1 The organization shall authorize access to management of audit functionality to only a defined subset of privileged users.

5.19Audit Record Retention

5.19.1 The information system owners shall retain audit records for organisational defined time period consistent with log retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

5.20Long-Term Retrieval Capability

5.20.1 The information system owners shall employ organisational defined measures to ensure that long-term audit records generated by the information system can be retrieved.

5.21Audit Generation

The information system shall:

5.21.1 Provide audit record generation capability for the auditable events as defined in organsational information system components.

5.21.2 Allow organisational defined personnel or roles to select which auditable events are to be audited by specific components of the information system.

5.21.3 Generate audit records for the events with the content as defined.

5.22Time-Corelated Audit Trail

5.22.1 The information system shall comply with audit records from organisational defined information system components into a system-wide (logical or physical) audit trail that is time-correlated to within organisational defined level of tolerance for relationship between time stamps of individual records in the audit trail.

5.23Standardised Formats

5.23.1 The information system shall produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

5.24Changes by Authorised Individuals

5.24.1 The information system shall provide the capability for organisational entity defined individuals or roles to change the auditing to be performed on organisational defined information system components based on defined selectable event criteria within organisational defined time thresholds.

6.0 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, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

7.0 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 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.

8.0 Maintenance

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

9.0 Definitions of Key Terms

Term	Definition

10.0Contact Information

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