OAG Records Retention and Destruction Policy

POL 36/2020

Commencement Date	23 January 2020
Review Date	The review date is 12 months after the commencement date and every three years after that.

POLICY STATEMENT

1.0 Introduction

1.1 The Office of the Auditor General (Office) does not currently have any policy on the retention and destruction of official records in the form of files, papers and electronic data.

1.2 As such, the Office guides in retaining or destructing official records of the Office.

2.0 Purpose

2.1 The purpose of this policy is to provide the Office with a framework to govern management decisions on whether particular documents should either be:

i) retained and if so, in what format and for what period; or
ii) disposed of and if so, when, by what method and by whom.

2.2 This policy ensures that the Office of the Auditor General (OAG):

1. retains valuable documents and saves time, money and space;
2. protects against allegations of selective document destruction; and
3. provides for a routine destruction of non-business, superfluous, and outdated documents.

3.0 Definitions and Acronyms

Define terms used in the policy and explain any acronyms, for example:

Policy Maker	Auditor General
Management	Approval of Executive Management Committee

4.0 Supporting Documents/References

IFRS Foundation Document Retention and Destruction Policy General Order

5.0 Key Words

Audit Files
Human Resource Records
Training Records
Accounts Records
Registry Records
Electronic Data files on the Servers

6.0 Monitoring

All records retention and destruction shall be monitored by Senior Admin Officer Human Resource who will oversee the responsibilities for the operations of Registry.

7.0 Supporting Procedures and Guidelines

The guidelines to the policy are attached as Annexure I to this policy. This information will provide the background to the development of the policy should Officers need clarification.

RESPONSIBILITIES	
Implementation	The Supervisors and Directors are responsible for implementing the policy.
Compliance	All staff are responsible for complying with the policy.
Monitoring and Evaluation	Corporate Services is responsible for monitoring and evaluating the policy.
Development and/or Review	The Corporate Services division will be responsible for developing and/or reviewing the policy.
Interpretation and Advice	Deputy Auditor General is responsible for interpreting and advising on the policy.

Annexure 1

1.0 Record Type

1.0 Listed below are the categories of records kept by the Office of the Auditor General.

a) Audit Files
b) Human Resource Records
c) Training Records
d) Accounts Records
e) Registry Records
f) Electronic Data files on the Servers

2.0 Document Retention

2.1 Any document that is required to be maintained by the Office of the Auditor General should be retained for the maximum time of 7 years that is mandated by this policy.

2.2 Each record of information should necessitate identifying when the retention period of each record is due to expire and taking immediate action to ensure its destruction in a proper and in a secured manner.

2.3 The Office has a legal duty to retain relevant documents which it knows or believes may be relevant to any legal action that could lead to the discovery of admissible evidence.

2.4 Failure to retain relevant documentation could result in the following serious consequences:

1. Costs penalties
2. Part or all of a claim or defence being struck out
3. Contempt of court proceedings against those involved
4. It may also amount to obstructing or perverting the course of justice.

3.0 Roles & Responsibilities of Retaining or Disposing Specific Documents

3.1 The ultimate responsibility for determining whether to retain or dispose of specific documents rests with the Deputy Auditor General as it is reasonable to assume that the Deputy Auditor General should be broadly conversant with the types of documents received, generated and stored.

3.2 The Deputy Auditor General may delegate the operational aspects of this function to one or more senior officers within the Office. In doing so, the Deputy Auditor General would ensure that any such officer is fully conversant with this policy and is also familiar with the operational requirements in relation to document retention/ disposal.

3.3 The Information Technology Support Section at the Office is available to provide the Deputy Auditor General and Senior Officers with advice and guidance on effective data records management practices. The Deputy Auditor General and Senior Officers need to be aware that the personal data processed for any purpose must not be kept longer than is necessary for that purpose.

3.4 There is no interpretive provisions in this policy and it is a matter for reasonable judgment and common sense as to how long personal data should be retained.

3.5 Storage of important original documentation shall be kept onsite (business premises), in a secure location and original documentation which is beyond its operational date should be kept offsite. The documentation should be recorded and archived at the designated offsite location (National Archives of Fiji). Using the Form in Appendix 2. The National Archives will assign a classification copies of which can be retained with copy of the completed Records Retention Form for the office records.

3.6 Hard or scanned copies of documentation beyond its operational date may be kept onsite for reference purposes. Electronic data shall be backed-up by the IT Support Section and the backed-up files shall be kept at an offsite location.

3.7 All electronic and paper document destruction should automatically be suspended when a lawsuit, claim or Government investigation is pending, threatened or reasonably foreseeable. In the case of electronic destruction, the IT Support Section is responsible for ensuring that any automatic destruction programmes are disabled. However, overall control shall lay with the Deputy Auditor General.

3.8 When information reaches the expiry date for retention it must be ensured that ALL of that information are permanently destroyed. Where information is held in more than one media the information must be removed from all record systems, for example, paper shredded or disposed-off at paper recycling company; electronic completely destroyed from any memory source or other media.

3.9 All documents, including electronic documents that are no longer relevant to the Office business, should be destroyed after seven (7) years. Disposal of significant documents should be documented by the relevant senior officer by keeping a record of the document disposed of, the date and method of disposal, and who authorised disposal. [Refer to 7.1 on records destruction method. Records destruction form is attached as Appendix 3].

4.0 Methods used for Draft Documents

4.1 Drafts of documents that have been finalised should not be retained, unless a Senior Officer advises otherwise.

4.2 The staff of the Office shall follow the following guideline:

- Not to deposit paper documents containing personal data or confidential information in the general waste bin. This could result in unauthorized disclosure of such information to third parties and be liable to prosecution. Such documents should be destroyed on site, using office shredders.
- If data is no longer relevant it should be deleted after thirty (30) days and if data is relevant it should be backed up and stored offsite in generic folders.

5.0 Records Destruction Method

5.1 The Managers or Senior Officer shall identify the files that have surpassed 7 years and need to be destroyed. Details of the records filled in the Records Destruction Form with an accompanying Minute shall be put up to the Deputy Auditor General through the respective Director to obtain formal approval to dispose-off obsolete files. This is done through removing from all record systems, for example, paper shredded or disposed-off at paper recycling company which should be witnessed by assigned staff.

5.2 The destruction of electronic data shall be done by IT Audit Manager upon the recommendations of the Section Manager and Director after obtaining formal approval from the Deputy Auditor General. Respective Directors shall be consulted to identify the electronic data that needs to be destroyed. All obsolete electronic data shall be completely destroyed from any memory source in the servers.

5.3 Proper consultation must be done with respective section Managers/ Director who are the owners of the records or the electronic data.

5.4 All staff involved in the destruction of documents or the electronic data are to sign as the witnesses on the Records Destruction Form for the purpose of assurance, accountability and transparency.

OFFICE of the AUDITOR GENERAL
Republic of Fiji

Annexure 2

RECORDS RETENTION FORM

Date	File Reference	File Name	Retention Method

This is to certify that the following files/ data with the details as per the list which has to surpassed 7 years and will be retained at the National Archives of Fiji with the authority of Deputy Auditor General and witnessed by the following staff.

Recommended By:

Name: _____

Designation: _____

Signature: _____

Date: _____

Authorised By:

Name: Sairusi Dukuno

Designation: Deputy Auditor General

Signature: _____

Date: _____

Witness 1

Name: _____

Designation: _____

Signature: _____

Date: _____

Witness 2

Name: _____

Designation: _____

Signature: _____

Date: _____

OFFICE of the AUDITOR GENERAL
Republic of Fiji

Annexure 3

RECORDS DESTRUCTION FORM

Date	File Reference	File Name	Disposal Method

This is to certify that the following files/ data with the details as per the list were destructed with the authority of Deputy Auditor General and witnessed by the following staff.

Recommended By:

Name: _____

Designation: _____

Signature: _____

Date: _____

Authorised By:

Name: Sairusi Dukuno

Designation: Deputy Auditor General

Signature: _____

Date: _____

Witness 1

Name: _____

Designation: _____

Signature: _____

Date: _____

Witness 2

Name: _____

Designation: _____

Signature: _____

Date: _____

8.0 Monitoring & Implementation

To ensure effectiveness of this policy it will be reviewed on an annual basis. Taking into account of challenges to the policy and any changes to legislation and national guidance.

9.0 Review

This policy will be reviewed 12 months after implementation and every 3 years after that.

10.0 Who Contact About this Policy

Any queries is directed to Deputy Auditor-General

11.0 Approval

This policy becomes effective on the date approved by the Executive Management Committee.

12.0 Revision/Change Log

Version 1.0	
Policy endorsed by:	Executive Management Committee
Policy approved by:	Auditor-General
Policy effective from:	23 January 2020
Policy to be reviewed by:	23 January 2021
Policy prepared by:	Senior Admin Officer (Human Resources)
Manager responsible for policy:	Manager Corporate Services