OFFICE OF THE
PUBLIC SERVICE COMMISSION

RECORDS & INFORMATION MANAGEMENT STANDARD OPERATING PROCEDURES

www.psc.gov.vu 678 +33360

Table of Contents:

Acronym:

RTI – Right to Information
DMS – Document Management System
HRMIS – Human Resource Management Information System
SOP – Standard Operating Procedures
OPSC – Office of the Public Service Commission
NSDP – National Sustainable Development Plan
GIP – Government Investment Proposal
GoV- Government of Vanuatu

Preamble to OPSC's Records and Information Management Standard Operating Procedure (SOP)

Prime Minister Charlot Salwai Tabimasmas in launching the Vanuatu National Policy for Records and Information Management (August 2018) stated:

> "The Vanuatu Government recognizes that sound records management in government is fundamental to good governance and effective and efficient administration. It forms the basis for formulating policy, managing resources and delivering services to the public. Records management provides the basis for accountability and protecting the rights of individuals. To support continuing service delivery and provide the necessary accountability, government bodies should create and maintain authentic, reliable and usable records.
>
> Government bodies must also ensure that the integrity of records is protected for as long as they are required as evidence of business operations. Records management is a process of ensuring the proper creation, maintenance, use and disposal of records to achieve efficient, transparent and accountable governance. Sound records management implies that records are managed in terms of organizational records management program governed by an organizational records management policy."

Well-managed records provide clear & durable evidence of what the Government has promised, what has been done, what services have been provided and how public funds have been spent. Weak records result in ad hoc, potentially misleading national evidence that opens opportunities for manipulation, corruption and fraud – especially in the area of the OPSC's mandate – the personnel records of Public Servants.

Poor management weakens a Public Servant's right to claim fair entitlements, also undermining the ability to plan as well as monitor policies and services as well as to provide open information fairly, effectively and openly. The Right to Information (RTI) is now enshrined in the Right to Information Act and the OPSC is legally obligated to provide better records management to ensure compliance to the legislative and policy framework under which the OPSC operates as well as to the principles of open government, organisational justice and fairness.

Out-of-date, inadequate Records Management must urgently be addressed to ensure that once our new ICT based HRMIS system is developed the data imported to the system will be validated, verifiable, and up to date in line with the Mission Statement of the Vanuatu National Policy for Records and Information Management:

Mission Statement
(Vanuatu National Policy for Records and Information Management)

> *It is the Mission of the Government of Vanuatu to provide, protect, promote and preserve Government public records, in collaboration with relevant public authorities for the benefit of the people of the Republic of Vanuatu."*

The National Sustainable Development Plan (NSDP) envisages under the Society Pillar 6 "A dynamic public sector with good governance principles and strong institutions delivering the support and services expected by all citizens of Vanuatu." The Policy Objective Society 6.1 clearly states how this strategy will be advanced *"enhance the capacity and accountability of public officials and ensure the impartiality and effectiveness of performance management systems"* and Soc 6.6 to *"strengthen national institutions to ensure they are cost effective and well-resourced to deliver quality public services."*

Central to this is Society 6.7 "*Guarantee the public's right to information*" and Society 6.9: "*Strengthen research, data and statistics for accountability and decision making."*

Core to achievement of these NSDP Policy Objectives is compliant timely up-to-date Records Management.

Therefore, the Office of the Public Service Commission (OPSC) has prepared a Standard Operating Procedure (SOP) with a linked Implementation Plan to commence sound and compliant practices of Record Management.

It is recognised that this SOP and its Implementation Plan are pivotal precursors to the OPSC's new ICT-based HRMIS and Document Management System (Paperles ngx), currently proposed for Development Partner support and development. Proper Records Management is not only a matter of organizational justice, service delivery and use of budget resources but essential for the reduction of litigation expenses, improper human resources management and failure to provide cost effective efficient public service delivery and governance.

Purpose

The purpose of this Standard Operating Procedure (SOP) is to operationalize the commitment to good recording management in support of good governance and responsibility assigning good record keeping within the Public Service Commission.

Two new officers have been appointed to the Corporate Services Unit to focus on Records Management

- Senior Officer Records Management
- Records Management Officer

With staff in place and a Government Investment Proposal (GIP) for an ICT-based HRMIS system, the time for action is now to ensure the personnel and general OPSC records are accurate and up to date.

This SOP is intended to be a living document. The Implementation Plan will focus on activities to end of the 2025 Business Plan year, then forecast activities as high priorities for action/implementation in the revised 2025 Business Plan be developed following the November Sitting of Parliament – the Appropriations Sitting.

Without proper financial support for storage archiving costs, this SOP cannot be implemented. Therefore, the Implementation Plan for the Records and Information Management SOP priorities as a critical step the confirmation of costs and budget for the SOP to be implemented – not as a cost but as an investment in compliant, functional records and information management.

Scope:

The SOP applies to all Public Service employees, including temporary and casual employees, contractors and volunteers whom are employed to handle records of the Public Service Commission.

Application:

This SOP applies to all files, emails, memorandum, Commission decisions, disciplinary cases, appointment approvals, Employee Performance Management Review (PMR) Appraisals, Reports, Personnel Files, Public Servants employment records,

Standard Operating Procedure Statement:

Records of Public Service actions and decisions are acknowledged as assets and are a vital part of the organization's corporate memory. Managing these assets efficiently will help save time and money by ensuring that vital information can be located when it is needed. Protecting this information, so that it is not lost or destroyed while it is still needed, is essential to accountability. It is also essential to protect the governments and the community's interests, and the rights and entitlements of the public servants. Moreover, the Public Service is responsible for maintaining the security, confidentiality and privacy of the information resources it holds.

To ensure that the Public Service Commission gains maximum benefit from its information resources, this policy requires all government organisations to ensure that:

- full and accurate records of all their activities are made;
- these records are managed efficiently to ensure they can be retrieved when needed and not released inappropriately;
- no records are destroyed without the permission of the National Archivist
- Records and Information Management is everyone's business.

Legislation, Regulation, Planning and Policy Framework:

The management of records and information operates under a complex framework of legislation, policy and planning of which the following are key components:

- Constitution of the Republic of Vanuatu -
- Public Service Act
- Public Service Staff Manual (PSSM)
- Right to Information Act #13 2016
- National Sustainable Development Plan
- Vanuatu National Policy on Records & Information Management
- Code of Practice on Records & Information Management 2018 (Government of Vanuatu)
- National ICT for All Policy
- Archives Act (Chapter 216),
- Deposit of Books Act
- Vanuatu National Cybercrime Act No.22 of 2021

Preliminary Reading & Training

All officers responsible for records and information management must prepare their roles by understanding their responsibilities, recognizing that sound Records and Information Management is everyone's business.

Step 1: Read the following documents

1. The Vanuatu National Policy on Records and Information Management
2. Code of Practice on Records and Information Management

Step 2: Right to Information Web Site Training PowerPoint

It is intended to provide a training program for OPSC officers and those officers in each Ministry responsible for records and information management. It is noted that this training should be part of a Records Officers Orientation training.

If this is not possible, the officer must undertake to review the RTI PowerPoints available on the RTI Web Site developed by the RTI Unit as a training package.

Roles & Responsibilities:

The **Director General** is responsible for ensuring that the Corporate Services Unit structure has a Records Management Officer position.

The **Director** of each Department is responsible for

- implementing the PSC SOP for Records & Information Management;
- ensuring that an officer is nominated, trained and recognised as the Focal Point Officer for records management
- the designated officer's Job Description includes this responsibility
- all officers understand their individual responsibility for records
- training for Department staff in the Department's Training Plan on records & information management
- budget in annual Business Plan for procurement of filing and archiving equipment and materials

Senior Managers are responsible for

- implementing the PSC SOP for Records & Information Management
- managing their Unit's records in compliance with GoV legislation, policy & procedures;
- maintaining the implementation and up-dating of the PSC records classification/file register system
- maintaining a Master Copy of File Register system
- oversight for digitization/scanning of files to HRMIS/ DMS(Paperless-ngx)
- overseeing the disposal process

Records Management Officers are responsible for

- implementing the PSC SOP for Records & Information Management
- providing a Monthly Report to the Manager on issues related to Records & Information Management for provision to the RTI Unit as per Vanuatu National Policy on Records & Information Management;
- maintaining a Master Copy of File Register system;
- digitization/scanning of files to HRMIS/DMS
- overseeing the disposal process
- conducting spot records management audits
- delivering training on Records & Information Management to Department/agency staff;
- supervising/mentoring junior officers responsible for Records & Information Management

All PSC Officers recognising that sound Records and Information Management is everyone's business

- accept responsibility for the documents and information generated by their work
- keep documents in compliance to records classification system (File Register)
- store documents safely pending filing or disposal
- participate in training and implementation of sound records management processes
- recognise that their work generates commercial-in-confidence documents and store such files securely
- comply with the
    - Vanuatu National Policy on Records and Information Management
    - Code of Practice on Records and Information Management

RECORDS MANAGEMENT PROCEDURES – HARD COPY

CREATION AND RECEIPT OF RECORDS

a. All correspondence received should be recorded in the incoming mail register and date stamped.
b. Records are allocated reference numbers from the Records Classification System.
c. The Records Clerk should write the reference number and description of the record in the register.
d. Reference numbers will be used consecutively.
e. All files should be recorded in a register of files opened. The register of files opened should have the following columns: (See Form 1: File Register)

    I. Date of receipt.
    II. File/reference number according to File Register.
    III. Description of record.
    IV. Recommended Disposal date.

Utilisation of Records Classification System/File Register

a. all employees in the Department must utilise the approved Records Classification Systems/File Register; (refer Form 1: File Register)
b. ensure that correct reference numbers are allocated when records are created;
c. prevent duplication of files and
d. Full file descriptions must be appended on the prescribed departmental file covers.

RECORDS STORAGE & MAINTENANCE

RECORDS STORAGE

a. All records that have been received/created must be stored in a safe environment which is conducive for preservation of records as per Vanuatu National Policy on Records and Information Management;
b. Storage places must be lockable to prevent unauthorised entry.
c. Windows and doors must have burglar guards.
d. Steel racks and lockable steel filing cabinets must be used to keep records.
e. All paper-based correspondence records that are not HR related should be kept in the central registry.
f. HR records up-loaded to HRMIS /DMS by responsible officer (once OPSC HRMIS is developed)
g. All these records are under the management of the Records Manager or designated Records Officer who is mandated to ensure that they are managed properly.

RECORDS MAINTENANCE

a. Records must **not** be placed on the floor.
b. Records must **not** be stored near roof leaks, water pipes, flammable liquids or material or bare electrical wiring that poses a hazard to the records.
c. Windows must have blinds or curtains to prevent direct sunlight.
d. Air conditioners should be installed to central filing facilities (recommended modern standards are between 18 and 22 degrees.)
e. It is recognised that many PSC offices will not have modern filing storage facilities and, in such cases, files should be stored as securely as possible under the operating circumstances;
f. Fire extinguishers with $C0_2$ (carbon dioxide) should be installed inside the Ministry filing storage facility and must be serviced annually.
g. Fumigation must be conducted quarterly to ensure preservation of records.
h. When file covers have been worn out, they must be replaced to ensure effective protection of records.
i. All files must have the components of a file (file cover, backing board, file fasteners, summary sheet and control movement cards) to ensure compliance with the registry guide and Registry Procedure Manual.
j. When files reach 3 cm to 5cm in thickness, a new volume must be opened accordingly.

RECORDS CLEARANCE

a. Records are either destroyed or transferred to appropriate file repository or records centres. (See Form 3: Transfer Register and Form 4: Disposal Register)
b. All methods of disposal of records, whether through recycling or shredding may be carried out only after the disposal authority has been obtained from National Archives
c. All records clearance must be conducted as per the Vanuatu National Policy on Records and Information Management.
d. In exceptional cases, it is necessary that some records may be held permanently in the department (i.e. litigation) and in such cases special approval by the Archivist is necessary.

RECORDS DISPOSAL PROCEDURE

a. All records disposals must be conducted as per the Vanuatu National Policy on Records and Information Management.
b. Records that are due for disposal are determined by the creator of the records.
c. The Records Manager must be consulted for advice and guidance on the disposal process.
d. All applications for disposal authority should be sent to the Records Manager of the department accompanied by the list of records due for disposal to the Vanuatu National Archives to dispose of records due for disposal. (See Form 4: Disposal Register)

SYSTEMATIC DISPOSAL PROGRAMME

a. The disposal of records is an essential and critical element of records management Programme defined by the Vanuatu National Policy on Records and Information Management.
b. Public records may be disposed of by the Departments in two ways, by either authorized disposal or through authorized transfer by the Archivist.

c. Offices must implement the Systematic Disposal Programme for records which no longer have administrative or functional values *on a regular basis.*
d. Disposal of records refers to an action which includes destroying/deleting a record or transferring of records to Archives repositories.
e. The systematic disposal consists of following steps:

- gaining control of both current and terminated records. Terminated records due for disposal must be sorted in their original categories, listed and batched
- submit application for disposal authority in writing to the Records Manager and attaching the list of records due for disposal. (Refer Form 4)
- the Records Manager will then send the disposal request to the Archivist.
- once the disposal authority has been issued and granted by the Archivist, then the office must clear up the records on the basis of disposal authorities obtained, either by Disposal or transfer to an archive's repository for permanent preservation. (Refer to Form 5: Archive Register)
- After the records have been disposed of a copy of the Disposal record must be completed by the office and submitted to the Records Manager. A copy will be filed at the office and the original will be submitted to the Archivist. (Refer Form 4: Disposal Register)

DISPOSAL OF RECORDS

Disposal of records is procedurally defined by the Vanuatu National Policy on Records and Information Management.

a. Public records may be destroyed in accordance with the requirements of the Vanuatu National Policy on Records and Information Management.
b. The Disposal of non-archival records must occur with the approval of the Records Manager or designated officer.
c. Prior to implementing an authorized disposal action, the Records Manager must ensure that no work is outstanding, and no litigation or investigation is being conducted that concerns the records in question.
d. The Records Manager must ensure that all Disposal actions are properly documented and maintain evidence of any records disposal activities that have occurred.
e. The office must ensure that the Disposal register and a register of authorities are in place and Disposal certificates are filed.
f. A Disposal Register is a Register which indicates the records which are due for Disposal. (See Form 4: Disposal Register)

TRANSFER OF RECORDS TO NATIONAL ARCHIVES

The National Archives of Vanuatu are a finite space and cannot store all the nation's documents. Documents will need to be transferred to a Ministry storage facility.

a. Only records of national importance will be considered by the Vanuatu National archives
b. Records marked for permanent preservation must be transferred to the Vanuatu National Archives Saralana, Port Vila after reaching 15 years. (Refer Form 3)

c. The Records Manager must liaise with the National Archivist to arrange space for the transferred records.
d. If there is no space at the Archives repositories then other off-site storage suitable for the records must be identified.
e. The Records Manager must ensure that the off-site storage is in compliance with the:

    - Code of Practice on Records & Information Management 2018 (Government of Vanuatu)
    - Archives Act (Chapter 216),
    - Deposit of Books Act
    - Vanuatu National Policy on Records and Information Management

f. When records are transferred, they must be packed in archival boxes in the same sequence as described on the transfer list.
g. The copy of the Transfer Register (Refer Form 3) must be sent to the receiving office.
h. The National Archivist may refuse to accept the records into custody if they are not properly packed as prescribed.

TRANSFER OF RECORDS TO OTHER OFFICES

a. When transferring records to other offices, the Records Officer must notify/inform the Ministry Records Manager of such transfers
b. A Transfer List/Register (See Form 3) should be prepared, and a record made of date of transfer and signed by sending & receiving officers
c. When records are transferred, they must be packed in boxes in the same sequence as described on the transfer list.
d. The copy of the transfer list must be submitted to the receiving office.
e. The office must ensure that a transfer register is in place which indicates all the approved transfers of records.
f. The Records Manager of the Ministry is ultimately responsible for the safety of the transfer of any records.

CLOSING OF FILES

a. Files must be closed when they reach 3cm- 5cm in thickness and a new volume must be opened marked volume 2 for example, see Volume 2 must be written on the outside of the file cover.
b. Indicate the closing date on the file which is the date of last item of correspondence.
c. A clean sheet of paper with words "Closed, See Volume 2" must be attached in the file after the last correspondence.
d. Closed files must not be filed with current files.

RETRIEVAL/ACCESSIBILITY OF DEPARTMENTAL RECORDS

Under the Right to Information Act, records/files must be easily accessible.

a. Records should be retrieved by using file reference numbers
b. Upon request of files, the Records Officer or designated staff member in each GoV agency will retrieve the file, complete the information on the file movement control card, fill in the

route form and thereafter forward it to the relevant section or official. (See Form 2: Request for Transfer)

c. The requested records are to be retrieved for a period ranging from 3 to 5 days.
d. The requested files must only be loaned for ten (10) days and thereafter must be returned to registry.
e. Should the file be required for more than ten (10) working days it must be requested again.
f. There should be no unauthorized access into the registry therefore files can only be accessed by the Records Officers or designated staff members.
g. Members of the public are not allowed to access classified departmental records and information except when granted access or permission by the Deputy Information

NON-COMPLIANCE AND REPORTING

A Vanuatu Government Public Servant who fails to comply with this Standard Operating Procedure shall be guilty of an act of misconduct.

ARCHIVING PROCEDURE

Officers in the Department should follow the archiving procedures or guidance provided in the Standard Operating Procedure for Records and Information Management.

FORMS

Forms for the administration of this SOP

- Form 1 – File Register
- Form 2 – Request for transfer
- Form 3 – Transfer Register
- Form 4 – Disposal Register
- Form 5 – Archive Register
- Form 6 – Record retention Schedule
- Form 7 – File Check list

RECORDS MANAGEMENT PROCEDURES – SOFT COPY

ROLES AND RESPONSIBILITIES

a. **Record Management Officers** are responsible for ensuring records are maintained correctly and securely within the system.
b. **IT Administrators** are the technical aspects of the Document Management system such as backups, encryption, and access controls are implemented and maintained.
c. **Data Owners/ Units/ Departments** are responsible for ensuring that records under their responsibility are complete, accurate, and compliant with SOP policies.
d. **End Users** are responsible for entering, updating, and retrieving records as per the SOP guidelines.

PROCEDURES

CREATION AND ENTRY OF RECORDS

a. **Data Input Standards**:
   - All records must be entered into the system following defined data input standards such as date formats, naming conventions, and metadata tagging document type.

b. **Version Control**:
   - Each record must have a clear version number, with a change log to capture any updates or modifications.
   - Systems must automatically track and timestamp each record entry or update.

RECORD STORAGE AND CLASSIFICATION

a. **File Naming Conventions**:
   - Use standardized file naming conventions that clearly identify the content, unique department, date, and version

b. **Metadata:**
   - Attach relevant metadata (department, document type, creation date) to ensure efficient searchability.

c. **Folder Structure**:
   - Organize records within an agreed-upon folder structure (department > year > project or subject) for ease of access

d. **Encryption**:
   - All sensitive records must be encrypted both at rest and during transmission.

e. **Regular Audits**:
   - Conduct regular security audits of the document management system to ensure that access controls, encryption, and other security protocols are functioning as required.

f. **Compliance with Regulations**:
   - Ensure that record-keeping procedures comply with applicable regulations (e.g., GDPR, HIPAA, industry-specific standards).

ACCESS AND PERMISSIONS

- **Role-Based Access Control (RBAC)**:
  - Access to records is determined by user roles and responsibilities, ensuring that only authorized personnel can view or modify records.
- **User Access Logs**:
  - Review user access logs to identify any abnormalities in record modification.

BACK UP AND DISASTER RECOVERY

- **Backup Schedule**:
  - Monthly automatic backups (Paperless ngx) should be performed weekly.

- Monthly backup to Microsoft OneDrive (Personal files).
- Monthly backup to Share drive (Office Documents)

- **Offsite Backup**:
  - Store backups in an offsite location (network attached storage device (NAS) or hard drives) or in cloud server to ensure data can be recovered in case of disaster.
- **Disaster Recovery Plan**:
  - The Record Management Unit will work closely with DCDT and FMIS to develop a clear disaster recovery plan to restore records in case of system failure or breach

RETENTION AND ARCHIVING

- **Record Retention Period**:
  - Maintain records for a specified period according to legal, regulatory, or business needs for 15 years (Hard Copy) and 20 years (Soft Copy).
- **Archiving Procedure**:
  - After the retention period, records should be archived to secure, read-only locations. Archived records must remain accessible for future reference.
- **Disposal of Records**:
  Securely delete records that are no longer required, following proper data. This includes:
  - Overwriting (data wiping)
    - Use when reusing or redeploying digital devices that held non-sensitive or declassified data.
  - Cryptographic erasure
    - Use when data is stored in encrypted form (e.g. in cloud platforms or on encrypted drives) and you need to render it inaccessible
  - Physical destruction
    - Use of highly sensitive or classified information, or when devices are being permanently decommissioned
  - Degaussing
    - Use of bulk disposal of magnetic media (e.g. backup tapes or hard drives), where the medica will no be reused
  - Certified destruction services
    - Use for secure disposal when internal capability doesn't exist or for large volumes of data. Ensure a certification of destruction is obtained.

MONITORING AND AUDITING

Internal Audits:
- Perform periodic audits to verify that records are maintained as per SOP guidelines and that retention policies are followed.

Compliance Checks:
- Ensure adherence to legal and regulatory requirements through regular compliance checks.

Audit Logs:

- Maintain detailed audit logs of user activity, including access, modification, and deletion of records.

TRAINING AND SUPPORT

User Training:

- Provide regular training sessions for staff to familiarize them with record-keeping policies, online systems, and security protocols.

Helpdesk Support:

- Maintain a helpdesk or support team to assist with any record-keeping issues, including data entry, access, and retrieval.

REVIEW AND UPDATE OF SOP

SOP Review:

- The SOP should be reviewed at least after two years, or when there are significant changes to systems, policies, or regulations.

Version Updates:

- Any updates to this SOP must be documented and communicated to all relevant personnel.

RECORD RETENTION SCHEDULE

RETENTION PERIODS BY REORD TYPE

Record Type	Description	Retention Period	Action After Retention Period	Legal/Regulatory Basis
Hard Copy	All Records	15 years after termination	Archive for historical records or securely destroy	National Archives Act
Soft Copy	All Records	20 years after termination	Archive for historical records or securely destroy	National Archives Act

DISASTER RECOVERY PROCESS

PRE-DISASTER PREPARATION

1. Develop a Disaster Recovery Plan (DRP)
- Document and maintain a formal DRP.
- Ensure the DRP covers all critical systems, data, and processes.
- Assign key personnel responsible for implementing the DRP.
- Keep copies of the DRP stored securely both onsite and offsite (e.g., cloud storage).

2. Identify Critical Systems and Data
- Create an inventory of critical IT systems (servers, applications, databases).
- Identify essential data and prioritize its recovery.
- Ensure all essential business functions are documented with recovery priorities.

3. Backup and Disaster Recovery
- Implement automated daily backups for all critical data.
- Store backups securely offsite or in the cloud.
- Regularly test backups to ensure data integrity and usability.
- Maintain multiple backup versions to prevent data loss.

4. Disaster Recovery Team
- Assign a disaster recovery team with clear roles and responsibilities.
- Ensure all team members are trained and aware of their duties.
- Develop a communication plan with key contacts (internal and external).

5. Testing and Drills
- Conduct regular disaster recovery drills (once a year).
- Test the recovery of critical systems and applications.
- Document the results of drills and make improvements as needed.

IMMEDIATE RESPONSE TO A DISASTER

1. Assess the Situation
- Identify the type of disaster:
  - hardware failure
  - cyberattack
  - power outage
  - natural disaster
- Determine the extent of damage to systems and data.
- Notify key personnel, including the disaster recovery team and management.

2. Activate the Disaster Recovery Plan
- Invoke the DRP if the disaster meets the criteria for activation.
- Follow the step-by-step procedures outlined in the DRP for recovery.
- Document the incident, including the time of occurrence and the initial impact.

3. Communication

- Inform all relevant stakeholders (DCDT, FMIS, RTI, National Archive) about the situation and recovery efforts.
- Establish internal communication channels for updates (email, phone call).

RECOVERY STEPS

1. Data and System Recovery

- Evaluate the damage to servers, applications, and data.
- Restore data from the most recent, verified backup.
- Rebuild or restore affected systems (e.g., reimage servers, reinstall software).
- Test the restored data and systems to ensure they function correctly.

2. Network Infrastructure Assessment and Recovery

- Assess the network and connectivity.
- Re-establish network access, including routers, switches, and internet connectivity.
- Review network security configurations (e.g., firewalls, VPNs) to ensure they are intact.

3. Application Recovery

- Restore critical applications Document Management System (Saperion) according to the recovery priorities in the DRP.
- Test applications to ensure full functionality.
- Validate user access and permissions after restoration.

4. Hardware Replacement (if necessary)

- Replace damaged hardware (servers, workstations).
- Restore software environments on the new hardware.
- Test hardware functionality and performance after installation.

POST-RECOVERY ACTIVITIES

1. Data and System Recovery

- Continuously monitor systems for any post-recovery issues or anomalies.
- Validate that all applications and data are fully restored and operational.
- Ensure security measures are re-enabled (e.g., antivirus, firewalls, encryption).

2. Communication and Reporting

- Provide status updates to stakeholders about the recovery process.
- Document the full timeline of events, recovery actions, and outcomes.
- Prepare a final incident report to submit to management.

3. Evaluate and Improve the Disaster Recovery Plan

- Conduct a post disaster review of the event and recovery efforts.
- Identify any weaknesses in the disaster recovery plan or response process.
- Update the DRP based on lessons learned and any new vulnerabilities discovered.
- Train the disaster recovery team and staff on any plan updates or new procedures.

4. Regulatory Reporting

- Ensure compliance with any regulatory reporting requirements for the incident (e.g., breach notifications under GDPR or HIPAA).
- Report the incident to regulatory bodies within the required time frame.

ONGOING MAINTENANCE AND PREPAREDNESS

1. Regular Updates

- Ensure that all systems and software are regularly updated with the latest patches and security updates.
- Maintain up-to-date hardware and infrastructure to avoid preventable failures.

2. Periodic Review of DRP

- Review and update the Disaster Recovery Plan at least annually.
- Ensure any changes to IT infrastructure, applications, or business processes are reflected in the DRP.

3. Employee Training

- Conduct regular training for employees on disaster recovery procedures and system usage during an outage.
- Hold refresher courses for the disaster recovery team on DRP protocols.

KEY CONTACTS AND RESOURCES

1. **Disaster Recovery Team Contacts:**

Department	Contact Person	Phone	Email:
DCDT- Network and Application Team	Nick Doan	33380	ndoan@digital.gov.vu
FMIS – System Administration Team	Joe Livu	22605	jlivu@doft.gov.vu
PSC-HRMIS Team	Jack Norris Philip	33360	jnphilip@vanuatu.gov.vu
PSC Records Management	Jessica Sisi	33360	jsisi@vanuatu.gov.vu

2. Backup and DRP Locations

- **Primary Backup**: Location of your primary backups (cloud storage DCDT / NSA Record Management Unitor offsite storage facility Record Management Unit).
- **DRP Copies**: Location of the latest DRP copies (e.g., secure cloud access or physical storage).

MONITORING REVIEW AND EVALUATION

The Standard Operating Procedure on Records Management will be monitored, evaluated and reviewed after three years or as and when the need arises.

The Vanuatu National Policy and Records and Information Management stipulates a Monthly Report to the RTI Unit on issues arising from Records and Information Management.

However, for practical purposes this SOP recommends a short Quarterly Report to the RTI Unit

AUTHORISATION:

The Records and Information Management Standard Operating Procedure is approved by the Commission on

Date…… Signed…….. Stamped

Annexes: Forms

Forms for the administration of this SOP

- Form 1 – File Register
- Form 2 – Request for transfer
- Form 3 – Transfer Register
- Form 4 – Disposal Register
- Form 5 – Archive Register
- Form 6 – Record retention Schedule
- Form 7 – File Check list

Form 1: File Register

OPSC - Corporate Service Unit – Records Management

FORM 1: FILE REGISTER

File No.	Department	Name	Date Open	Registrar

Form 2: Request for File Transfer

OPSC - Corporate Service Unit – Records Management

FORM 2: REQUEST FOR FILE TRANSFER

Who wants it?_____

Name of the File_____

Department or Ministry_____

Date Requested_____

Date Returned_____

Signature _____

Note:

1. When you have finished filling in the Form please scan and send to records office copying the Manager CSU.

2. The file requested will be collected from the Records office the next day.

3. Files can only be loaned for 10days, should the file be required for more than 10 days then it must be requested again.

4. Due to some officers not returning the files, the Filing Room is no longer available to all staff. The Filing Room will be locked & accessed only by the Record Officers.

Form 3: Transfer Register

OPSC - Corporate Service Unit – Records Management

FORM 2: TRANSFER REGISTER

Reference # / Position Number	Department	Description of records to transfer

Transferers Name:_____ Records Management Officer:_____

Signature:_____ Signature:_____

Date:_____ Date:_____

Form 4: Disposal Register

OPSC - Corporate Service Unit – Records Management

FORM 2: DISPOSAL REGISTER

File No.	Department	Description of Records for Disposal	Reason for Disposal	Date of Disposal

Records Management Officer: _____

CSU Manager: _____

National Archivist: (if documents are of National Importance) _____

Form 5: Archive Register

OPSC - Corporate Service Unit – Records Management

FORM 5: ARCHIVE REGISTER

Archive Box No.	Department	Description of Records	Date Archived

Records Management Officer: _____ Signature: _____

Date: _____

Form 6: Record Retention Schedule

OPSC - Corporate Service Unit – Records Management

FORM: RECORD RETENTION SCHEDULE

Record Type	Description	Retention Period	Action After Retention Period	Legal/Regulatory Basis
All Records	All Records	15 years after termination	Archive for historical records or securely destroy	National Archives Act

Form 7: File Checklist

OPSC - Corporate Service Unit – Records Management

FORM 7: FILE CHECK LIST

Name: _____ File#_____

File Opened: _____ File Closed:_____

Date	Description of record insert

Records and Information Management is everyone's business