SOP: Documentation and Archiving of Assessment Records

This SOP details the procedures for **documentation and archiving of assessment records**, ensuring accurate, secure, and organized storage of evaluation data. It covers the systematic recording, verification, and retention of assessment materials, compliance with data protection standards, and protocols for easy retrieval and long-term preservation of records to support transparency and accountability in evaluation processes.

1. Purpose

To define and standardize the process for documenting and archiving assessment records, ensuring data integrity, confidentiality, and accessibility in compliance with institutional and regulatory requirements.

2. Scope

This procedure applies to all personnel responsible for handling, recording, storing, and retrieving assessment records within the organization.

3. Responsibility

- **Evaluators/Assessors**: Complete and submit assessment records accurately and promptly.
- **Administrative Staff**: Verify, archive, and control access to assessment records.
- **Quality Assurance**: Audit documentation and archiving compliance.

4. Procedure

1. **Documentation**
    - Record assessment data immediately after evaluation using approved forms/templates.
    - Include all relevant details (date, assessor, assessed entity, evaluation criteria, results, signatures).
    - Review records for completeness and accuracy before submission.
2. **Verification**
    - Designated personnel verify each record for accuracy and completeness.
    - Discrepancies or missing data are resolved with the assessor before archiving.
3. **Archiving**
    - Securely store validated records in approved digital or physical archives.
    - Index records for easy retrieval (e.g., by date, type, assessment ID).
    - Apply access controls as per data classification and confidentiality requirements.
4. **Retention and Disposal**
    - Retain records for the period specified by policy or regulation (typically 5â€“7 years).
    - Dispose of expired records securely (shredding for paper, permanent deletion for digital files).
5. **Retrieval**
    - Retrieve records upon authorized request using the archive index.
    - Log all access and retrieval activities for audit purposes.
6. **Backup**
    - Regularly back up digital records to secure, off-site locations.
    - Test backup restoration procedures periodically.

5. Compliance & Security

- Ensure all procedures comply with data protection laws (e.g., GDPR, HIPAA, as applicable).
- Train personnel on data handling and confidentiality protocols.
- Implement physical and digital security measures, including password protection, encryption, and locked storage for physical records.

6. Documentation

Record Type	Location	Retention Period	Access Level

Assessment Forms	Central Archive / Secure Server	7 Years	Authorized Staff Only
Verification Logs	QA Office	5 Years	QA Team
Access Logs	Digital Archive	3 Years	Admin Staff

7. Review and Audit

- Conduct periodic review and audit of archived records and documentation practices.
- Report and address any discrepancies, non-compliance, or security breaches promptly.

8. References

- Data protection and privacy policy
- Records retention and disposal schedule
- Assessment policy and procedure manual

9. Revision History

Version	Date	Description	Approved By
1.0	2024-06-12	Initial SOP creation	SOP Committee