SOP: Archiving and Retention of Internal Communications

This SOP details the processes for **archiving and retention of internal communications**, including classification of communication types, storage methods, retention periods, access controls, legal and regulatory compliance, and procedures for secure disposal. The aim is to ensure proper management, preservation, and retrieval of internal communication records to support organizational accountability, knowledge management, and regulatory requirements.

1. Purpose

To establish standardized procedures for the archiving, retention, accessibility, and secure disposal of internal communications.

2. Scope

This SOP applies to all employees, contractors, and affiliates who generate, receive, or manage internal communications, including but not limited to emails, instant messages, memos, and collaboration platform records.

3. Definitions

- **Internal Communications:** All correspondence shared within the organization for business purposes.
- **Archiving:** The process of storing communications for long-term retention.
- **Retention Period:** The designated duration for which a record must be preserved.

4. Roles and Responsibilities

- **IT Department:** Maintains archiving systems and ensures secure storage.
- **Records Management Officer:** Monitors compliance with retention schedules.
- **Department Managers:** Ensure staff adhere to archiving procedures.
- **Employees:** Classify and submit communications for archiving as necessary.

5. Classification of Communication Types

Type of Communication	Description	Examples
Email	Electronic mail messages sent internally	Project discussions, directives
Instant Messaging	Real-time messaging within internal platforms	Slack, Teams, Skype messages
Official Memos	Formal written communications	Policy changes, HR notifications
Collaboration Records	Files and discussions within shared platforms	Google Drive docs, Microsoft Teams files

6. Storage Methods

- Use of secure, centralized electronic document management systems (EDMS) for long-term storage.
- Encryption of archived records to ensure confidentiality and integrity.
- Routine backups of all archives to offsite or cloud-based storage.

7. Retention Periods

Type of Communication	Retention Period
Email	5 years
Instant Messaging	1 year

Official Memos	7 years
Collaboration Records	3 years

Note: Retention periods may be adjusted according to legal or regulatory requirements.

8. Access Controls

- Role-based access to archived communications enforced through user authentication.
- Confidential and sensitive communications restricted to authorized personnel only.
- Regular audits conducted to review access logs and permissions.

9. Legal and Regulatory Compliance

- Adherence to applicable data protection and privacy laws (e.g., GDPR, HIPAA).
- Regular review of policies to ensure ongoing compliance with statutory obligations.
- Litigation hold procedures in place when required for investigations or legal proceedings.

10. Secure Disposal Procedures

- Records scheduled for disposal are documented and reviewed prior to destruction.
- Use approved secure destruction methods (e.g., digital shredding, physical destruction of media).
- Certificates of destruction obtained when third-party services are used.

11. Review and Updates

- This SOP is reviewed annually or as needed in case of regulatory or organizational changes.
- All revisions are documented, approved, and communicated to relevant stakeholders.

12. References

- Information Governance Policy
- Records Retention Schedule
- Relevant National and International Data Protection Regulations