Records Management Process

1. Creation and Classification

This stage focuses on identifying and documenting a record's attributes from the moment it's created.

- **Policy Definition:** A clear policy must define what constitutes an official record and who is responsible for its creation. This includes establishing a universal naming convention and a standardized file directory structure to ensure consistency.
- **Classification:** All records must be classified based on the **Information Classification and Labelling Policy** you have in place. Each record should be assigned an owner who is responsible for its classification. This initial classification determines how the record will be handled throughout its lifecycle. For example, records containing personally identifiable information (PII) would be classified as "Restricted" and have stricter handling requirements than a public-facing document.
- **Access Control:** Access rights are assigned at the time of creation based on the record's classification. Only authorized users with a need-to-know are granted access.

2. Storage and Protection

This stage ensures records are securely stored to prevent unauthorized access, loss, or corruption.

- **Data Protection:** Records must be protected according to their classification. This includes using encryption for all sensitive data at rest and in transit. Access controls established in the creation phase must be enforced through technical measures, such as role-based access control (RBAC) in your cloud environment.
- **Tamper-Proofing:** Implement controls to prevent the falsification or unauthorized modification of records. This could include using version control systems for documents, as well as audit logs that track all access and modification activities. These logs serve as an immutable record of a document's history.

- **Backup and Recovery:** A robust backup strategy is essential to prevent data loss. Records should be backed up regularly to a secure offsite or cloud location, and a disaster recovery plan should be in place to restore records quickly in the event of an outage or data loss event.

3. Retention and Disposal

This stage governs how long records are kept and how they are securely destroyed.

- **Retention Schedule:** An official records retention schedule must be established, outlining the minimum and maximum retention periods for each type of record. This schedule must conform to all applicable legal, regulatory, contractual, and business requirements. For instance, financial records might have a seven-year retention period to comply with tax laws.
- **Secure Disposal:** Once a record has reached the end of its retention period, it must be disposed of securely to prevent unauthorized recovery. For digital records, this means using secure data destruction methods that make the data unrecoverable. For physical records, this means shredding or other methods of physical destruction.

4. Auditing and Review

This final stage ensures the integrity of the entire process.

- **Periodic Audits:** Conduct regular audits to verify that records are being classified, protected, and managed according to this process and the established retention schedule. Audits should review access logs, data protection measures, and disposal records to ensure compliance.
- **Documentation:** Maintain comprehensive documentation of the records management process, including the retention schedule, audit reports, and any policy changes. This documentation is crucial for demonstrating compliance to third parties during a security questionnaire or audit.