Title: Document Retention Policy
Section: Organisational

Obligations

Businesses in Australia must comply with many levels of legal requirements to operate. From protecting personal data – such as confidential client and employee details – to safeguarding sensitive company information and abiding by sector-specific regulations. Failure to comply at any level can impact business continuity, reputation, and the bottom line, as well as incur severe punitive and criminal damages.

Purpose and Scope

The purpose of this Document Management Policy and attached schedules ("Policy") is to ensure that UBC's documents are properly managed and maintained and that documents no longer of any value are timely and properly discarded. This Policy is intended to assist, directors, employees, members, and volunteers of UBC in understanding their responsibilities for the management and maintenance of the UBC's documents.

This Policy includes schedules for the retention and destruction of specific categories of documents to ensure legal compliance, organisational efficiency, consistency and to accomplish other objectives, such as cost management. Compliance with federal, state, and local retention requirements will override all other objectives. Documents created prior to the adoption of this Policy will be catalogued as soon as practicable to comply with the terms of this Policy.

APPLICATION

UBC also recognise the significant challenge that many face in knowing how long documents should be kept before they need to be securely destroyed or de-identified. A document retention policy is the best way to keep track of the various minimum legal requirements. It also ensures that confidential information is not kept for so long that it becomes a risk in the event of security breach; or contravenes Australian Privacy Principle 11 (APP 11) which states that APP entities must take reasonable steps to destroy or de-identify the personal data as soon as it is no longer required for its primary purpose.

The factors to consider include:

» The type of business

» The categories of documents

» The minimum legal retention periods for each document type

» The document lifecycle from the business perspective

» The secure destruction process once the retention period is over.

The Privacy Act allows for APP entities to de-identify personal information rather than destroy it. Even though this method can be effective in preventing re-identification of an individual, it may not remove that risk altogether.

Making sure, however, that the documents are irreversibly destroyed will reduce this risk, especially in case of a security breach. A Certificate of Destruction is required to adequately document compliance. To help create the right retention schedule for the business, a list of documents that contain confidential information, along with the recommended retention period for each type in accordance with certain legal requirements is attached as Appendix A. These recommendations on document retention are general guidelines only. UBC Honorary Solicitors should be consulted whenever there is any uncertainty regarding the retention period for a document.

Definitions

UBC: The Uncle Bobs Club

State Committee: Directors of the Uncle Bobs Club

Responsible Director: State Secretary

Document: is any record generated during an Organization's operation, whether in written, digitally recorded, electronically stored or other form, whether tangible or intangible. Examples of Documents include, but are not limited to memoranda, electronic mail or "e-mail," facsimiles, contracts, forms, binders, recorded voice mails, calendars, photographs, .pdf files, receipts, and computer files.

Electronic Documents: Electronic Documents, or any Documents stored electronically, shall be treated under this Policy as if they were paper Documents. The retention period of an Electronic Document depends on the subject matter of the Document and shall be retained as listed on the appropriate retention schedule. In other words, the content of a Document determines how it is managed and retained, not the format of the Document.

Policy

COMPLIANCE AND POLICY ADMINISTRATION

The State Secretary of UBC shall be the Policy administrator (Responsible Director) and as such is the officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Policy is followed. The Responsible Director is authorised to:

- Advise directors, employees, members, and volunteers on the Policy.
- Make modifications or additions to the Document retention schedules included in the Policy from time to time to ensure that the schedules are in compliance with local, state, and federal laws.
- Monitor or have monitored local, state, and federal laws affecting Document retention.
- Conduct scheduled periodic reviews of the Policy, and monitor compliance with the Policy.

DOCUMENT CREATION

Documents shall be created for the purposes and in the conduct of the business of UBC only. At no time should documents be created for personal purposes. Directors, employees, members, and volunteers should always refrain from unprofessional, embarrassing, offensive or inflammatory communications, including those in electronic and other formats.

DOCUMENT RETENTION

The law requires UBC to maintain Documents, depending on their content, usually for a specific minimum period. Failure to retain those Documents may subject directors, employees, members, volunteers, and UBC itself to penalties and fines, cause a loss of rights, obstruct justice, spoil potential evidence in a legal action, adversely impact UBC's position with regulatory authorities, place UBC in contempt of court, or seriously disadvantage UBC in the pursuit or enforcement of its legal rights.

DOCUMENT DESTRUCTION

Generally, Designated Documents shall be destroyed annually during a period established by the Responsible Director of UBC. All Documents that are not of a confidential or otherwise non-public nature may be destroyed by any feasible means and shall be recycled when possible. All confidential or otherwise non-public Documents shall be shredded or destroyed using appropriate alternative means to the extent necessary to ensure the continued privacy of the information contained therein and to ensure compliance with applicable law. Electronic records shall be destroyed by a method most appropriate to the storage media, ensuring the continued privacy of information contained therein when necessary.

Exception for Litigation, Investigation, or Audit Relevant Documents. Any Organization Documents that are relevant to litigation, potential litigation (i.e., a dispute that could result in future litigation), an investigation or audit by a regulatory or other authority or that are responsive to any legal request for the Documents, including but not limited to a subpoena, in each case, as determined by the Responsible Director of UBC, shall be preserved according to the Responsible Director of UBC's instructions until the Responsible Director of UBC advises that the Documents are no longer needed. Directors, employees, members or volunteers must report any event they believe would require the preservation of Documents for litigation, investigation, audit or legal purposes, as described herein, to the Responsible Director of UBC immediately, who shall evaluate the circumstances and, if appropriate, take steps to inform promptly all necessary individuals to preserve such Documents and otherwise suspend any applicable destruction schedule. This exception supersedes any previously or subsequently established destruction schedule for the Documents

SCHEDULES

Attached as Appendix A is a Document Retention Schedule. This schedule sets forth the minimum retention periods for major classes of Documents. If a director, employee, member or volunteer is unsure under which category a Document falls, he or she should consult with the Responsible Director of UBC.

Communication/Implementation

This Policy will be communicated to all employees during induction and ongoing refresher training.

Review

This policy and related procedures will be reviewed every three years, unless changed circumstances require earlier review.

References

Policy Name: Document Retention Policy

Responsible Director: State Secretary

Functional Area: Organisational

Date adopted: 27 August 2020

Review Date: 27 August 2023

Review History

Date	Review Details	Action

APPENDIX A

Category	Minimum Retention Period
COMPANY DOCUMENTS	
Formal company documents: Statutory books Board minutes Resolutions	Indefinitely
Accounting records detailing company transactions	7 years including supporting documents
PERSONNEL FILES	
Other business registers	5 years (min.) from date of last entry
Payroll, wage and other employee records	Min 7 years from end of financial year
GST RECORDS	
Details relating to: Taxable supply Creditable acquisition Creditable importation	5 years following assessment period
CORPORATION TAX RECORDS	
Records of all Company assets (e.g. receipts, sales and purchases) Company liabilities Income and expenses	5 years (min.) from end of accounting period. Longer if returns are late
WORKPLACE OHS RECORDS	
Health and safety policies and procedures. Standard operating procedures. **Organisational** code of conduct. Training and induction **records**. Register of Injuries. Workplace health and safety committee meeting minutes. Equipment **records** including inspections, maintenance, and repair.	5 years (min.) from date of last entry
Employee health monitoring records / Hazchem exposure records.	30 years (min). even if employee is no longer employed by the organisation.

For more information:

Privacy Commissioner – oaic.gov.au

Privacy Act – comlaw.gov.au

Corporations Act 2001 – comlaw.gov.au