Company Name: Calypso Creative Agency cc
Company Reg Nr: 2009/194454/23
Date: 23 June 2021

2. Policy: Information Retention and Destruction

2.1. INTRODUCTION

It is important to identify the time periods that Information should be retained by the Company. A retention period is usually the minimum period that Information must be retained. After the retention period has elapsed, such Information must either be archived or destroyed.

It is also important not to retain Information for longer than necessary. Where a retention period has expired, the record in question can be destroyed (*Section 14(1) (a-d) of the Protection of Personal Information Act 4 of 2013*).

2.2. OBJECTIVE

The objective of this Policy is to determine the retention period of Information that the Company keeps and describe the process of destruction or archiving such Information.

This Policy applies to all employees, contractors, visitors, Data Operators, and other persons authorised to access and use the Company's systems that create and use Information that relate to the Company's business operations and Data Subjects.

This Policy applies to all records of Information, whether in manual or electronic format.

This Policy should be read in conjunction with other policies of the Company that regulated the protection of Personal Information.

2.3. PROCEDURES

Lifecycle of Information

The Company acknowledges that Information has a lifecycle and that, if they have come to an end of their retention period, a decision should be made regarding archiving or destroying them. The Information management lifecycle is as follows:

- The origination of the Information is determined either by the creation of the Information by the Company, or the receipt of the Information by the Company from a compliant third party.
- Once the Information is created or received, it is used, updated, modified, stored, maintained, and protected by the Company on a day-to-day basis.
- At the end of the useful life of the Information in question, or when required by relevant and applicable legislation, the Company must evaluate whether such Information should be archived or destroyed.

Retention of Information

Proper Information management is an important part of doing business and the Company must ensure that it complies with all legislation that is applicable to the Information held by it. As there may be different retention periods depending on the nature of the Information. The guidelines set out below will assist in determining the applicable retention period for Information:

- If a minimum retention period is prescribed by legislation, then the retention period set out in such legislation applies.
- If there is no legislated retention period, the retention period set out in the Company's Policy applies.
- If there is no retention period stipulated in the Policy, or if the Company does not have a Policy, then the retention period prescribed by any specific applicable contract or agreement applies.
- If there is no retention period stipulated in any specific contract or agreement, then any retention period agreed to by the Data Subject in question applies. A Data Subject may

agree to records of their Personal Information being held for longer periods of time than that prescribed by legislation or by the Company itself.
- If a Data Subject has not stipulated or consented to a specific retention period in respect of their records of Personal Information, then any retention period prescribed by the CEO applies.
- If none of the above apply, then the Company's Information Officer may determine the applicable retention period.

A table of retention periods are also set out in *Annexure A* for further guidance. Please refer to the *SAICA Guide on The Retention of Records* for more information

Destruction decision

The destruction of Information is not the same as the disposition of Information:
- The disposition of Information refers to the wide range of actions undertaken to manage Information over time, which may include the transfer of Information to an archival storage.
- The destruction of Information is the act of destroying Information permanently by obliterating such Information, so that the Information stored can no longer be physically or electronically reconstructed or recovered. Any decision to destroy Information must be formally approved by the CEO and Information Officer in writing.

Where the retention period for Information has expired, a decision must be made to either:
- Continue to retain the document (if permitted by law).
- Transfer the Information to an archival storage.
- Destroy the Information.

Some of the factors that will influence this decision are:
- If the Information reached its useful life.
- Could there be a future challenge where the Information is needed in a civil or criminal case?
- Does the Information need to be retained for commercial or business purposes?

The abovementioned decision must be formally made and must be properly documented. Such decision must be in writing and must be signed off by the CEO and the Information Officer.

Destruction of paper records

Where a formal decision has been made to destroy Company Information, the destruction must be done securely. Paper records must either be shredded by the Company or placed in confidential bins to be removed for shredding by a reputable third-party provider.

Paper records must not be discarded in trash cans or destroyed by other unsecured methods.

Destruction of electronic Information

Before electronic Information is destroyed, archiving the Information should be considered. If the decision is made to destroy the Information, then one of the following techniques must be used:

- Overwriting: Overwriting is an effective method of destroying electronic Information. This method involves the use of software that overwrites the record multiple times. This makes the possibility of recovering the Information much more remote.
- **Physically destroying storage media**: Physically destroying the storage media or record must be used where Personal Information, and sensitive or confidential Information of the Company is stored. This is also the most appropriate method of destroying Information stored on portable media, such as hard drives, and shredding CDs and DVDs.

2.4. **RETENTION PERIOD OF INFORMATION**

Document / Record / Information	Retention period (years)
Acceptance forms	12
Accident book and records	7
Accounting records of stock of brokers and carrier against shares	5
Accounts payable ledgers and schedules	7
Action Plans / Requests	5
Agreements after termination	5
Agreements with architects and builders (after day of completion)	5
Allotment letters	12
Allotment sheets and return of allotment	15
Annual Financial Statements	15
Annual return and supporting documents	15
Application for jobs – unsuccessful	1
Application forms	12
Apprentice records of remuneration	3
Arbitration award records	3
Aspects and Impacts Register	Continuous
Audit Reports	Permanently
Bank Reconciliations	2
Bank statements, deposit slips, stock lists paid by its member	4 years from last date of entry
Books of account	15
Calibration Records	5
Cancelled share of debenture certificates and balance receipts (many large transfer offices keep for one year only)	3
Cancelled share transfer forms	12
Cash books	15

Certificates and documents of title	Permanently or until sold
Change of address – notification	1
Checks (for important payments and purchases)	Permanently
Collective Agreement records	3
Contract Reviews	5
Contracts and leases (expired)	7
Contracts and leases (still in effect)	Permanently
Correspondence (general)	2
Correspondence (legal and important matters)	Permanently
Correspondence (with customers and vendors)	2
Costing Records	5
Creditor’s invoices and statements	5
Customer Complaints	5
Customer Sign-off/Proof of Delivery	5
Customer Specifications	5
Debtor’s statements	4
Deeds of Title	Permanently or until disposed
Delivery Notes/Advice Notes	5
Deposit slips	4
Depreciation Schedules	Permanently
Detailed records of the registered vendor’s transactions	4 years from last date of entry
Determination records made in respect of the Wage Act	3
Dispute records	3
Dividends and interest	15
Documents of incorporation including: • Certificate of change of name • Certificate of incorporation • Certificate to commence business	Permanently
Duplicate deposit slips	2
Employee Training records and certificates	5 years after service terminated.
Employment applications	3
Employment Equity Plan	3 years after expiry date
Evaluation of legal and Other Requirements	Continuous
Expense accounts	4
Expense Analyses / expense distribution schedules	7

Financial Statements (year-end)	Permanently
Fixed asset register	15
General ledgers	15
Goods received notes	4
Incidents reported at work	3
Income tax required records	4
Indemnities and guarantees	5 years after date of expiry
Index of members	15
Inspection and Test Records	5
Insurance Policies	5
Insurance Policies (expired)	3 years
Insurance records, current accident reports, claims, policies and the like	Permanently
Internal audit reports	3
Invoices (to customers, from vendors)	7
Leases (after date of expiry of lease and all queries have been settled)	5
Letter of Good Standing with Compensation Commissioner	3 years after expiry date
Letters of indemnity for lost share certificates	Permanently
Licensing agreements	5 years after date of expiry
Maintenance Records	5
Management Reviews	5
Memorandum and Articles of Association	Permanently
Method Statements & Drawings	5
Minute books, bylaws, and charter	Permanently
Minutes of Health and Safety Committee meetings	3
Minutes of meetings (originals for): • Board meetings • Committee meetings • General meetings	Permanently
NCI (Nonconformity, Corrective/Preventive Action, Improvement) reports	5
Obsolete personal data	Destroy
Payroll records and summaries	7
Payrolls	7

Personal information and purpose for which data was collected must be kept by the person who electronically requests, collects, collates, processes, and stores the information.	As long as the information is used plus 1 year.
Personal records of organisation's executives	Permanently
Personnel files (terminated employees)	7
Petty Cash books	15
Power of attorney, stop notices and similar court orders (from date person ceased to be a member)	15
Purchase invoices	4
Purchase orders	4
Purchase Specification / Orders	5
Receipts	4
Records of strike, lock-out or protest action	Permanently
Records of subscriptions or levies paid by its members	15
Records of third parties to whom the information was disclosed.	As long as the information is used plus 1 year.
Redemption / conversion discharge forms of endorsed certificates	12
Register of debenture holders	15
Register of directors and officers	15
Register of directors' interest on contracts	15
Retirement records	Permanently
Salary revision schedules	7
Salary wage register	7
Sales invoices	4
Sectional title records	Permanently
Share investment certificates	Permanently or until sold
Staff records (after date employment ceased)	7
Subcontractor Records	5
System Audit Reports	5
Tax return - employees	4
Tax returns and worksheets	Permanently
Taxation returns and assessments	15
Time and piecework records	7
Trademark registrations and copyrights	Permanently
Transfer duty records	Permanently
Unemployment insurance	Until service terminated

Wage and salary records (including overtime)	7
Waste Transfer Notes	3
Withholding tax statements	7
Workmen's Compensation records	3

2.5. RIGHTS RESERVED BY THE COMPANY

The Company reserves the right to monitor, audit, screen, and preserve Company information as the Company deems necessary, to maintain compliance with these Policies and all relevant provisions of the Promotion of Access to Information Act 4 of 2013 (POPIA). Any distribution, unauthorised use, or benefit from Company information by an employee or user, in contravention of these Policies may result in disciplinary action being taken by the Company. The use of any system in such a way that breaches any of the provisions of these Policies, will be reported to the Information Officer at the Company, which may lead to further disciplinary action being taken.

2.6. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of these Policies may result in disciplinary action being taken against the employee or user in question. Such disciplinary action will be taken in accordance with the Company's disciplinary code and may include the termination of employment for employees of the Company, or cancellation of contractual relations in the case of other users, such as contractors or consultants.

2.7. POLICY AWARENESS AND UPDATE

Training and awareness:

The requirement for these Policies will be explained in detail in the Company's induction program, in the case of employees of the Company. Further training regarding these Policies will be offered from time to time by the Company. The Company will specifically make users who are not employees of the Company aware of these Policies.

Dissemination:

These Policies will be made available on the Company's website, intranet, or notice boards.

Review:

These Policies will be reviewed from time to time to ensure ongoing compliance with POPIA. Such revisions will take place at least annually.

2.8. INTERNAL DOCUMENT APPROVAL

Information Officer Name	Signature	Date
Mrs Paula Gageiro		23 June 2021

2.9. DOCUMENT VERSION CONTROL

Version	Date	Summary of Changes
