DATA RETENTION, STORAGE AND DISPOSAL POLICY

Effective Date	Version Reference	Approved By
	1	

1 **DEFINITIONS**

In this Policy (as defined below), unless the context requires otherwise, the following words and expressions bear the meanings assigned to them and cognate expressions bear corresponding meanings –

1.1 "**Company**" means Kruinkloof Bushveld Estate NPC;

1.2 "**Data Retention Matrix**" means the retention schedule attached to this Policy as Annexure "**A**";

1.3 "**data subject**" means the person (natural or juristic, where applicable) to whom the personal information relates;

1.4 "**de-identify**" in relation to personal information of a data subject, means to delete any information that: (a) identifies the data subject; (b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or (c) can be linked by a reasonably foreseeable method to other information that identifies the data subject;

1.5 "**destruction**" means the process of destroying or deleting a record, beyond any possible reconstruction;

1.6 "**ECTA**" means the Electronic Communications and Transactions Act No. 25 of 2002;

1.7 "**Information Officer**" means the employee appointed as the Company's information officer, responsible for ensuring the Company's compliance with POPIA and PAIA, and overall responsibility for this Policy;

1.8 "**PAIA**" means the Promotion of Access to Information Act No. 2 of 2000;

1.9 "**personal information**" has the meaning set out in section 1 of POPIA, and includes "special personal information" as defined in section 26 of POPIA;

1.10 "**Policy**" means the record retention, storage and disposal policy contained in this document, as amended and updated from time to time;

1.11 "**POPIA**" means the Protection of Personal Information Act No. 4 of 2013;

1.12 "**process**" means any operation or activity whether or not by automatic means, concerning records including collecting, receiving, recording, organising, collating, storing, updating, modifying, retrieving, altering, consulting or using, disseminating, distributing or making available and merging, linking, blocking, degrading, erasing, destroying records;

1.13 "**record**" means any recorded information –

1.13.1 regardless of form or medium, including any of the following:

1.13.1.1 writing on any material;

1.13.1.2 information produced, recorded or stored by means of any tape recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

1.13.1.3 label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

1.13.1.4 book, map, plan, graph or drawing;

1.13.1.5 photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

1.13.2 in the possession or under the control of the Company;

1.13.3 whether or not it was created by the Company; and

1.13.4 regardless of when it came into existence;

1.14 "**records management**" is a process of ensuring proper creation, maintenance, use and disposal of records throughout their lifecycle to achieve efficient, transparent and accountable governance;

1.15 "**records system**" means an information system for capturing, managing and providing access to records and may consist of records management software or non-technical processes for records management;

1.16 "**restriction**" means to withhold from circulation, use or publication any record, but not to delete or destroy such record; and

1.17 "**special personal information**" means any personal information that is more sensitive than ordinary personal information and which requires a higher level of protection including personal information about sexual orientation, criminal behaviour, ethnicity, trade union membership and political views.

2 INTRODUCTION

2.1 The Company must comply with its obligations under certain laws whenever it processes personal information relating to data subjects, including its staff, customers, suppliers and any other individuals we interact with.

2.2 This includes the obligation not to process any personal information which permits the identification of data subjects for any longer than is necessary and the purpose of this policy is to assist the Company to comply with that obligation.

2.3 This Policy should be read alongside the Data Retention Matrix (**Annexure A**) and which provides guideline data retention periods for various different types of personal information we hold.

2.4 Compliance with this policy will also assist the Company to comply with our 'data minimisation' and accuracy obligations under data retention and disposal laws which require Company to ensure that it does not retain personal information, which is irrelevant, excessive, inaccurate or out of date.

2.5 A failure to comply with data retention and disposal laws could result in enforcement action against the Company, which may include substantial fines, significant reputational damage and potential legal claims from individuals. It can also have personal consequences for individuals in certain circumstances i.e. criminal fines/imprisonment or director disqualification.

2.6 Compliance with this Policy will also assist in reducing the Company's information storage costs and the burden of responding to requests made by data subjects under data protection laws such as access and erasure requests.

2.7 The Company is also required under data protection laws to inform data subjects about how long the Company will retain their personal information in our privacy notices.

2.8 This Policy is for internal-use only and cannot be shared with third parties, customers or regulators without prior authorisation from our Information Officer.

3 PURPOSE OF THIS POLICY

3.1 The primary purpose of this Policy is to ensure that records, irrespective of the format or medium thereof, that are received or created by the Company in the performance of its functions and in the execution of its business activities, are managed in such a manner that promotes good governance and compliance with applicable legislation.

3.2 The objectives of this Policy are –

3.2.1 To ensure that all records:

3.2.1.1 are retained in an appropriate manner, having regard to the content of the record;

3.2.1.2 are retained for an appropriate period of time, having regard to statutory obligations, business requirements and industry best practices;

3.2.1.3 which are required for evidentiary purposes, are kept in a manner that ensures their admissibility;

3.2.1.4 containing personal information and special personal information are retained and destroyed / deidentified in the manner required by law;

3.2.2 To ensure that the operational business needs of the Company are met in respect of records; and

3.2.3 To ensure that record management and destruction is done in an orderly and efficient manner and is properly recorded.

3.3 Records shall be controlled as specified in this Policy because they provide evidence of conformity to requirements and of the effective operation of the quality management system. Various statutes which specify minimum retention periods for certain records must be considered. As a general rule the retention of records should be kept at minimum (statutory) levels. Documents not required for retention purposes (legally or operationally) should be disposed of in accordance with the process described in this Policy.

4 SCOPE AND APPLICATION

4.1 This Policy applies to all Company staff, contractors, consultants, advisors and service providers that may deal with the Company records and covers all records in whatever medium such records are contained.

4.2 This Policy covers all records which are processed by the Company including those listed in the Data Retention Matrix, irrespective of the media on which such records are created or stored. This includes (i) paper or hardcopy records; (ii) electronic or softcopy records (word documents, database, emails, spreadsheets, power-point presentations etc.); (iii) scanned images, photographs, external storage media (CD-ROMS, flash drives, video tapes).

4.3 This Policy impacts upon the Company's work practices for all those who (i) create records; (ii) have access to records; (iii) have any other responsibilities for records, for example storage and maintenance responsibilities; (iv) have management responsibility for staff engaged in any of these activities, or manage, or have design input into record systems including information technology infrastructure.

4.4 This Policy therefore applies to –

4.4.1 all persons within the Company's organisation including employees (permanent, fixed-term and part-time) and also to all agents, subsidiaries, consultants, contractors, advisors and service providers who have access to any the Company records; and

4.4.2 records located anywhere including at the Company's premises, at the homes of employees, on the premises of service providers and at offsite storage facilities.

4.5 Each employee, contractor, consultant, advisor, service provider or any other third party who has access to or control over any of the Company records must return all such records to the

Company upon the end of their employment or service with the Company or the expiration of the relevant services agreement with the Company.

5 RESPONSIBILITIES AND DATA INVENTORIES

5.1 Records management and record systems that facilitate the use of records are a responsibility shared by all employees.

5.2 The Information Officer is ultimately responsible for the identification, storage, protection, retrieval and disposition of records and is expected to make himself familiar with the requirements for record management as prescribed by this Policy as well as any applicable legislation.

5.3 The Information Officer will retain a record of the training provided to personnel to ensure that they understand the Company's data retention and destruction obligations, their own responsibilities and the internal processes they need to follow. The Information Officer retains ultimate responsibility for the implementation of this Policy.

5.4 The Information Officer is ultimately responsible for ensuring that all information assets containing personal information are retained and destroyed in accordance with this Policy and the Data Retention Matrix. He must implement measures to ensure that they can identify when a retention period is due to expire, so that they can carry out a review and determine whether the personal information should be deleted or destroyed. In addition, the Information Officer should carry out periodic reviews at least annually of the personal information contained in the information assets that are within their control (even if that personal information is not covered by a retention period contained in the Data Retention Matrix), to determine whether it is being retained and destroyed in accordance with this Policy. The Information Officer may delegate routine tasks, where appropriate.

6 RECORDS AND RECORD SYSTEMS

6.1 In determining the appropriate storage mechanism / record system for a particular record, the Data Retention Matrix should be consulted as well as the Information Officer. The Data Retention Matrix sets out the required format for specified types of records. The actual storage mechanisms need to take cognisance of a number of factors including –

6.1.1 the content of the record – does it contain personal information or confidential information;

6.1.2 the purpose of the record – does it need to be easily accessible;

6.1.3 cost of storage; and

6.1.4 level of security required. In this regard, physical security and technical security are of equal importance.

6.2 In respect of paper / hard copy records, the following should be considered when determining the appropriate storage mechanism –

6.2.1 protection against loss due to theft, fire or water damage;

6.2.2 location of records which are hosted offsite;

6.2.3 access control to files containing records, especially those containing sensitive information;

6.2.4 transport to and from offsite storage facilities;

6.2.5 good filing practices – ensuring that records are kept in an organised and orderly manner which allows for easy retrievability and use; and

6.2.6 whether a third party is responsible for storage and if so, if there is a written agreement in place with such third party which is aligned with the requirements of this Policy and applicable legislation.

6.3 In respect of electronic / soft copy records, the security and storage of such records should be carried out in accordance with the Company's IT policies and procedures for access controls and for details on the format or encryption of relevant records in order to secure their confidentiality, integrity and accessibility of the records. Further, the following should be considered when determining the appropriate storage mechanism –

6.3.1 the temperature, humidity and magnetic fields where servers are located;

6.3.2 password protection, antivirus and access control mechanisms;

6.3.3 location of records which are hosted offsite;

6.3.4 back-up requirements and redundancy; and

6.3.5 whether a third party is responsible for storage and if so, if there is a written agreement in place with such third party which is aligned with the requirements of this Policy and applicable legislation.

6.4 Where any third party service provider stores records or otherwise processes records on behalf of the Company, a written agreement must be in place with such service provider which obliges the service provider to comply with any instructions of the Company in relation to records, to implement security safeguards consistent with the requirements of this Policy, to assist the Company with complying with any regulatory or business requirements in relation to access to records, to allow the Company to audit the premises and record systems in place and to, at the Company's request, destroy or return any records and certify such destruction or return to the Company.

7 SECURE DELETION/DESTRUCTION OR ANONYMISING DATA

7.1 A record may only be destroyed if the relevant record retention period has expired and no exceptions to such destruction applies (including a legal requirement to maintain the record or a specific hold has been placed on the destruction of the records in question). In which case, the record must first be reviewed the Information Officer. The following actions may be taken pursuant to such review –

7.1.1 Destruction of the record;

7.1.2 Retention of the record for a further period; or

7.1.3 Archiving of the record.

7.2 **Recording the Disposal Decision**:

7.2.1 As a first step, the nature and contents of any record being considered for disposal should be ascertained. No record should be designated for disposal unless this has been done. Depending on the complexity of the document, this should only be done by individuals who possess sufficient operational knowledge to enable them to identify the record concerned and its function within the Company. Typically, the review should be done by the Information Officer in consultation with other relevant stakeholders (such as legal advisers, the Information Officer, external audit or regulatory bodies).

7.2.2 Any decision regarding whether to destroy a record should take the following into account:

7.2.2.1 Applicable legislative and regulatory requirements;

7.2.2.2 Costs associated with continued storage versus costs of destruction;

7.2.2.3 The legal and reputational risks associated with retaining, destroying or losing control over the record;

7.2.2.4 Whether the record has any long-term historical, statistical or research value; and

7.2.2.5 Whether the record may be required for investigations, litigation or similar proceedings;

7.2.3 Destruction should be documented by keeping a register of the record destroyed, the date and the name of the Information Officer that authorised the destruction. When and why a document is destroyed is particularly important in the event of a claim against the Company. The Company shall fully document and approve the destruction process. The applicable statutory requirements for the destruction of information, particularly requirements under applicable data protection laws, shall be fully observed. The prescribed data destruction record template is contained in Annexure "**B**" to this Policy.

7.3 **Factors to Consider before Destroying Records**

7.3.1 The destruction of a record should not take place other than in accordance with this Policy. Before destroying a record, it must be confirmed with the Information Officer that –

7.3.1.1 there are no pending access requests in terms of PAIA or POPIA in relation to the record;

7.3.1.2 there is no restriction on processing in relation to the record;

7.3.1.3 the record is no longer required by any part of the business;

7.3.1.4 there is no legal or regulatory reason to maintain the record;

7.3.1.5 the record will not be required for the purposes of proof or in any litigation or investigation; and

7.3.1.6 there is no improper motive for the destruction of the record (for example, to destroy evidence).

7.3.2 The Company shall maintain and enforce a detailed list of approved destruction methods appropriate for each type of record archived whether in physical storage media such as CDROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives or in database records or backup files.

7.4 **Destruction of Hard Copy Records**

Personal information or confidential or restricted information must be disposed of in a manner that maintains the confidentiality of the record. While records not containing personal information or other confidential information can be thrown into bins, confidential records (including those containing personal information) must be shredded and/or placed in paper rubbish bins designated for collection by an approved disposal service provider. All copies of paper records marked for destruction, whether made for security or back-up purposes, must be destroyed in the same manner.

7.5 **Destruction of Soft Copy / Electronic Records**

Electronic records contained on servers or storage devices shall be destroyed by the physical destruction of that media or by completely wiping the electronic record such that it can never be reconstructed. Personal data records or confirmation and restricted records must be disposed of as confidential waste and in some cases, where records are not fully destroyed but are anonymised instead, appropriate steps need to be taken to ensure that the process of anonymisation (i.e. the process of turning a record into a form which does not identify the persons to whom the information relates). A record of destruction must be certified and all back-up copies of the electronic records should also be destroyed in the same manner.

7.6 **Destruction Exceptions and Litigation Holds**

There may be valid reason for a record not to be destroyed in accordance with the destruction requirements of this Policy. In this case, an exception request should be lodged with the Information Officer specifying the reason for the exception, which may include a client or business requirement, a legal requirement or there may be a vital historical purpose for such record/s being retained. In addition, a litigation hold may also be issued (by the Company Legal Department) in respect of any information or records that form part of or are related to any litigation proceeding, which records should be retained and not destroyed in accordance with this Policy. Such litigation hold may be retained in place for the relevant records to be preserved for as long as the litigation proceeding is under way or the threat of pending litigation, regulatory action or government action or order is applicable.

8 RETENTION OF ELECTRONIC RECORDS UNDER THE ECTA

8.1 The legal framework in respect of electronic communications, including the use of electronic copies as opposed to hard copies, is largely set out in the ECTA.

8.2 The ECTA applies in respect of any electronic transaction or data message and recognises that information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message. In other words, the ECTA applies to all electronic records.

8.3 In assessing the evidentiary weight given to an electronic record, regard must be had to –

8.3.1 The reliability of the manner in which the electronic record was generated, stored and communicated;

8.3.2 The reliability of the manner in which the integrity of the electronic record was maintained;

8.3.3 The manner in which the originator was identified; and

8.3.4 Any other relevant factor.

8.4 In terms of the ECTA, where the law requires that information be presented or retained in its original form, the requirement of originality is met by retaining an electronic record if –

8.4.1 the record is in the format in which it was generated, sent or received, or in a format which can be demonstrated to preserve the integrity of the information (i.e. that the information has remained unaltered, complete and accurate);

8.4.2 information contained in the record is accessible to be usable for subsequent reference; and

8.4.3 that information is capable of being displayed and or produced to the person to whom it is to be presented.

8.5 In light of the above, it is extremely important to take all reasonable steps to ensure the reliability and integrity of any electronic record system used by the Company. It is also important to maintain evidence of the steps taken to preserve the integrity and authenticity of records stored electronically.

9 RECORDS CONTAINING PERSONAL INFORMATION

9.1 The Company is obliged to respect the privacy of all data subjects. This includes complying with the provisions of POPIA insofar as they relate to records containing personal information.

9.2 All records should be assessed to determine whether they contain any personal information or special personal information. If you are unsure about whether a record contains this information, please contact the Information Officer.

9.3 In terms of POPIA, the Company may not retain personal information for a period longer than is necessary to achieve the purpose for which it was collected or processed and is required to delete, destroy (in such a way that it cannot be reconstructed) or de-identify the information as

soon as is reasonably practicable once the purpose has been achieved. This prohibition will not apply in the following circumstances –

9.3.1 where the retention of the record is required or authorised by law;

9.3.2 the Company requires the record to fulfil our lawful functions or activities;

9.3.3 retention of the record is required by a contract between the parties thereto;

9.3.4 the data subject (or competent person, where the data subject is a child) has consented to such longer retention; or

9.3.5 the record is retained for historical, research or statistical purposes provided safeguards are put in place to prevent use for any other purpose.

9.4 When the Company is no longer authorised to retain a record containing personal information, the Company is obliged to destroy, delete or de-identify such record. Any destruction or deletion of a record must be done in a manner that prevents its reconstruction in an intelligible form.

9.5 In instances where the Company utilises personal information for decision-making purposes, an additional requirement is imposed on the Company, namely that the records be retained for the period prescribed by law or code of conduct, in the absence of which, for such period which will allow a data subject a reasonable opportunity to access the records.

9.6 **Restricted Processing**

9.6.1 In certain instances, the Company is required to place a restriction on the processing of personal information.

9.6.1.1 In terms of POPIA, the instances where the Company must place a restriction on the processing are where –

9.6.1.1.1 the accuracy of such information is contested by the data subject;

9.6.1.1.2 the personal information is no longer required to achieve the purpose for which it was collected or subsequently processed (but has to be maintained for purposes of proof);

9.6.1.1.3 the processing is unlawful and the data subject requests the restriction of use; or

9.6.1.1.4 the data subject requests to transmit the data into another automated processing system.

10 DATA RETENTION MATRIX

10.1 All records must be characterised by their nature and purpose and must be retained in accordance with the requirements specified in the Data Retention Matrix unless an exception applies.

10.2 The Data Retention Matrix indicates –

10.2.1 the minimum retention period (derived from statute or business needs as indicated in the Data Retention Matrix);

10.2.2 the format in which the record must be retained;

10.2.3 the place of storage; and

10.2.4 the method of destruction.

10.3 The retention periods listed in the Data Retention Matrix are examples of the minimum periods as prescribed by the relevant legislation. The Data Retention Matrix covers only certain records used in our business. Unless otherwise stated, the retention period is the minimum number of years from the date of the last entry in the record. Where there is no statutory requirement, the retention is based on the conservative period of 5 years used in general practice. Where different legislation is applicable to the same record, the longer retention period has been selected.

10.4 Notwithstanding the Data Retention Matrix, guidance on each specific record should first be sought from the Information Officer, prior to the default position being implemented.

11 EFFECTIVE DATE AND CHANGES TO THIS POLICY

11.1 The Company reserves the right to change this Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Policy.

11.2 Any changes to this Policy must be approved by the board of directors of the Company.

12 ENFORCEMENT AND REPORTING OF BREACHES OF THIS POLICY

12.1 Any noncompliance with the terms of this Policy could have serious legal and reputational repercussions for the Company and may cause significant damage to the Company. Therefore, any noncompliance could lead to disciplinary action being taken against the relevant employees.

12.2 Should any employee become aware of any noncompliance with the terms of this Policy, they are required to immediately report this to the Information Officer.

Annexure "A"

Data Retention Matrix

1. Statutorily prescribed retention periods and regulatory retention periods:

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Accounting / Tax	Finances	Annual/quarterly financial reports, balance sheets, accounts payable, purchase orders, financial and tax related audits, invoices, taxes, audited financial accounts, records relating to reserves, accounting records, expense reports, financial statements, bank accounts and other accounts, inventory, bookkeeping vouchers (e.g. copies of invoices, tax assessments, wage lists, payment instructions, travel expense accounting), risk reports/ models, records of cumulative client assets, source documents to substantiate books of account, returns and reports.	Yes – 5 (Five) years.	Tax Administration Act, No 28 of 2011 ("**TAA**") (Section 29)	For any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Companies Act No. 71 of 2008 ("**Companies Act**"), such as annual financial statements, the company is required to keep such records for a period of 7 (seven) years.	N/A	(i) Companies Act - Section 24(1) requires that the information must be kept in written form, or other form or manner that allows that information to be converted into written form within a reasonable time; and (ii) the TAA – Section 30, requires that records be kept a) in their original form in an orderly fashion at a safe place; b) in any other form (including electronic) as may be prescribed by the South Africa Revenue Services ("**SARS**") Commissioner in a public notice; or c) in a form specifically authorised by a senior SARS official.	(i) Companies Act – Section 25, requires records to be accessible at or from the company's registered office or another location within South Africa; (ii) Tax records must be kept in South Africa in order to be available for inspection by a SARS official, per Section 30 of the TAA.	

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Corporate Entity	Corporate records	Company Secretarial, certificate of incorporation, title, deeds, board of directors, shareholder records, stock certificates, contracts, agreements, internal/external audit, board minutes, register of shareholders, memorandum and articles of association, register of charges, share transfer documentation, written resolutions, company registers, powers of attorney, annual and quarterly reports, merger treaties, board resolutions, resolutions (i) of stockholder meetings; and/or (ii) regarding amendments to the memorandum of association and related minutes, records on subscriptions to shares, reports of the executive board, documentation regarding capital share payments, register of loan agreements between the company and its officers, documents relating to real/ personal property, intellectual property, technical and IT designs/source code/process flows/user documentation and licenses, product documentation, patents, facilities related agreements including supplier agreements, insurance policies and certificates accident records and documentation related to inspections and hazardous materials, fire certificates, pension scheme documents, access control records, security reports,	Yes – As a general rule, for any documents, accounts, books, writing, records or other information that a company is required to keep in terms of the Companies Act, the company is required to keep such records for a minimum period of 7 (seven) years.	Companies Act, Sections 24, 50 and 85.	(i) Where a company has been in existence for shorter than 7 (seven) years, the company is only required to keep information for that period for which has been in existence (Section 24(2)); (ii) For documents relating to: a) registration certificates; securities registers and uncertificated securities register; register of company secretary and auditors, the company is required to keep such documents indefinitely - (Section 85(1) and Section 50; and b) For real property records such as a title deed, the company is required to keep such documents indefinitely, or until such time that the relevant property is disposed of.	N/A	The Companies Act requires that the information must be kept in written form, or other form or manner that allows that information to be converted into written form within a reasonable time.	Companies Act – Section 25(1)(a), requires records to be accessible at or from the company's registered office or another location within South Africa.	

		building drawings and plans, building inspections and safety reports business continuity plans.							

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Customers and transactions	Records relating to setting up customer accounts and ongoing work with customer including details of transactions entered into by company	Product/service agreements, quotations and order documents, order tracking, order audit trail, statements of work, delivery schedules, terms and conditions, price/volume data, data protection agreements, client advice records, contact details, financial analysis records provided to customer, particulars of each client's assets and liabilities, summaries of telephone conversations relating to orders and transactions, credit records, customer payment , agreements and transactions with third parties other than clients and employees (e.g. suppliers, service providers); Environmental/health and safety policies, claims and records.	Yes – 5 (five) years: (i) in relation to documents relating to establishment of business relations, from the date on which the agreement was terminated; and (ii) in relation to records of transactions concluded, from the date on which the transaction was concluded.	Standard Practice / Financial Intelligence Centre Act, Section 23.	N/A	N/A	Financial Intelligence Centre Act only provides that records kept in terms of sections 22 and 22A may be kept in electronic form but must be capable of being reproduced in a legible format. Where records are kept by a third party on behalf of a company, the company must have free and easy access to the records and the records are readily available to the Centre (per the Financial Intelligence Centre Act - Section 24) and the relevant supervisory body for the purposes of performing its functions in terms of the Financial Intelligence Centre Act.	N/A	

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Consumer Protection	Records relating to activities performed in an intermediary capacity and records of promotional competitions	Record of information given to the consumer in relation to intermediary activities, written instructions from consumers, terms and conditions of promotional competitions, list of prizes to be awarded, offer to participate.	Yes - 3 (three) years.	The Consumer Protection Act - section 27(3)(b) read with regulation 9 and 10 in relation to an intermediary and section 36 (11)(b) read with regulation 11 in relation to promotional competitions.	N/A	N/A	The Consumer Protection Act – regulation 10(3) provides that records be kept in an appropriate electronic or recorded format, which must be easily accessible and readily reducible to written or printed form.	N/A	

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Financial Services	Recordings relating to the provision of financial services	Cancellations of transactions by clients of the provider; complaints received; feedback on complaint resolution; statement of non-compliance with Financial Advisory and Intermediary Services Act and reasons therefore; verbal and written communications concerning a financial service rendered.	Yes - 5 (five) years.	The Financial Advisory and Intermediary Services Act - section 18 and the General Code of Conduct for Authorised Financial Services Providers and Representatives ("**the Code**") – Section 3(2).	Only in so far as the financial service provider has been exempt of its document retention obligations by the Registrar.	N/A	Financial Advisory and Intermediary Services Act provides that records may be kept in an appropriate electronic or recorded format, which are accessible and readily reducible to written or printed form and the Code provides that providers are not required to keep the records themselves but must ensure that they are available for inspection within 7 (seven) days of the registrar's request. Records may be kept in an appropriate electronic or recorded format, which are accessible and readily reducible to written or printed form.	N/A	

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)	Relevant statute (Identify statute name and relevant section only)	Exceptions to retention periods	Reason for retention period if no statutory requirement present	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Employees and HR	Records relating to employees	Employee records and payroll, personnel files, job applications, work authorisations, pension, CVs, background checks,	Yes – 3 (three) years	Basic Conditions of Employment Act No 75 of 1997 ("**BCEA**") –	(i) The Compensation for Occupational Injuries and Diseases Act 130 of 1993 ("**COIDA**"), Section 81(1) and (2), requires employers to retain the following information for a period of 4 (four) years from the date of last entry into the relevant record: a) register, record or	N/A	The Occupational Health and Safety Act 85 of 1993 - General Administration	The Occupational Health and Safety Act 85 of 1993 - General Administration	

		licenses / reviews / examinations, training records, personal dealing, injuries/accidents, health and safety, employee contracts, personnel records (including director's investment policy), records of benefits, disability records, unsuccessful applications, expense records, pension and investment policy, temporary employee contracts, attendance records, profit sharing agreements, medical files, test papers, references, job descriptions, employment passes/visas/work permits, drug testing and interview notes.		Section 29(4) and Section 31; and Labour Relations Act 66 of 1995 ("**LRA**") – Section 205(1) – (2) and Section 205(3) read with Schedule 8 – Section 5	reproduction of the earnings, b) time worked, c) payment for piece work and overtime and d) other prescribed particulars of all the employees; (ii) The Occupational Health and Safety Act 85 of 1993 -Section 20(2), under the following Regulations: General Administration Regulations 2003, 9(1) and 5(1) Asbestos Regulations, 2020, Regulation 23 a requires certain information to be kept for 50 years, Hazardous Biological Agents Regulations, 2001, Regulation 9(1) and (2); Hazardous Chemical Substance Regulations, 1995, Regulation 9; Lead regulations, 2001, Regulation 10; and Noise Regulations, Regulation 11, requires certain information to be kept for 30 – 40 (thirty to forty) years. Other exceptions include that staff records (after employment terminated) are to be retained for 7 (seven) years (per BCEA and COIDA); time and piecework records are to be retained for 7 (seven) years (per BCEA and COIDA); UIF contributor's cards are to be retained until service is terminated (per BCEA -Section 29(4) and per Unemployment Insurance Act, No 63 of 2002 – Section 56(2)(c)) and wage and salary records (including overtime) should be retained for 7 (seven) years (per TAA, BCEA and COIDA). In respect of payroll and wage records, details of overtime worked, bonuses, expenses and benefits in kind, given their potential relevance to pay disputes they should be retained for seven years after employment ends (standard practice – a longer retention period is therefore prescribed). LRA, Section 205(3) – requires employers to retain prescribed details of any strike, lock-out or protest action involving its employees Indefinitely.		Regulations 2003, 9(1) and 5(1) provides that records of injuries/accidents must be recorded and retained in the prescribed form annexed to the Regulations for a period of three years, which must be easily accessible and readily available for inspection by an inspector.	Regulations 2003, 9(1) and 5(1) provides that records of injuries/accidents must kept at a workplace or section of a Workplace.	

Category	**Description**	**Examples of documents/data in category (these are examples only and should not be considered**	**Statutorily prescribed retention period**	**Relevant statute (Identify statute name and relevant**	**Exceptions to retention periods**	**Reason for retention period if no**	**Record format (paper,**	**Place of storage**	**Destruction method**

		exhaustive)	(Yes/No – if yes, please include relevant period)	section only)		statutory requirement present	media, electronic etc.)		
Legal / Regulatory	Required reports to regulatory enquiries	Regulatory submissions, legal/regulatory enquiry, investigation, complaints, lawsuits, subpoenas, hearings, litigation files, legal correspondence. records of regulatory relationships, records relating to management of pension scheme, details of risk management systems, documents relating to tax investigation, financial promotion records, records of lending policy, fraud reports to regulators, money laundering reports, Insurance claims, compliance records including reports & fillings, regulatory audit reports, succession files, records required to demonstrate compliance with regulatory requirements, internal organisation schemes, records on internal control systems, records on internal audits, reports to management, IT-emergency documents, records on information on private and corporate customers and transactions (with regard to money laundering and insider trading).	No – Indefinitely	N/A	N/A	Standard Practice	Not specified	Not specified	
Category	**Description**	**Examples of documents/data in category (these are examples only and should not be considered exhaustive)**	**Statutorily prescribed retention period (Yes/No – if yes, please include relevant period)**	**Relevant statute (Identify statute name and relevant section only)**	**Exceptions to retention periods**	**Reason for retention period if no statutory requirement present**	**Record format (paper, media, electronic etc.)**	**Place of storage**	**Destruction method**
General	Correspondence and publications (to the extent not addressed above)	General correspondence (electronic or otherwise), press releases, publications.	3 (three) years	Standard Practice	N/A	Subject to certain exceptions, a civil claim may be brought against a company for a period of up to 3 years in South Africa (because the general prescription	N/A	N/A	

						period in South Africa is 3 years)			

2. Standard practice retention periods

The retention periods below apply generally to the extent that there are no statutorily prescribed retention periods or regulatory periods. Accordingly, the following guideline retention periods are standard practice of the Company.

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Standard practice retention period	Exceptions to retention periods	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Employment related	Recruitment records (pre-employment)	Completed online application forms or CVs; Equal opportunities monitoring forms; Assessment exercises or tests; Notes from interviews and short-listing exercises; Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references; Criminal records checks.	For unsuccessful candidates 6 (six) – 12 (twelve) months after notifying candidates of the outcome of the recruitment exercise. These records may be transferred to a successful candidate's personnel file if they are relevant to the ongoing employment relationship.	Only in so far as the BCEA or LRA retention periods do not apply to the relevant records.	N/A	N/A	

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Standard practice retention period	Exceptions to retention periods	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Employment related	Collective agreements	Any copy of a relevant collective agreement, collective workforce agreements and past retained on an employee's record will remain while agreements that could affect present employees.	While employment continues and for seven years after the contract ends.	Only in so far as the BCEA or LRA retention periods do not apply to the relevant records.	N/A	N/A	

Category	Description	Examples of documents/data in category (these are examples only and should not be considered exhaustive)	Standard practice retention period	Exceptions to retention periods	Record format (paper, media, electronic etc.)	Place of storage	Destruction method
Client records	Client records – Contracts	Any contracts with clients.	These documents must be kept for a period of at least 5 (five) years after the cancellation of the contract.	N/A	N/A	N/A	

ANNEXURE "B" – DESTRUCTION RECORD TEMPLATE

Date of Destruction	Type of Record Destroyed	Location Where Record is Stored	Method Used to Destroy the Record	Serial Number of Hard Drive or Storage Devices Destroyed, where applicable.