Knowledge Integration Dynamics (Pty) Ltd

DATA PROTECTION and RETENTION

POLICY & GUIDELINES

Version	1
Publishing Date	1 July 2021
Last Review Date	n/a
Frequency of Review	annually
Next Review Date	1 July 2022
Policy Owner	Compliance Department
Responsible Business Unit/s	Information Officer and Deputy Information Officer/s

Enquiries:

Knowledge Integration Dynamics Pty (Ltd) - head office situated at:

KID House, 812 Hammets Crossing Office Park,
2 Selborne road, Maroeladal, Johannesburg,
South Africa, 2191

Contact: 011-462-1277

1. Introduction

This policy is owned by Knowledge Integration Dynamics Pty (Ltd) and its subsidiaries (KID group of companies) and covers the protection, retention and disposal of all data held by KID. “Data” and “information” is used interchangeably to mean the same thing.

The KID group of companies includes:

Knowledge Integration Dynamics Pty (Ltd)	Reg# - 1999/07653/07
and subsidiaries:	
IT and Business Services (SA) Pty (Ltd).	Reg# - 2002/020436/07
Infoflow Pty (Ltd).	Reg# - 2005/037547/07
KID Enterprise Information Management Pty (Ltd).	Reg# - 2014/162453/07
Information Dynamics Pty (Ltd).	Reg# - 2014/184236/07
Centerfield Software Pty (Ltd).	Reg# - 2002/011957/07
Cubic Blue Pty (Ltd).	Reg# - 2010/000921/07

This policy prescribes the maintenance of the organization’s data for a pre-determined length of time. Different types of data require different lengths of retention and computer systems and applications have added increased complexity to the issue. In addition to describing how long various types of information must be maintained whilst in possession, it also high-lights the procedures for retaining/archiving/protecting the information and gives guidelines for destroying the information.

The information contained in this policy represents the actions taken by KID concerning all its data and/or information acquisition, storage, usage and/or deletion.

Data and/or information includes that of KID’s clients, partners, service providers, staff and other information as necessary for its operation.

KID adopts this data / information retention policy to ensure that we retain all information that we have an obligation to keep and that information is deleted where there is no business or legal requirement for it to be retained. The reasons for the necessity of this policy include:

- To comply with legal and regulatory requirements.
- To support KID to bring / defend legal proceedings or if KID is under investigation.
- To preserve information that has operational and historical value.

KID ensures that this Policy is implemented and that files and documents are regularly reviewed and disposed of when these are no longer needed.

This policy makes reference to, and should be read alongside, the Data Retention Schedule (refer to the section below in this document).

It is everyone’s responsibility to ensure that the Policy is adhered to; however, automation should be in place wherever possible to ensure that data is correctly managed as per the Data Retention Schedule.

2. Definitions

“Account Data” consists of client agreement, cardholder, bank data and/or sensitive authentication data.

“Anonymisation” is the process of turning data into a form which does not identify individuals. It is a type of information sanitization whose intent is privacy protection.

“Archiving” is the process of moving data that is no longer actively used to a separate storage device or location for retention.

"Asset Owner" is the Functional or Business Line Head who is responsible for the Data Asset (or within whose function or business line the Data Asset resides or is used).

"Data Asset" is any item or entity that comprises data. For example, databases are data asset that comprise records. A data asset may be a system or application output file, database, document, or webpage. A data asset may also include a means to access data from an application.

"Data Processing" is the collection and manipulation of data to produce meaningful information. Processing includes transformation, accessing, updating, transferring, destruction and any other manipulation of data.

"Data Retention" is usually required to meet applicable legal or contractual obligations or meet business objectives. Retention Periods are determined accordingly. For Personal Data it must be no longer than necessary to protect the rights and freedoms of individual data subjects in accordance with this policy. In some cases, retention may be in the form of "Archival", to preserve storage space or bandwidth on the system or container originally employed for Active Use processing.

"Destruction" is defined as physical or technical destruction sufficient to render the information contained in the document irretrievable by ordinary commercially available means.

"Document" as used in this Policy, is any medium which holds Information used to support an effective and efficient organizational operation. Examples of Documents include: (a) Policies (b) Agreements (c) Procedures (d) Templates.

"Financial Records" is pieces or sets of information related to the financial health of a business. The pieces of data are used by internal management to analyse business performance and determine whether tactics and strategies must be altered

"Personal Data" (also "Personally Identifiable Information") is any information relating to an identified or identifiable natural person (the "Data Subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"PCI DSS" The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes. It is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. It was created to increase controls around cardholder data to reduce credit card fraud. Validation of compliance is performed annually.

"Record" as used in this policy, is any medium which holds information or evidence about a past event. Examples of Records include: (a) Case records (b) Reports (c) Minutes (d) Video and audio recordings (e) Data generated by physical access control systems

"Retention" is the continued processing of data, after the initial "Active Use" has achieved the purpose for which the data was originally collected.

3. Data Retention Schedule

The Data Retention Schedule is a comprehensive list of information items, held by KID, which may be retained for specified periods of time for legal, statutory, fiscal, historical or operational reasons. This must be read in conjunction with the KID – POPI Internal Approval Policy.

	Record / Data Type	On active System	Off System - Maximum period
1	Medical Record	Duration of employment	30 years or based on contractual commitments and applicable regulations
2	Occupational Health Assessment Record	4 years	30 years or based on contractual commitments and applicable regulations

3	Human Resources (Staff) Record	Duration of employment	Based on contractual commitments and applicable regulations
4	Customer Record	Duration of service / product licence	Based on contractual commitments and applicable regulations
5	Medical and Security Assistance Case Record	3 years	3 years
6	Card Services Record		
	(a) CVV	72 hours	72 hours
	(b) Inactive card data	90 days	90 days
	(c) Inactive case record - no PAN or CVV	2 years	3 years
7	Call Recordings	1 year	2 years
8	Audit Logs	3 months	1 year
9	Corporate Records (Registration, Directors, Shareholders, Minutes etc…)	Life of the entity	Life of the entity plus 15 years
10	Accounting and Financial Record	5 years	15 years or based on applicable regulations
11	Procurement and Contract Record Contract	Contract duration	Contract duration or based on applicable regulations
12	Tracker Record	2 years or based on contractual commitments	2 years or based on contractual commitments
13	Other Records	3 years or based on applicable regulations	3 years or based on applicable regulations

4. Retention Considerations

For the purposes of enforcing retention in accordance with this policy, each business unit / function is responsible for the Records and Documents it creates, uses, stores, processes and destroys.

Record and Document types shall be maintained by each business unit / function under guidance from the KID Information Officer.

NOTE:

There are certain occasions when information needs to be preserved beyond any limits set out in the Policy. The Policy must be reconsidered or suspended where a specific customer or document has information retained beyond the period specified in the KID Data Retention Schedule, in the following circumstances:

- Legal proceedings or a regulatory or similar investigation or obligation to produce information are known to be likely, threatened or actual.
- A crime is suspected or detected.
- Information is relevant to a company in liquidation or receivership, where a debt is due to KID.
- Information is considered by the owning unit to be of potential historical importance and this has been confirmed by KID management and/or Information Officer.

In the case of possible or actual legal proceedings, investigations or crimes occurring, the type of information that needs to be retained relates to any that will help or harm KID or the other side's case or liability or amount involved.

If there is any doubt over whether legal proceedings, an investigation or a crime could occur, or what information is relevant or material in these circumstances, the KID management and/or Information Officer should be contacted and take legal advice sought.

The Data Protection Act states that non-billable customer data / information should be retained only for a period where there is a business need. KID's policy is set for a maximum as determined by contractual agreements or dure to the circumstances as listed above, although some data will be deleted prior to this.

Throughout the data processing, for Information Security and Disaster Recovery/Business Continuity purposes, regular back-ups or copies may be created of the data. Retention periods of such back-ups should be only as long as required to fulfil this purpose. Back-up tapes should not serve as a replacement for data retention.

In addition, any retained information can only be used for the purpose for which it is stored.

5. Personally held electronic information

Personally held electronic information relates to an individual that has custody (or is in possession) of information in certain circumstances may cause KID to be:

- Legally bound to a certain course of action.
- Contracted to a supply or purchasing agreement.
- Construed as a business record of KID.

This information is stored in an uncontrolled system or an individual's Personal or Laptop Computer.

Personally held electronic information in these circumstances is also subject to the Data Retention and Destruction rules as documented in this policy, and the following directives also apply:

For email, electronically stored documents, texts, pictures, videos, recordings and files:

1. Any retention period relating to any electronically generated or modified file (including email) is governed by its content.
2. Each user of any computer system or software program is individually responsible for retaining or deleting electronic information in accordance with this policy.
3. All material that does not need to be retained should be deleted as soon as possible after receipt, creation or use.
4. Data stored in any computer or networked system (either on-line or offline, in personal folders or archives) must be reviewed at least every year. It is recommended that it is reviewed at least every 6 months needing a current good business reason for further storage.
5. Where it is possible, KID staff should store retained files on its shared, internal, network storage device.
6. Where a file is stored on another medium for information retention purposes, (paper, CD, disc etc), the original electronic file should then be deleted.
7. Each individual user is responsible for determining which files and electronic media should be retained as business records in accordance with this policy and their business unit requirements.
8. Retention periods should be governed by the creation date or issue date of the information, not from the date of the last data save.
9. Retention periods should be noted in any document footers for clarity purposes, where possible.

6. Data / Information Inventory

- Documents and Records should be organised into Data Assets such as SharePoint sites, databases or electronic information systems (examples would be a payroll and benefits system) to allow systematic, standardised management.
- Data Management outside of such systems must be reduced to a minimum.
- It is the responsibility of the respective Functional or Business Line Head to ensure that each Data Asset is registered on the Inventory by the nominated Asset Owner.

- Each Data Asset is subject to a specific retention period for the data, reflecting the legitimate basis justifying the need for and use of the data. Retention periods for different types of data will depend on the nature of such data.
- Data Asset Owners are to ensure that their Data Asset Inventory entries are reviewed, and if necessary updated, at least annually and every time significant changes are made to a process involving a Data Asset assigned to them.

7. Data / Information Security Measures

KID information must be both protected and disposed of in accordance with the KID security and privacy policy, using appropriate security classification.

KID endeavours to protect the personal data / information that it processes. The security measures that are put in place is to ensure that data protection and that no unauthorised personal accesses your personal data / information.

KID will take appropriate, reasonable technical and organisational measures to avoid loss of or unlawful access and usage of personal data / information.

The following operational controls are implemented within the KID environment.

- access controls to premises;
- confidentiality clauses in employment and supplier agreements;
- POPIA and data protection training.

ICT controls:

- Firewalls;
- Password protections on computers and laptops;
- Storage of electronic data in a cloud that is access controlled;
- Storage of hard copies of data / information of subjects in locked cabinets.

8. Data / Information Destruction

- All Data, whether held electronically, on individual employees' devices or on paper, should be reviewed on a regular basis to decide whether to destroy or delete any data in accordance with the designated retention period.
- Responsibility for the destruction of data included in the Data Asset Inventory falls to each Functional or Business Line Heads.
- Responsibility for the destruction of data included in local departmental document and record inventories falls to each Departmental Head.
- Personal Data or confidential or restricted information must be disposed of as confidential waste and be subject to secure electronic deletion or Anonymisation.
- Some expired or superseded contracts may only warrant in-house shredding.
- Paper Documents shall be shredded using secure, locked consoles designated in each office from which waste shall be periodically picked up by security screened personnel for disposal.
- The IT department shall maintain and enforce a detailed list of approved destruction methods appropriate for each type of information archived whether in physical storage media such as CD-ROMs, DVDs, backup tapes, hard drives, mobile devices, portable drives or in database records or backup files.
- The IT department 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 specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that the IT department subcontracts for this purpose. All external service providers must be thoroughly vetted and reviewed to ensure their full compliance with data protection requirements.

- Appropriate controls (as described in this policy) shall be in place that prevent the permanent loss of essential information of the company as a result of malicious or unintentional destruction of information.

Exceptions: The reasons may be a client requirement, business requirement, legal requirement or vital historical purpose.

9. Other advice / measures / disciplines

- The best defence against a search or a subpoena is to **minimize the amount of information** that it can reach. Every organization should have a clear policy on how long to keep particular types of information.

- **Do not destroy evidence**. You should never destroy anything after it has been subpoenaed or if you have reason to believe you are under investigation and it is about to be subpoenaed — destruction of evidence and obstruction of justice are serious crimes that carry steep fines and possible jail time, even if you didn't do the original crime. Nor should you selectively destroy documents — for example, destroying some intake files or emails but not others — unless it's part of your policy. Otherwise, it may look like you were trying to hide evidence, and again might make you vulnerable to criminal charges.

- **Destroying paper documents.** Just tossing your old membership rolls in the garbage is not the way to go. If you are concerned about the privacy of the documents that you throw away, you should destroy them before they go in the trash. At the very least you should run documents through a "cross-cut" paper shredder that will cut them in two directions and turn them into confetti, and then mix up the shreds from different documents to make them harder to put back together (documents cut in one direction by "strip-cut" shredders are very easy to put back together).

  If you have evidence giving you reason to believe that your trash is being or is about to be searched, you should also completely burn all of the shreds. Even if you're not particularly worried about someone searching your trash, you should still destroy or thoroughly erase any computer equipment or media that you throw out.

  If you destroy any of your papers and disks before throwing them out, you should try to destroy all of them, even the ones you don't need to keep private. If you don't destroy everything, anyone with access to your trash can will be able to quickly isolate the shreds of your private documents and focus on reconstructing them.

- Your web browser's watching you, so you have to **watch your browser**. You may have many things you'd like to keep private, but the point is that your browser is a security hole that needs to be plugged. You need to take regular steps to clear out all the stuff it's been storing, such as a history of the web sites you've visited and the files you've downloaded, cached copies of web pages, and cookies from the web sites you visit (which we will talk more about later). In particular, it's a bad idea to have the browser save your passwords for web sites, and it's a bad idea to have it save the data you've entered into web forms.

  If your computer is seized or stolen, that information will be compromised. So consider turning these features off completely. Not having these features is less convenient — but that's the security trade-off. Are you worried enough about your computer's security that you're willing to type a few extra times each day to enter a password or a web address?

- **When you delete computer files, really delete them**. When you put a file in your computer's trash folder and empty the trash, you may think you've deleted that file — but you really haven't. Instead, the computer has just made the file invisible to the user, and marked the part of the disk drive that it is stored on as "empty" — meaning, it can be overwritten with new data. But it may be weeks, months, or even years before that data is overwritten, and the government's computer technicians can often retrieve data that has been overwritten by newer files. Indeed, no data is ever really deleted, just overwritten over time, and overwritten again. The best way to keep those "deleted" files hidden, then, is to make sure they get overwritten immediately, and many times. Your operating system probably already includes software that will do this, and overwrite all "empty" space on your disk with "0"s, thereby protecting the confidentiality of deleted data.

- **Minimize computer logging**. If you run a network, an email server or a web server, you should consider reducing or eliminating logging for those computer and network services, to protect the privacy of your colleagues and your clients.

- Many instant messaging (IM) clients are set by default to log all of your IM conversations. You should **check the software's preferences** so you know what it's doing, and figure out how these logs fit into your retention policy. Will you clean them out every month or week? Or will you take the simple route and just set the preferences so that your IM client doesn't log any messages at all? You should consider such logs very sensitive. If you do insist on logging your IMs, all the more reason to make sure they are protected by encryption.

- **Destroying hardware and electronic media**. When it comes to CD-ROMs, you should do the same thing you do with paper — shred it. There are inexpensive shredders that will chew up CD-ROMs. Never just toss a CD-ROM out in the garbage unless you're absolutely sure there's nothing sensitive on it. If you want to throw a piece of hardware away or sell, you'll want to make sure no one can retrieve your data from it. So, before selling or recycling a computer, be sure to overwrite its storage media with gibberish first.

- **Make data hygiene a regular habit, like flossing**. The easiest way to keep this all straight is to do it regularly. If you think you face a high risk of government seizure, or carry a laptop around with you and therefore face a high risk of theft or loss, perhaps you should do it at the end of each day. If not, you might want to do it once a week.

  For example, at the end of each week you could:
  - Shred any paper documents or electronic media that are scheduled for destruction under your policy.
  - Delete any emails or other documents that are scheduled for deletion under your policy.
  - Clear your browser of all logs.
  - Run your secure-deletion software to overwrite all of the newly deleted stuff.
  - Have your organization put this weekly ritual or something like it in its written policy.

10. Responsibilities

Functional or Business Line Heads

- Responsible for the data it creates, uses, stores, processes and destroys.
- Responsible to nominate an Owner for each Data Asset and Personal Data Processing Activity.
- Responsible to ensure that each Data Asset and Personal Data Processing Activity is registered on the Data Asset and Personal Data Processing inventories by the nominated Owner.
- Responsible for implementing procedures for the retention, archiving and destruction of data, communicating these periods to the relevant employees and enforcing compliance.
- Responsible for submitting exception requests to the process, including consulting and receiving legal advice if necessary to justify making an exception.
- Responsible in each location to ensure that Data Asset and Data Processing inventories are compiled, regularly reviewed, updated and maintained, at least annually.
- Responsible for the destruction of Data in accordance with the retention periods defined in departmental Data Processing inventories.

Compliance Department

- Responsible for audit the compliance to this Policy from time to time and provide recommendations to be reviewed by the Chairman of the KID's Management Committee.
- Responsible to provide guidance with regard to this Policy.
- Responsible to administrate and oversee the use of Data Asset and Personal Data Processing Inventory systems.

Employees

- Each employee shall be responsible for returning Records and Documents in their possession or control to KID upon separation or retirement.
- Final disposition of such Records and Documents shall be determined by the immediate supervisor in accordance with this policy and the respective country employee exit process.