designhygiene	Quality Management System **Records Management Policy**

Document Type	Human Resources Policy
Area of Application	All Employees of Design Hygiene (Pty) Ltd.
Purpose	This policy sets out how we identify, secure, store, preserve or dispose of records which are essential for historical, commercial and legal purposes and effective business continuity. It ensures that our record-keeping: • is transparent, consistent, and accountable; • meets legal, regulatory, fiscal, operational, and historical requirements; • supports the efficient conduct of our business; and • ensures the preservation of archives documenting our history and development for historical, commercial and legal purposes.

DOCUMENT METADATA

Document number:	0003
Document version:	0001
Document approval authority:	INFORMATION OFFICER
Document approval date:	30 JUNE 2021
Document owner:	INFORMATION OFFICER
Document author(s):	INFORMATION OFFICER
Last updated:	30 JUNE 2021
Next review date:	30 JUNE 2022
Visibility (where will it be displayed):	RECEPTION

Table of Contents

1. WHY WE HAVE THIS POLICY

Records management is an important aspect to proper information governance. It helps us to understand our data and retention periods and effectively govern these in order to mitigate compliance risks and ensure the effective and efficient operations of our business.

Records management is the practice of creating, identifying, categorising, archiving, maintaining, and properly disposing of business information. A 'record' is information about facts, events, transactions, or opinions that our organisation creates, receives or maintains during the course of its business.

At Design Hygiene, we are committed to identifying, securing and preserving our records which are essential for historical, commercial and legal purposes. This policy sets out how we achieve that

This policy ensures that our record-keeping:

- is transparent, consistent, and accountable;
- meets legal, regulatory, fiscal, operational, and historical requirements;
- supports the efficient conduct of our business; and
- ensures the preservation of archives documenting our history and development for historical, commercial and legal purposes.

2. THE SCOPE OF THIS POLICY

This policy applies to:

- all our information, in all formats, whether electronic or otherwise, in any location;
- all information systems and applications; and
- employees, contractors, and other individuals who have access to our information.

3. WHY IT IS IMPORTANT TO COMPLY WITH THIS POLICY

The organisation only works when we all do our part, and all of us want to see the organisation succeed. If you do not comply with this policy, or if you discover that we are not complying with the policy and you do not tell us about it, you could face disciplinary action.

If the company does not comply:

- We could fail to create appropriate records or to be able to retrieve records when we need them;
- We could fail to meet the requirements imposed by the Protection of Personal Information Act 4 of 2013 on information quality, records retention, information security and transparency;

- We could fail to effectively manage requests for information from the public under the POPIA and the Promotion of Access to Information Act 2 of 2000;
- Our business could be disrupted, or operate inefficiently, including ineffective use of staff time to create or retrieve records, unnecessary records storage and retrieval costs;
- We could face action against the organisation for failing to meet audit, regulatory or statutory requirements;
- We could be unable to defend the organisation during investigations, disputes and litigation;
- We could lose records and valuable intellectual property through security breaches (e.g. the unauthorised destruction of records) and when employees leave the organisation or change positions within the organisation; and
- We could suffer reputational damage.

If you don't comply:

- You could face disciplinary action in terms of our Disciplinary Code and Procedure if you do not comply with this policy, or if you discover that we are not complying with the policy and you fail report it to us immediately;
- possible job losses due to loss of business and negative financial impact;

4. DEFINITIONS

Confidential information means information that is available only to specified and relevant employees within the organisation.

Confidential information should be subject to strict access controls. Unauthorised disclosure, modification or destruction of confidential information could cause us, another organisation, or individual, significant harm, or provide an unfair advantage.

Examples include:

- contracts and agreements;
- tender documents;
- security-related information, i.e. server configurations and password documents;
- infrastructure or network information (including hardware and software);
- research data and associated information;
- information relating to supply or procurement of goods or services before approval;

	• legal advice or other information on legal action against or by us; • trade secrets, intellectual property intended for commercialization; • business plans and projects while in development; • internal memoranda and emails; • minutes and agendas; • technical documents such as system configurations and floor plans; • research reports and publications; • internal audit reports; and • risk registers and reports.
Incident	An incident includes: • non-compliance with this policy and any related procedures; • contraventions of any data protection legislation such as the POPIA; and • security incidents such as breaches of confidentiality, failures of integrity or interruptions to the availability of personal information.
Information processing activities	means a collection of interrelated tasks that achieve a specific result during which information is created, collected, used, transformed, stored, or destroyed. A processing activity is important if we could experience critical or high levels of risk if the process or activity is disrupted or could no longer continue.
Record	means Information created, received and maintained by the organisation as evidence of actions or decisions, to meet legal, regulatory, fiscal, operational and historical requirements.
Our Information	means all data, records, and knowledge in electronic or any other format that forms a part of the intellectual capital we use, transform, or produce. It includes public, private, confidential, and personal information.
Personal Information	means any information relating to an identifiable individual (living or deceased) or an existing organisation (e.g. a organisation or public

body). This includes the personal information of all customers, staff members, job applicants, shareholders, board members service providers, contractors, suppliers, members of the public, and visitors.

Examples include (but are not limited to):

- Information relating to the race, gender, sex, identifiers such as name, identity number, employee number, account number, customer number, company registration number, tax number, photographs, videos, or any other unique information that may be used to identify a person;
- biometric information – this relates to the techniques of identification that are based on physical, physiological, or behavioural characteristics, such as fingerprints, blood-type, DNA analysis, retinal scans, facial and voice recognition;
- demographic information such as race, gender, pregnancy, marital status, age, culture, language and birth;
- Information relating to physical or mental health, well-being or disability;
- background information such as education, financial, employment, medical, criminal or credit history;
- contact details – physical / postal address, telephone number(s), email address(es), online identifier (i.e. twitter handle), or location information;
- an individual's preferences, opinions and views;
- confidential or private correspondence and any correspondence that would reveal the contents of the original correspondence;
- views and opinions about an individual like trade references, job references, performance reviews and interview notes;

Special / Sensitive Personal Information

means information about an individual that pertains to racial or ethnic origins, political, religious, or philosophical beliefs, health or sexual life, trade union membership or political persuasion, biometric information, or criminal behaviour (to the extent that such criminal behaviour relates to the alleged commission by a data subject of an offence or any proceedings in respect of any offense allegedly committed by a data subject).

Sensitive Personal Information may only be processed under strict conditions and will usually require the **express written consent** of the data subject.

POPIA:	means The Protection of Personal Information Act 4 of 2013 and its regulations.
Private Information	means our information that is only available to authorised employees. The release of this information to the general public could cause us, another organisation, of an individual minor harm.
Public Information	means our information that is publicly available without restriction, and that is unlikely to cause us, another organisation, or an individual harm.
The Company / organisation / business we / us	Design Hygiene (Pty) Ltd.
Third Parties	External organisations or individuals

5. OUR POLICY

5.1. It is our policy to:

- follow proper records management principles; and
- Conduct records management assessments.

5.2. Principles of good records management

- To ensure that we maintain adequate records, we follow these records management principles:
  - We create, approve and maintain a records retention schedule.
  - We apply the principles of information security management.
  - We apply effective version control.
  - We minimise duplication.
  - We adequately preserve records when employees, contractors and other individuals who have access to our information leave.
  - We securely archive or destroy records.
  - We develop and document records management procedures.
  - We continuously monitor compliance with this policy and the records retention schedule.
  - We manage incidents.
  - We train employees on their responsibilities under this policy.

5.3. We create, approve and maintain a records retention schedule.

The organisation must ensure its record-keeping complies with all legal, regulatory or business requirements.

To achieve this, the Information Officer must create, approve and maintain a records retention schedule that contains:

- a list of categories of records that must be maintained for legal, regulatory or business requirements;
- a default retention rule for each category of records;
- any exemptions from the default rule for specific records within a category;
- the legal, regulatory or business requirement that necessitates the retention of a particular category of records or a specific record (the reason for retention);
- the period for which the category of records or specific record must be retained;
- the event that triggers the start of the period;
- dates on which the schedule was agreed.

The Information Officer will create, approve and maintain the records retention schedule, but Senior Management must ensure that they identify and meet all legal, regulatory or business requirements for the retention of records in their relevant business areas.

Senior Management must review and update the records retention schedule for their relevant business areas annually.

5.3..1. We ensure that the principles of information security management are applied

Senior Management must ensure that the principles of the organisation's Information Security Policy are applied to all records and related infrastructure within their business areas to protect the records from unauthorised destruction, modification or access.

5.3..2. We apply effective version control practices

Effective version control practices support data quality, reduce the uncontrolled distribution of information and allow for more economical storage by deleting earlier versions of documents (if the records retention schedule permits it).

Senior Management must ensure that:

- version control practices are applied to all records to ensure that the correct version of the record is retained; and that
- a reliable record of all activities of users is maintained and monitored to detect unauthorised or irregular handling of records.

5.3..3. We minimise duplication

We minimise the duplication of records (except when records are duplicated to create a back-up record) to:

- ensure the accuracy of records by recognising one version of the record as authoritative;
- advance compliance with data protection legislation;
- eliminate wasted cost from storing unnecessary duplicates of records;
- improve the security of records by centrally controlling access.

The Information Officer must ensure that the organisation minimises the duplication of records by identifying and controlling master records.

If there are persuasive operational reasons to duplicate master records or master data sets, the Information Officer must authorise the duplication, and the copies should only be retained for a limited time and for the stated purpose for which the duplication was made.

5.3..4. We ensure that records are adequately preserved

Senior Management must put processes in place to ensure that records are adequately preserved when employees, contractors, and others who have access to the organisation's information leave.

5.3..5. We ensure that records are securely archived or destroyed

When a record no longer needs to be retained, Senior Management must confirm whether the record must be:

- securely destroyed; or
- in exceptional circumstances relating to that specific record, retained for another (specified) period.

Senior Management must ensure that a record is kept of which documents were destroyed, the date on which they were destroyed and how they were destroyed.

When a specific record must be retained for another (specified) period, this is referred to as a disposal hold. A disposal hold takes precedence over the retention periods in the records retention schedule. The reason for the disposal hold must be documented.

5.3..6. We develop and document records management procedures

Senior Management must develop and document procedures to implement this policy and the records retention schedule within their business areas.

5.3..7. We continuously monitor compliance with this policy and the records retention schedule

Senior Management must continuously monitor whether this policy and the records retention schedule have been effectively implemented.

5.3..8. We manage incidents

All employees must report incidents in accordance with our Information Security Management Policy and Incident Management Procedure.

An incident includes:

- non-compliance with this policy and any procedures that relate to it;
- contraventions of any data protection legislation such as the POPIA; and
- security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information.

Employees must immediately report:

- any known or suspected incidents; or
- any circumstances that increase the risk of an incident occurring;
- Reports must be sent to Wanda@designhygiene.co.za.

5.3..9. We train employees on their responsibilities under this policy

Anyone who has access to our information (including employees, contractors and others) must keep adequate records. They must follow our policies and comply with all data protection legislation.

We ensure that all users are trained on the record-keeping requirements that apply to the information to which they have access.

5.4. We conduct records management assessments

Senior Management must ensure that all information, services and related supporting infrastructure that they are responsible for are assessed regularly to identify records management risks.

A records management assessment must be conducted before we:

- continue with an information processing or management activity;
- change an existing information processing or management activity;
- process information for a new purpose;
- launch new products or services;
- use new systems/software for processing information; or
- share confidential or personal information with third parties.

All activities that are rated as critical or high risk during the records management assessment must undergo an assessment every three years.

6. ROLES AND RESPONSIBILITIES

These are the responsibilities in respect of this policy

The Information Officer (The MD)	The Managing Director (MD) is our Information Officer. The Information Officer has a coordinating function that focuses on the policy-based protection of our information and is the policy owner of this policy. The Information Officer must ensure that this policy receives support from senior management throughout the organisation and that senior management discharges their responsibilities.
Deputy Information Officer(s)	Deputy Information Officer(s) must support the Information Officer and are responsible for strategic guidance to the organisation on data privacy risk management. The Deputy Information Officer(s) must: • oversee the implementation of this policy; • develop procedures and standards to support records management; • create, approve and maintain a records retention schedule, • identify master records to minimize duplication, • provide advice on the identification and management of records management risk, • monitor whether records management risk assessments are performed when required, • develop training on records management, • monitor whether this policy is implemented throughout the organisation.
Manager of IT	The Manager of IT supports the Information Officer and the Deputy Information Officer(s) by: • developing Information Technology policies, procedures, standards and guidelines; • providing technical advice on records management; • supporting the implementation of this policy through appropriate technology investments; • ensuring that the organisation only invests in information technology that complies with this policy.
Head of Legal	The Head of Legal: • oversees the management of data records management legal obligations; • ensures that the appropriate contracts with third parties concluded; • ensures that employees are aware of contractual obligations and their responsibilities;

	• provides legal advice on the interpretation of legislation; and • manages legal risks and provides legal advice when an incident occurs.
Head of HR	The Head of HR: • assists the Information Officer and Deputy Information Officer(s) with the ongoing implementation and adherence to the POPIA framework within the context of HR records management; • communicates the key aspects of records management as it relates to the Protection of Personal Information Act that impact HR to the HR team; • ensures a records retention schedule for all the records in the HR division is created and maintained; • ensures a records management process for all the records in the HR division is implemented and monitored; • records management assessments are conducted before confidential and personal information is processed; • ensures records management-related risks in Human Resources are managed; • their business area participates in investigations into records management incidents. • articulates records management HR activities that require attention as a result of the Protection of Personal Information Act; • clarifies and monitors the responsibilities of HR personnel involved in records management; • assists the Deputy Information Officer in the development and implementation of a compliance framework for records management within the HR function; • develops a records management plan for HR information; • monitors the compliance framework for records management in HR.
Senior Management	Senior Management must implement this policy, create or align other policies and processes in their business areas with this policy, and monitor and advocate for compliance within their business areas. Senior Management must ensure that: • business areas comply with this policy; • a records retention schedule for all the records in their

	business area is created and maintained; • a records management process for all the records in their business area is implemented and monitored; • records management assessments are conducted before confidential and personal information is processed; • records management-related risks in their business area are managed; and • their business area participates in investigations into records management incidents.
Users of information	All users who have access to the organisations' information or information systems must: • adhere to all policies, procedures and guidelines that relate to the use of information; and • report any actual or suspected incidents immediately.
Internal and external audit	Internal and external audit provides independent assurance that the organisation's risk management, governance and internal control processes are operating effectively, including compliance with this policy.

7. SUPPORTING DOCUMENTS

Supporting documents to this policy:

- Records Retention Schedule.
- Records Management Assessment Procedure and assessment.
- Records Management Procedures in specific areas of the organisation.

8. REVIEW

This document shall be reviewed annually by the Information Officer, who is the owner of this document, and updated with any new legislation to ensure that it remains fit for purpose.