designhygiene	Quality Management System **Information Security Management (ISM) Policy**

Document Type	IT Policy
Area of Application	All employees, contractors, and other individuals who have any level of access to the information of Design Hygiene (Pty) Ltd.
Purpose	To communicate to everyone in the company their obligation in protecting our information by ensuring our protections are adequate, implemented and adhered to, to secure our information against: • breaches of confidentiality • failures of integrity; and • interruptions to the availability of information.

DOCUMENT METADATA

Document number:	0002
Document version:	0001
Document approval authority:	INFORMATION OFFICER
Document approval date:	30 JUNE 2021
Document owner:	IT MANAGER
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

For our organisation to grow and prosper, we need to ensure everyone in the business is aware of their responsibility for protecting our information.

This policy is intended to communicate to everyone in the company their obligation in protecting our information by ensuring our protections are adequate, implemented and adhered to, to secure our information against:

- breaches of confidentiality
- failures of integrity; and
- interruptions to the availability of information.

2. THE SCOPE OF THIS POLICY

This policy applies to:

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

3. WHY IT IS IMPORTANT TO COMPLY WITH THIS POLICY

Our reputation is our biggest asset. Without our reputation, our relationships with key stakeholders and investors would suffer, and we could lose clients, prospective clients, and top-class candidates. We could also face substantial fines. The ongoing protection of information within the organisation is therefore the responsibility of everyone, given that any negative implications would directly affect all stakeholders.

If the company does not comply:

- Far reaching consequences for our business which will negatively impact our data integrity, and our reputation.
- Financial impact - substantial fines negatively impacting the finances of the organisation which could lead to possible retrenchments.
- More severe penalties i.e. imprisonment, permanent reputational damage and permanent loss of business.

If you do not 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 commercialisation;
- 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.
Information Asset	means a body of information that is organised and managed as a unit. Examples include: • a database: in any format whatsoever, whether it is in an Excel spreadsheet or in an information management system; • a folder in which we keep all information relating to a particular topic in a centrally accessible location (e.g. SharePoint or Google Drive); and • physical records stored in a cupboard, filing cabinet or filing room.
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

While all our information should be secured, we take a risk-based approach to information security management. We prioritise the security of information we use in those activities that, if interrupted or cancelled, could lead to high or critical levels of risk. We call these activities important processing and management activities.

It is our policy to:

- follow information security principles; and
- conduct information security assessments.

4.1. Principles of good information security

To protect the confidentiality, integrity, and availability of all our information, we follow these information security principles:

- We manage information security risk.
- We have responsible and empowered users.
- We manage information assets.
- We manage third parties.

- We enhance information quality.
- We ensure the availability of information.
- We comply with binding rules.
- We manage incidents.

4.1.1. We manage information security risk

Our risk-based approach means we do not treat every risk in the same way. We measure how likely a security risk is, and what the impact of each risk could be. This approach helps us decide what the appropriate level of security safeguard or control is that we must apply to our information.

We:

- identify and review all the internal and external information security risks that we can reasonably foresee;
- ensure that we have adequate security safeguards in place at each stage of the lifecycle of our systems and processes;
- maintain appropriate safeguards against the risks we identify;
- regularly verify that we implement the safeguards effectively; and
- ensure that we continually update the safeguards in response to new risks or deficiencies in the safeguards.

4.1.2. We have responsible and empowered users

Anyone who has access to our information (including employees, contractors, and other individuals) must keep information secure. They must follow our policies and comply with data protection legislation.

We ensure that all users are:

- trained to work responsibly with and protect our information; and
- empowered to protect their own privacy.

All users must immediately report:

- any breach of our this policy;
- any known or suspected incidents; or
- security weaknesses. Reports must be sent to Wanda@designhygiene.co.za.

4.1.3. **We identify, classify and manage information assets**

We:

- identify and classify our information assets as either public, private, confidential or personal information;
- assign information asset owners who will be accountable to define the appropriate uses of the information; and
- protect our information from unauthorised destruction, modification, or access, by controlling access to information systems, buildings that house information, and related supporting infrastructure.

To achieve this, we:

- only provide access to information to those who require access by virtue of their role in the organisation;
- restrict the level of access to ensure that users only have the privileges that their position requires;
- have information access control standards in place to authorise, revoke and review access rights to our information;
- use appropriate ways to verify users that require higher levels of authentication to protect personal and confidential information;
- ensure that we maintain and monitor a reliable record of all activities of users to detect unauthorised or irregular activities; and
- develop standards for the use of mobile computing devices (regardless of who owns them) that store, process, or transmit information.

4.1.4. **We manage third parties**

We:

- identify all instances when we share confidential or personal information with third parties;
- ensure that sharing personal information complies with all data protection legislation (e.g. the POPIA);
- enter into appropriate contracts and take additional steps that may be necessary to reduce the risks that are created by sharing information;
- conduct an assessment to determine who must ensure that we conclude contracts, who must review the contracts, and whether we must take additional steps to reduce the risks created by sharing information; and
- keep a record of sharing activities, including the outcome of assessments, a record of additional steps, what information was shared, when it was shared, and how.

4.1.5. **We enhance information quality**

We enhance the quality of information by implementing processes to ensure that the information is complete, unique, timely, valid, accurate, and consistent.

To achieve this, we:

- define and monitor appropriate quality standards and guidelines for our information;
- create a uniform set of definitions for commonly used information;
- ensure that we record, manage, and use the appropriate metadata to meet our needs and priorities;
- ensure that we remain aware of relevant information flows between systems and external sources and set conditions for the integration of information from different sources;
- avoid unnecessary duplication of information by facilitating sharing and integration within our organisation;
- monitor the integrity of information;
- authorise new information collection and disposal processes; and
- implement business processes and technology to ensure appropriate information quality.

4.1.6. **We ensure the availability of information**

We consider the protection of information assets and the resilience of information technology infrastructure in all business continuity plans.

4.1.7. **We comply with binding rules**

We comply with all legislation, internal policies, contracts and other binding rules that govern information security. Specifically, we comply with all privacy regulations such as the POPIA by enforcing this policy as well as the Data Privacy Policy.

4.1.8. **We manage incidents**

We:

- foster a culture of transparency, where employees feel comfortable reporting incidents;
- implement mechanisms to detect and report incidents;
- respond rapidly and consistently to incidents that threaten our information assets, information systems, and the networks that deliver the information;

- create and implement a clear Incident Management Procedure;
- assign an incident owner;
- engage with and notify external and internal stakeholders of an incident that affects them;
- identify, collect, and preserve information that can serve as evidence;
- analyse and document incidents;
- adjust procedures to mitigate the risk of future incidents and to improve the responses to future incidents; and
- ensure appropriate follow-up reports. 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.

4.2. We conduct information security assessments

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

An information security assessment must be conducted before we:

- continue with an information processing activity;
- change an existing information processing 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 information security 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 information security risk management. The Deputy Information Officer(s) must: • oversee the implementation of this policy; • develop procedures and standards to support information security management; • provide advice on the identification and management of information security risk; • monitor whether information security risk assessments are performed when required; • develop training on information security 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 information security 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 information security related legal obligations; • ensures that the appropriate contracts with third parties are 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 information security management; • demonstrates an understanding of the impact of the Protection of Personal Information Act on the processing of HR information; • communicates the key aspects of the Protection of Personal Information Act that impact HR to the HR team; • articulates the 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 the processing of personal information; • develops and implements a compliance framework for the protection of personal information within the HR function; • develops an information security management plan for HR information, together with the IT Director; • monitors the compliance framework for information security 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 register of information assets used in important information processing activities in their business area is created and maintained; • information used in important information processing activities is classified; • information security assessments are conducted before confidential and personal information is processed;

	• information security-related risks in their business area are managed; and • their business area participates in investigations into 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 upon discovery thereof..
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

The list below is (loosely) based on thestandards that are required for ISO 27001 and NIST compliance:

- Information security assessment procedure and assessment
- Information Asset Register
- Information Security Classification Schedule
- End-User Manual
- Asset Management Standard
- Access Control Standard
- Cryptography Standard
- Physical and Environmental Security Standard
- Operations Security Standard
- Communications Security Standard
- Systems Acquisition, Development and Maintenance Standard
- Third Party Risk Management Procedure and Assessment
- Contract Management Policy and Procedure
- Data Protection Clause Negotiation Playbook
- Data Quality Procedures and Standards
- Incident management procedure

8. REVIEW

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