Channelport Pty Ltd

PROTECTION OF PERSONAL INFORMATION COMPLIANCE POLICIES

Table of Contents

Privacy Policy

Policy	**Privacy Policy - General Processing of Personal Information**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # A

1. Purpose

The purpose of this policy is to establish a compliance framework for Channelport Pty Ltd to ensure compliance with the Protection of Personal Information Act.

2. Definitions

2.1 "**availability**" means data being accessible and usable upon demand by an authorised entity.

2.2 **"confidentiality"** means information is not made available or disclosed to unauthorised individuals, entities, or processes.

2.3 **"data"** means the representation of facts as text, numbers, graphics, images, sound, or video and includes all electronic and non-electronic data, either in structured or unstructured form which exists within Channelport Pty Ltd irrespective of the means of storage or retrieval.

2.4 **"data subject"** means the person to whom personal information relates.

2.5 **"direct marketing"** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of –

a. promoting or offering to supply, in the ordinary course of business, any goods or service to the data subject; or
b. requesting the data subject to make a donation of any kind for any reason.

2.6 **"electronic communication"** means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

2.7 **"filing system"** means any structured set of personal information, whether centralised, decentralised dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.8 **"information"** means data in the context of one or more of:

a. the business meaning of data and related elements;
b. the format in which data is presented;
c. the timeframe represented by the data; and / or
d. the relevance of the data to a given usage.

2.9 **"Information Officer"** of, or in relation to, –

a. a public body means an information officer or deputy information officer as contemplated in terms of Section 1 or 17 of PAIA; or
b. a private body means the head of a private body as contemplated in Section 1 of PAIA; and
c. Channelport Pty Ltd means the person duly nominated and authorised by Channelport Pty Ltd management, from time to time, to act as the Information Officer and who is duly registered with the Information Regulator.

2.10 **"integrity"** means protecting the accuracy and completeness of assets.

2.11 **"interruptions"** means an event that causes a disruption, temporary halt or break in an activity of process, to any IT system, infrastructure or application that includes servers, network infrastructure, application such as emails etc., desktops, laptops, or tablets due to physical or system errors, loss of equipment or connectivity, and human error.

2.12 **"operator"** means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

2.13 **"person"** means a natural person or a juristic person.

2.14 **"personal information"** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

a. information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language, and birth of the person;
b. information relating to the education or the medical, financial, criminal or employment history of the person;
c. any identifying number, symbol, e-mail address, telephone number, location information, online identifier, or other particular assignment to the person;
d. the biometric information of the person;
e. the personal opinions, views, or preferences of the person;

f. correspondence sent by the person that would reveal the contents of the original correspondence;
g. the views or opinions of another individual about the person; and
h. the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.15 **"private body"** means –

a. a natural person who carries or has carried on any trade, business, or profession, but only in such capacity;
b. a partnership which carries or has carried on any trade, business, or profession; or
c. any former or existing juristic person but excludes a Public Body.

2.16 **"processing"** means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

a. the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
b. dissemination by means of transmission, distribution or making available in any other form; or
c. merging, linking, as well as restriction, degradation, erasure, or destruction of information.

2.17 **"Promotion of Access to Information Act"** and/or **"PAIA"** means the Promotion of Access to Information Act 02 of 2000.

2.18 **"Protection of Personal Information Act"** and/or **"POPIA"** means the Protection of Personal Information Act 04 of 2013.

2.19 **"public body"** means –

a. any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or
b. any other functionary or institution when –
    i. exercising a power or performing a duty in terms of the Constitution or a Provincial Constitution; or
    ii. exercising a public power or performing a public function in terms of any legislation.

2.20 **"public record"** means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body.

2.21 **"record"** means any recorded information regardless of form or medium, including any of the following:

a. writing on any material;
b. 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 divided from information so produced, recorded or stored;

c. label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
d. book, map, plan, graph, or drawing;
e. photograph, film, negative, tape or other device in which one or more visual images are embodied to be capable, with or without the aid of some other equipment, of being reproduced;
f. in the possession or under the control of a responsible party; and
g. regardless of when it came into existence.

2.22 **"responsible party"** means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

2.23 **"the business", "we", "us"** and/or **"Channelport Pty Ltd"** means Channelport Pty Ltd, a private body operating as a company duly registered in terms of the Companies Act 71 of 2008.

2.24 **"special personal information"** means personal information as referred to in Section 26 of POPIA.

3. Policy Statement

3.1 Channelport Pty Ltd recognises its accountability in terms of the POPIA and its regulations, to all its stakeholders. Channelport Pty Ltd needs to collect personal information from its employees, clients, suppliers, operators as well as other stakeholders to carry out its business.

To maintain a trust relationship with our stakeholders, we are committed to complying with both the spirit and the letter of POPIA and to act with due skill, care, and diligence when dealing with personal information. This is to mitigate the risk, which may include loss of reputation, fines, imprisonment, and to prevent a significant loss of clients.

The responsibility to facilitate compliance throughout Channelport Pty Ltd has been delegated to the appointed Information Officer who have the responsibility of supervising, managing, and overseeing the compliance with POPIA. However, it must be emphasised that the primary responsibility for complying with POPIA lies with all members of staff dealing with personal information. All staff must therefore understand their responsibility in terms of POPIA as well as with this Privacy Policy, the supplementary policies and/or any guidance notes and ensure that they are applied when processing personal information.

This Privacy Policy sets out the approach to managing the compliance risks faced by the organisation.

Any breach of this Privacy Policy is considered serious and will result in disciplinary action that could ultimately lead to the dismissal of the offender.

3.2 Breach of this policy and reporting lines

3.2.1 Any Employee who is part of, or becomes aware of, a data breach must report to the Information Officer.

3.2.2 The Information Officer reports to the Managing Director and the board of directors of Channelport Pty Ltd, who in return reports to the Information Regulator.

3.3 Roles and responsibilities

3.3.1 The Information Officer must ensure this policy is followed by each employee through the support of all management levels who must discharge their responsibilities.

3.3.2 The Information Officer, in their duty to ensure data privacy risk management, must:

- ensure the implementation of this policy in all business areas;
- Ensure that standard operating procedures are developed for all departments of the business;
- monitor whether this policy is implemented in all departments of the business.
- respond to data subject requests and objections subject to paragraph 3.2 above.
- respond to requests from the Information Regulator and work with the Information Regulator subject to paragraph 3.2 above.

3.3.3 The Information supported by the IT Service Provider (if applicable), must:

- Developing IT policies, procedures, standards, and guidelines;
- Provide technical support;
- Support the implementation of this policy through appropriate technology investments which comply with this policy;

4. Compliance principles

A. The Information Officer must ensure that the business adheres to the following conditions for the lawful processing of personal information in terms of POPIA

4.1 **Condition 1: Accountability**

The business must ensure that the conditions of lawful processing of personal information and all measures that give effect to such conditions are complied with at all times.

4.2 **Condition 2: Processing limitation**

4.2.1 Personal information must be processed in a lawful and reasonable manner that does not infringe the privacy of the data subject.

4.2.2 Personal information may only be processed providing the purpose for which it is processed, it is adequate, relevant, and not excessive;

4.2.3 You may only process and access information as is allowed for in order to perform your duties in terms of your employment function.

4.2.4 Information may not be accessed, stored, or distributed other than is required by your employment function.

4.2.5 You may only process personal in following legal or contractual obligations, to achieve business goals, alternatively with the consent of the data subject after the purpose has been explained to the data subject, who confirmed that the purpose is understood. You may also process information when the processing is in the legitimate interest of the data subject, the business or a third party.

4.2.6 Information must be collected directly from the data subject where possible. If personal information is collected from another source, the data subject must be advised thereof, and the purpose for the collection.

4.3 **Condition 3: Purpose specification**

4.3.1 The business may only collect personal information for a specific, explicitly defined, and lawful purpose that relates to the function or activity of the business.

4.3.2 It is the employees' instruction to ensure the data subject is made aware of the purpose for which their personal information is processed.

4.3.3 Each employee may only destroy and/or de-identify personal information as is allowed for by this policy, as well as the Data Destruction Policy and the Data Retention Policy.

4.4 **Condition 4: Further processing limits**

4.4.1 If information is processed for any other purpose other than the reason why the information was originally collected, then permission for such further processing must be granted by the Information Officer in writing if the further processing is allowed in terms of POPIA.

4.4.2 To assess whether further processing is compatible with the purpose of collection, the business must take account of –

a. The relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

b. The nature of the information concerned;

c. The consequences for the data subject's intended further processing of his, her or its personal information;

d. The manner in which the personal information has been collected from the data subject; and

e. Any contractual rights and obligations bestowed on the parties.

4.5 **Condition 5: Information quality**

4.5.1 Information must be kept complete, accurate, must not be misleading, and must be updated where necessary.

4.5.2 If you become aware that a data subject's details have changed, notice must be sent to **lanib@channelport.co.za** and the relevant department must be informed of the changes. Changes may only be effected upon proper verification.

4.6 **Condition 6: Openness**

When Channelport Pty Ltd collects personal information, reasonable, practicable steps must be taken to ensure that the data subject is aware that the personal information is being collected in line with this and other related policies.

4.7 **Condition 7: Security safeguards**

4.7.1 Each employee of Channelport Pty Ltd must secure the integrity and confidentiality of all personal information this is in its or under its control to prevent –

a. The loss of, damage to, or unauthorised destruction of personal information; and

b. The unlawful access to or processing of personal information.

4.7.2 When sharing personal information with an operator, the employee must ensure that a Data Processing Agreement is entered into with the operator that must make provision for the following:

a. the operator must have sufficient security measures in place;

b. the operator must notify Channelport Pty Ltd immediately of any suspected security compromise;

c. internal responsibility for information security management;

d. devoting adequate personnel resources to information security;

e. carrying out verification checks on permanent staff who will have access to the personal information;

f. requiring employees, vendors, and others with access to personal information to enter into written confidentiality agreements, and

g. conduct training to make employees and others with access to personal information aware of information security risks presented by the processing.

4.8 **Condition 8: Data subject participation**

4.8.1 When a data subject provides sufficient proof of identity (for example copy of an identity document or driver's license) the data subject is entitled to:

a. confirmation whether the company holds information of the data subject;

b. access to that information;

c. be advised of his/her/it's right to request the correction or deletion of personal information;

d. confirmation of what action was taken in response to their request.

4.9 To comply with these principles, you must consider the following policies, procedure, and management tools:

- Internal Privacy Notice;
- Privacy Notice;
- Data Mapping;
- PAIA Manual;
- Impact Assessment;
- Standard Operating Procedures;
- Assessment;
- Data Processing Agreements;
- Information Security Policy and supplementary policies;
- Incident Response Policy;
- Clean Desk Policy;
- Data Retention Policy;
- Data Destruction Policy.

B. The business must adhere to the following provisions of POPIA when processing special personal information

4.10 Prohibition on the processing of personal information:

4.10.1 The business will not process personal information, concerning –

a. The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

b. The criminal behaviour of a data subject to the extent that such information relates to –

i. the alleged commission by a data subject of any offence; or

ii. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings; unless such processing is justified as follows:

- the Data Subject has consented to process it (in circumstances where we are legally obliged to obtain the data subject's consent); or
- it is necessary to exercise or defend a right or obligation in law; or
- it is necessary to comply with an international legal obligation of public interest; or
- it is for historical, research, or statistical purposes that would not adversely affect your privacy; or
- the data subject deliberately made their personal information public.

C. The business must adhere to the following provisions of POPIA when processing personal information of children

4.11 Prohibition on processing personal information of children

4.11.1 Definitions:

a. **"child"** means a natural person under the age of 18 years who is not legally competent to take any action or make any decision in respect of any matter concerning him- of herself, without the assistance of a competent person.

b. "**competent person**" means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

4.11.2 It is important to note that the business may not process personal information concerning a child, unless such processing is:

a. carried out with the prior consent of a competent person;

b. necessary for the establishment, exercise, or defence of a right or obligation in law;

c. necessary to comply with an obligation of international public law;

d. for historical, statistical, or research purposes to the extent that –

i. the purpose serves a public interest, and the processing is necessary for the purpose concerned; or

ii. it appears to be impossible or would involve a disproportionate effort to ask for consent; and

iii. sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or

e. of personal information which has deliberately been made public by the child with the consent of a competent person.

D. The business must adhere to the following provisions of the POPIA when marketing directly to a data subject through unsolicited electronic communication

4.12.1 The processing of personal information of a data subject for the purpose of direct marketing through any form of electronic communication, including automatic calling machines, facsimile machines, SMSs, or email is prohibited unless the data subject –

a. has given his, her or its consent to the processing; or

b. is a customer of the business.

4.12.2 In the above context “automatic calling machine” means a machine that is able to do automated calls without human intervention.

4.12.3 The business may approach a data subject only once to request the consent of that data subject and only if the data subject has not previously withheld such consent.

4.12.4 The data subject’s consent must be requested in the prescribed manner and form 4 to the Regulations.

4.12.5 The business may only process the personal information of a data subject who is a customer of the business if –

a. the business has obtained the contact details of the data subject in the context of the sale of a product or service;

b. the purpose of direct marketing is through the business’s own similar products or services; and

c. the data subject has been given a reasonable opportunity to object, free of charge, and in a manner free of unnecessary formality, to such use of his, her, or its electronic details –

i. at the time when the information was collected; and

ii. on the occasion of each communication with the data subject for the purpose of direct marketing if the data subject has not initially refused such use.

4.12.5 Any communication for the purpose of direct marketing must contain –

a. details of the identity of the sender or the person on whose behalf the communication has been sent; and

b. an address or other contact details to which the recipient may send a request that such communications cease.

E. The business must adhere to the following provisions of POPIA when transferring personal information outside of the Republic of South Africa

4.13 The business may not transfer personal information about a data subject to a third party who is in a foreign country unless the personal information that is collected automatically is collected by third parties whose technology we use to provide website functionality and acquire website analytics information. Some of these third parties will be outside of the borders of South Africa and data subject's information will be stored outside the borders of South Africa. We make use of productivity software solutions such as Microsoft 365 or Google Business and the information collected through this third party will be kept on the servers used by of the software solution provider.

5. Training

Staff will receive training as part of the induction process. Further training will be provided at least every year or whenever there is a substantial change in the policies and procedures, or IT Infrastructure.

Training may be provided through information sessions, regular emails to all staff as well as pre-recorded online webinars, and will cover the latest subjects related to the use of Channelport Pty Ltd IT systems and applications, the applicable laws relating to data protection, and Channelport Pty Ltd's data protection, and related policies and procedures. Completion of training is compulsory.

If you have any questions or concerns about anything in this policy, do not hesitate to send your query to **lanib@channelport.co.za**.

6. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

7. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

8. Change history

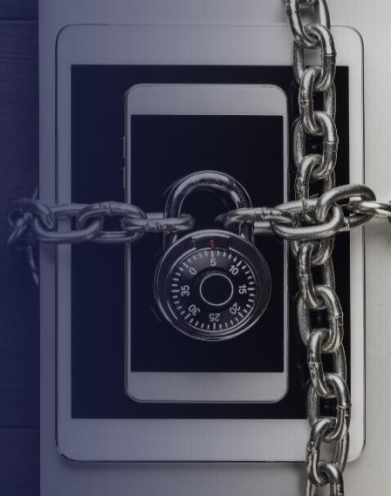
Date	Author	Version	Change reference

9. Policy approval

Signed: _____

Date: _____

Information Security Policy



Policy	**Information Security Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # B

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing all aspects related to the Information Systems' use and procedures within the business. This Policy and Procedures is an overview that consist of various supplementary policies referenced within this policy.

Channelport Pty Ltd is required to take appropriate, reasonable technical and organisational measures to protect the information systems, infrastructure, and applications that we possess or control, to prevent unauthorised access, collection, use, disclosure, or similar risks.

For Channelport Pty Ltd to prosper and comply with the above stated requirement and its commitment to accountability in terms of POPIA, we need to protect the information and systems entrusted to us. That is why we have created this policy, and the supplementary policies, to ensure that our information is adequate and secured against:

- Irresponsible use of information systems and infrastructure.
- Breaches of confidentiality.
- Failures of integrity, and
- Interruptions to the availability of information systems, infrastructure, and applications.

2. Scope

This policy applies to:

- All our information, whether electronic or otherwise, in any location.
- All information systems, infrastructure, and applications.
- Employees, contractors, and other individuals who have access to our information systems, infrastructure, and applications.
- IT equipment that includes desktop PCs, laptops, tablets, printers, physical and wireless network, VPN, and all data centre equipment (servers, switches, routers).

You must be familiar with this policy and comply with its terms. We may supplement or amend this policy with additional policies and guidelines from time to time.

3. Purpose

The purpose of this policy is to inform all Channelport Pty Ltd employees of their responsibilities and guidelines when making use of and accessing information systems, infrastructure, and applications provided by Channelport Pty Ltd, as well as to inform employees of the technical and organisational measures to secure the integrity and confidentiality of all IT systems, infrastructures and applications.

This policy should be read in conjunction with all supplementary policies as per paragraph 7. It is of utmost importance that all employees take great care in complying to the security measures put in place, and to be very diligent when working with company and client information.

4. Roles and responsibilities

- Channelport Pty Ltd management will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.
- Channelport Pty Ltd management is responsible for implementing the requirements of this policy or documenting non-compliance.
- All of the business's employees are required to read and acknowledge this policy.

5. Policy directives

Part I - Management Requirements

- Channelport Pty Ltd will establish formal standards and processes to support the ongoing development and maintenance of the business's IT system and infrastructure.
- Channelport Pty Ltd management will commit to the ongoing training and education of the business's staff responsible for the administration and/or maintenance and/or use of the business's IT system and infrastructure facilities.
- Channelport Pty Ltd management will establish a formal review cycle for all Information Security Policy initiatives and regular tests.
- Any issues with regard to Information Security Policy discovered will be reported to the Information Officer.

Part II – Ownership

All IT systems, infrastructure and applications under the custody and control of the business are the property of the business and employee use of these systems, infrastructure and applications is neither personal nor private. Channelport Pty Ltd management reserves the right to monitor and/or log all employee use of the business's information resources with or without prior notice.

6. Technical and organisational measures

Channelport Pty Ltd's information systems, infrastructure, and applications are provided purely for business purposes and work related research activities where approved.

To guide employees on the various aspects that is contained and referenced to with regard to the use of Channelport Pty Ltd's information systems, infrastructure, and applications, this policy references the following "supplementary" policies which contains comprehensive details regarding each of the aspects related to this Information Security Policy and must be read in conjunction herewith. Each employee is required to familiarise themselves with these "supplementary" policies:

a. Acceptable Use Policy
b. Email Policy
c. Handheld & Mobile Device Policy
d. Access Control Policy
e. Physical Security Policy
f. Antivirus policy
g. Surveillance and Monitoring Policy
h. Risk Management Policy
i. Information Classification Policy
j. Incident Response Policy

The following technical and organisational measures apply to this policy:

- Access to all IT systems, infrastructures and application will be managed by Channelport Pty Ltd management.
- Any changes to access to the IT systems for employees needs to be approved by the Information Officer.
- Access will be limited to allow access only to the required systems and application for the employee to fulfil his/her job.
- Identify all reasonably foreseeable internal and external risks to information in our position or under our control.
- Establish and maintain appropriate safeguards against the risks identified.
- Regularly verify that the safeguards are effectively implemented.
- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.
- Safeguards include but are not limited to:
    - Firewall configurations and monitoring.
    - Cloud firewall applications.
    - Email security measures.
    - Security updates on all servers and other computer equipment used by employees.
    - Security updates on network infrastructure.
    - Antivirus deployment to all servers, and user devices that connects to the network.
- Regular security audits and penetration testing to be conducted on the entire IT environment.

Any issues with regards to security of the IT systems, infrastructure of applications discovered must be reported to Channelport Pty Ltd management on **lanib@channelport.co.za**, where after the incident will be investigated and allocated to either the IT Service Provider's network and systems security analyst, and to the Information Officer for privacy related security issues. Please refer to the "Incident Response Policy" in accordance with this policy.

7. Training

Staff will receive training as part of the induction process. Further training will be provided at least every year or whenever there is a substantial change in the policies and procedures, or IT infrastructure.

Training will be provided through information sessions, regular emails to all staff as well as pre-recorded online webinars, and will cover the latest subjects related to the use of Channelport Pty Ltd's IT systems and applications, the applicable laws relating to data protection, and Channelport Pty Ltd's data protection, and related policies and procedures. Completion of training is compulsory.

If you have any questions or concerns about anything in this policy, do not hesitate to send your query to **lanib@channelport.co.za**.

8. Enforcement

All users are expected to exercise good judgement and act in a professional manner in relation to the use of Channelport Pty Ltd's information systems, infrastructure, and applications. Be aware that disciplinary actions, including possible dismissals, depending on the nature and number of the transgressions, may result from failure to adhere to these standards, and the employee concerned may be held responsible for the costs incurred for not complying to this and related policies.

Channelport Pty Ltd reserves the right to monitor all activities on its information systems, infrastructure, and applications to measure compliance with these standards and to advise appropriate officials of any violations if necessary.

Managers have a responsibility to monitor compliance as with all other Channelport Pty Ltd policies, e.g., POPIA, human resource, finance, and IT policies.

If an employee is in doubt about any aspect of this policy or its interpretation, implementation, and all related policies published by Channelport Pty Ltd, advice should be sought from the employee's immediate manager, the IT Service Provider and Information Officer.

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

Any employee may, at any time, anonymously report policy violations to the IT Service Provider and the Information Officer.

9. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

10. Change history

Date	Author	Version	Change reference

11. Policy approval

Signed: _____

Date: _____

Acceptable Use Policy

Policy	**Acceptable Use Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # C

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing personal information as set out in the Privacy Policy and Information Security Policy.

2. Scope

This policy applies to:

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

You must be familiar with this policy and comply with its terms. We may supplement or amend this policy with additional policies and guidelines from time to time.

3. Purpose

The purpose of this policy is to direct all employees of Channelport Pty Ltd in the acceptable use and security of the business's IT system and infrastructure. These standards contain directions for employees, indicating both acceptable and unacceptable internet use to control employee behaviour and actions that contribute to the business's internet risks while maximising the benefits gained by Channelport Pty Ltd through internet usage. As the software, hardware, and computer network is the property of Channelport Pty Ltd, we reserve the right to keep our systems secure through monitoring electronic information and regular checks on the system.

4. Roles and responsibilities

- Channelport Pty Ltd management will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.

- Channelport Pty Ltd management is responsible for implementing the requirements of this policy or documenting non-compliance.

- All of the business's employees are required to read and acknowledge this policy.

5. Policy directives

5.1. Part I: Management requirements

5.1.1. Channelport Pty Ltd will establish formal standards and processes to support the ongoing development and maintenance of the business's IT system and infrastructure;

5.1.2. Channelport Pty Ltd management will commit to the ongoing training and education of the business's staff responsible for the administration and/or maintenance and/or use of the business's IT system and infrastructure facilities;

5.1.3. Channelport Pty Ltd management will establish a formal review cycle for all Acceptable Use initiatives;

5.1.4. Any security issues discovered must be reported to the Information Officer.

5.2. Part II: Ownership

Electronic files and communications created, sent, received, or stored on information resources owned, leased, administered, or otherwise under the custody and control of Channelport Pty Ltd are the property of Channelport Pty Ltd and employee use of these files and communications is neither personal nor private. The Information Officer may access all such files and communications at any time without the knowledge of the user or owner. The Information Officer and the IT Service Provider reserves the right to monitor and/or log all employee use of the business's information resources with or without prior notice.

5.3. Part III: Acceptable use requirements

5.3.1. Employees will only be given sufficient rights to all systems to enable them to perform their job functions. User rights will be kept to a minimum at all times;

5.3.2. Employees must report any weaknesses in the business's computer security to the IT Service Department. Weaknesses in computer security include unexpected software or system behaviour, which may result in unintentional disclosure of information or exposure to security threats;

5.3.3. Employees must report any incidents of possible misuse of the IT system and infrastructure or violation of this Acceptable Use Policy to Channelport Pty Ltd management;

5.3.4. Employees must not attempt to access any data, documents, email correspondence, or programs contained on the business's systems for which they do not have authorisation;

5.3.5. Employees must not attempt any access penetration tests, any investigations, or perform any other activities to compromise the access controls of the business's computing facilities unless there is a demonstrated business requirement to do so and Channelport Pty Ltd management has approved of such activities;

5.3.6. Systems administrators and authorised users must not divulge remote connection modem phone numbers or other access points to the business's computer resources to anyone without proper authorisation in writing;

5.3.7. Employees must not share their account(s), passwords, Personal Identification Numbers (PIN), security tokens (i.e., smartcard), or similar information or devices used for identification and authorisation purposes;

5.3.8. Employees must not make unauthorised copies of copyrighted software or software owned by the Channelport Pty Ltd;

5.3.9. Employees must not use non-standard shareware or freeware software without approval from Channelport Pty Ltd management

5.3.10. Employees must not purposely engage in activity that may harass, threaten, or abuse others or intentionally access, create, store, or transmit material that Channelport Pty Ltd may deem to be offensive, indecent, or obscene, or that is illegal in terms of legislation;

5.3.11. Employees must not engage in activity that may degrade the performance of information resources, deprive authorised user access to the business's resources, obtain extra resources beyond those allocated, or circumvent the business's computer security measures;

5.3.12. Employees must not download, install, or run security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of the business's computer resources unless approved by Channelport Pty Ltd management

5.3.13. The business's information resources must not be used for personal benefit, political activity, unsolicited advertising, unauthorised fundraising, or for the solicitation of performance of any activity that is prohibited by relevant legislation;

5.3.14. Access to the internet from home-based computers or computers owned by Channelport Pty Ltd must adhere to all the policies. Employees must not allow family members or other non-employees to access non-public accessible computer systems of the business. Employees are not allowed to use personal computers or laptops for business use or connections to Channelport Pty Ltd's network, locally or via VPN;

5.3.15. Employees must not attempt to change the configuration of desktop computers and notebooks. All configuration changes must be handled by Channelport Pty Ltd management for example, upgrading operating systems, changing Windows settings, installing new software or systems, and installing modems, memory, or storage upgrades.

5.3.16. In particular, the business's IT system and infrastructure may not be used for any of the following:

a. Communications in connection with the personal business interests of the user or the user's family;

b. Downloading, transmission, and possession of pornographic and sexually explicit materials;

c. Transmitting defamatory, slanderous, threatening, and abusive messages, inflammatory statements, or any message that may be construed as such;

d. Political or religious statements, foul language, or any other statements viewed as harassing others based on race, creed, colour, age, sex, national origin, disability, or physical attributes are prohibited;

e. Unauthorised attempts to bypass or any attempt to circumvent any security mechanisms of computers connected to the internet;

f. Propagating, sending, responding to, redirecting, forwarding, or otherwise participating in chain letters or junk email;

g. The alteration, destruction, or infringement of the privacy of other employees' computer-based information residing on the IT system and infrastructure and email systems;

h. Playing computer games or engaging in any other form of entertainment or sporting activities during business hours;

i. Any communications or activity which could harm the good name and reputation of the business.

5.3.17. Employees of Channelport Pty Ltd may not send or publish confidential and private material of Channelport Pty Ltd (internal memos, policies, etc.) on any publicly accessible or external internet computer of Channelport Pty Ltd unless the owner of the information has first approved the publication of these materials.

5.3.18. Employees should not transmit confidential information, information of the business, copyrighted materials, or any trade secrets of Channelport Pty Ltd or its clients over any public computer system or network unless properly protected through encryption methods.

5.3.19. Any security issues discovered must be reported to Channelport Pty Ltd management and the Information Officer.

6. Enforcement, Auditing, Reporting

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.
Any employee must, at any time, report policy violations to the Channelport Pty Ltd management which report will be reported as confidential and may be done anonymously.

7. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

8. Change history

Date	Author	Version	Change reference

9. Policy approval

Signed: _____

Date: _____

Email Policy

Policy	Email Policy
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # D

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing personal information. This policy and procedures are a supplement to Channelport Pty Ltd's Information Security Policy.

2. Scope

This policy applies to:

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

You must be familiar with this policy and comply with its terms. We may supplement or amend this policy with additional policies and guidelines from time to time.

3. Purpose

The business provides employees with electronic communication tools, including an email system. This email policy, which governs employee use of the business email system, applies to email use at the business's premises, as well as remote locations, including, but not limited to employee homes, airports, hotels and client and supplier offices. The business's email rules and policies apply to full-time employees, part-time employees, independent contractors, interns, consultants, suppliers, clients, and other third parties. Any employee who violates the business's email rules and policies is subject to disciplinary action, up to and including termination.

4. Email exists for business purposes

The business allows email access primarily for business purposes and employees may not use the email system for any personal use.

5. Email monitoring activities

The business reserves the right to monitor, inspect, copy, review, and store any and all employee's email use at any time and without prior notice. In addition, the business may monitor, inspect, copy, review, and store any files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored through the business's email system. The business reserves the right to disclose e-mail information and images to regulators, courts, law enforcement agencies and other third parties without the employee's consent.

6. Offensive content and harassing or discriminatory activities are banned

Employees are prohibited from using e-mail to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

7. Employees are prohibited from using email to

7.1. Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.

7.2. Send, receive, solicit, print, copy or reply to messages that are disparaging or defamatory.

7.3. Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties.

7.4. Send, receive, solicit, print, copy or reply to sexually orient messages or images.

7.5. Send, receive, solicit, print, copy or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.

7.6. Send, receive, solicit, print, copy or reply to messages or images that are intended to alarm others, embarrass the business, negatively impact employee productivity, or harm employee morale.

8. Confidential, proprietary, and personal information must be protected

Unless authorised to do so, employees are prohibited from using email to transmit confidential information to outside parties. Employees may not access, send, receive, solicit, print, copy or reply to confidential or proprietary information about the business, its employees, clients, suppliers, and other business associates unless there is a legitimate reason to do so. Confidential information includes, but is not limited to, client lists, credit card numbers, identification numbers, employee performance reviews, salary details, trade secrets, passwords and information that could embarrass the business and its employees if the information were disclosed to the public.

9. Information exchange and internet transactions

9.1. All messages communicated on the business's internet and email system must contain the employee's name, surname, title, and contact details. No email or any other electronic communication may be sent which hides the identity of the sender or represents the sender as someone else. All emails sent must include the email signature of the sender.

9.2. The disclaimer as prescribed by Channelport Pty Ltd management be used at the end of all email messages.

10. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

Any employee must, at any time, report policy violations to Channelport Pty Ltd management which report will be reported as confidential and may be done anonymously.

11. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

12. Change history

Date	Author	Version	Change reference

13. Policy approval

Signed: _____

Date: _____

Access Control Policy

Policy	**Access Control Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # E

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing personal information.

2. Purpose

This policy establishes the guidelines for managing user access to information of the business. The purpose is to ensure the necessary user access controls are in place for controlling the actions, functions, applications and operations of legitimate users. The aim is to protect the confidentiality, integrity, and availability of all the business's information resources.

All managers of the business's information resources will ensure that access to the business's information is properly authorised and granted with correct access levels and privileges applied.

3. Scope

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the business's operating environment or connected to the business's information infrastructure.

4. Operational definitions

3.1 Authentication

Verification that the user's claimed identity is valid and is usually implemented through a user password at logon.

3.2 Discretionary user access

The ability to manipulate data using custom or general-purpose programs. The only information logged for discretionary control mechanisms is the type of data accessed and at what level of authority.

3.3 Identification

The act of a user professing an identity to a system, usually in the form of a logon to the system.

3.4 Non-discretionary user access

The access obtained in the process of specific business transactions that affect information in a predefined way. For example, the business's deployment specialists need to access participant information to make travel arrangements, but may not need the ability to change any existing information.

3.5 Password

An arrangement of characters entered by a system user to substantiate their identity, authority, and access rights to an information system they wish to use.

3.6 Privilege

The level of user authority or permission to access information resources. Privileges can be established at the folder, file, or application levels or for other conditions as applicable.

3.7 Special user access privileges

Privileges that allow users to perform specialised tasks that require broad capabilities. For example, changing control functions such as: access control, logging, and violation detection, require special access privileges.

3.8 User account

An issued name with authority, granted to an individual to access a system or software application. System administrators, with proper management approval, typically grant accounts. To access an account, a user needs to be authenticated, usually by providing a password.

3.9 User access controls

The rules and deployment of mechanisms, which control access in information resources, and physical access to premises.

5. Access control measures

5.1. User accounts

The creation of a user account must be initiated through a request to the Information Officer who is authorised to approve access to the specified resources.

5.2. Account management

Channelport Pty Ltd management manages user accounts for the business's systems. Records of processed and denied requests for creation of user accounts must be kept for auditing purposes. Records will be retained for one year, unless otherwise specified in the Data Retention Policy.

5.3. **User accounts characteristics**

All employee user accounts must be unique, and traceable to the assigned user. Channelport Pty Ltd management of the business will take appropriate measures to protect the privacy of user information associated with user accounts. The use of group accounts and group passwords is not allowed, unless specifically approved by the Director(s) of the business.

5.4. **Password reset**

Channelport Pty Ltd management of the business will establish a procedure for verifying a user's identity prior to resetting their password.

5.5. **User account privileges**

Users will be granted the minimum access required to perform their specific tasks. Granting access levels to resources shall be based on the principle of least privilege, job responsibilities and separation of duties. The level of minimum access requires the recommendation of the user's manager and the evaluation of the Information Officer. The Information Officer has final determination as to the level of a user's access for their system.

5.6. **Inactive accounts**

Accounts will be disabled after 30 days of inactivity. Users planning to deploy to field operating locations or to be away from the office for other approved periods of extended absence should coordinate with Channelport Pty Ltd management to ensure proper disposition of the account.

5.7. **Temporary user accounts**

All requests for temporary user accounts shall provide an expiration date to be applied at the time the account is created. Applications for temporary user accounts should be submitted for approval to Channelport Pty Ltd management.

5.8. **Password characteristics**

Channelport Pty Ltd management will establish the minimum requirements for password characteristics.

5.9. **Automatic logon**

The use of automatic logon software to circumvent password entry shall not be allowed, except with specific approval from the Information Officer, for special tasks such as automated backups.

5.10. **User account and password safekeeping**

Each individual assigned a user account and password is responsible for the actions taken under said account, and must not divulge that account information to any other person for any reason.

5.11. **Management of user accounts**

Management access to user accounts will be limited to business purposes only, such as during an emergency or contingency situation, cases of extended user absence or user abuse of the business's information resources. Channelport Pty Ltd management will establish procedures for providing their management with access to accounts assigned to a user within their department. These procedures will be coordinated with the Information Officer.

5.12. **Transfers**

Personnel transferring from one area of responsibility to another shall have their access accounts modified to reflect their new job responsibilities.

5.13. **User access cancellation**

Channelport Pty Ltd management will implement procedures to immediately cancel account access and physical access for users whose relationship with the business has concluded, either on friendly or unfriendly terms.

5.14. **User session time-out**

User sessions will time-out after the prescribed period of inactivity has lapsed, unless otherwise specified as part of the system or application security plan. This includes user connections to the internet, or to specific applications.

5.15. **Remote access security**

Access points for remote computing devices shall be configured using necessary identification and authentication technologies to meet security levels of physically connected computers.

5.16. **New information systems**

All new information systems acquired or developed by Channelport Pty Ltd management will incorporate access controls to properly protect the business's information resources.

5.17. **Sensitive information access**

Individuals in positions with access to sensitive information will be screened for best suitability to the position. These individuals will be subject to the provisions of the business's policies and procedures to protect and safeguard such information from unauthorised disclosure or access.

5.18. **Temporary access to sensitive resources**

Temporary access to resources categorised as sensitive will be set with expiration dates where possible. Channelport Pty Ltd management will monitor temporary access to ensure activities comply with the intended purpose.

6. Roles and responsibilities

6.1. Channelport Pty Ltd management will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy;

6.2. Channelport Pty Ltd management is responsible for implementing the requirements of this policy or documenting non-compliance;

6.3. The Information Officer, are required to train employees on the policy and document issues with policy compliance;

6.4. All of the business's employees are required to read and acknowledge this policy by signing it;

6.5. The Information Officer has primary management responsibility for administering user access to the business's information resources.

7. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

8. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

9. Change history

Date	Author	Version	Change reference

10. Policy approval

Signed: _____

Date: _____

Handheld and Mobile Device Policy

Policy	**Handheld And Mobile Device Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # F

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing personal information.

2. Scope of application and obligations

This policy applies to all employees, consultants, vendors, contractors, students and others using business or private mobile handheld devices on any premises occupied by the business. Adherence to these requirements and the security policies derived from them and implementation of provisions is binding across the whole of the business, its subsidiaries and majority holdings. Wilful or negligent infringement of the policies jeopardises the interests of the business and will result in disciplinary, employment and/or legal sanctions. In the case of the latter the relevant line managers and where applicable legal services shall bear responsibility. These requirements and the security policies derived from them and implementation provisions also apply to all suppliers of the business. They shall be contractually bound to adhere to the security directives. If a contractual partner is not prepared to adhere to the provisions, he must be bound in writing to assume any resulting consequential damage.

3. Purpose

This policy establishes rules for the proper use of handheld devices in the business in order to protect the confidentiality of sensitive data, the integrity of data and applications and the availability of services at the business, protecting both handheld devices and their users, as well as corporate assets (confidentiality and integrity) and continuity of the business.

4. Roles and responsibilities

4.1. Channelport Pty Ltd management must ensure that all employees using devices falling into the category of “handheld devices” have acknowledged this security policy and the associated procedures before they are allowed to use corporate services using handheld devices.

4.2. Channelport Pty Ltd management must ensure that handheld devices and their users comply with this security policy and all security policies as stipulated by the business.

4.3. In a general sense, all users are required to use their common sense in order to act in the best interest of the business, its assets and its services.

4.4. In case of doubt, users must contact Channelport Pty Ltd management to clarify a given situation.

4.5. Users of handheld devices must diligently protect such devices from loss and disclosure of private information belonging to or maintained by the business.

4.6. Before connecting a mobile handheld device to the network at the business, users must ensure it is on the list of approved devices issued by Channelport Pty Ltd management.

4.7. Channelport Pty Ltd management must be notified immediately upon suspicion of a security incident, especially when a mobile device may have been lost or stolen.

4.8. The cost of any item beyond the standard authorised equipment is the responsibility of the employee.

5. Use of private handheld devices

The Information Officer and IT Service Provider must define whether private handhelds are authorised to connect to the business's networks.

5.1. If Private handhelds are not authorised:

- In highly restricted facilities, private handheld devices must be prohibited. In that case, mobile devices must be collected prior to the user's entrance into the facility.
- Private handhelds are authorised in offices, but are not allowed to connect to internal networks.
- Private handhelds must not connect to the business's networks and access corporate information. This includes synchronisation with a workstation connected to the internal networks. The business's networks must be protected accordingly, using network access control mechanisms and must not grant access to any corporate information to unregistered devices.

5.2. If Private handhelds are authorised:

- Any non-business-owned (private) device able to connect to the business's network must first be approved by the Channelport Pty Ltd management.
- If allowed, privately-owned handheld devices must comply with this policy and must be inventoried along with corporate handheld devices, but identified as private. This is in order to prevent theft of corporate data with unmanaged handhelds.

6. Roles and responsibilities

6.1. Channelport Pty Ltd management is responsible for the mobile handheld device policy at the business and shall conduct a risk analysis to document safeguards for each device type to be used on the network or on equipment owned by the business.

6.2. This policy should be reviewed on an annual basis by Channelport Pty Ltd management, taking into account changes according to new services available, new capabilities of devices, changes in corporate backend servers and new threats to mobile devices.

6.3. Channelport Pty Ltd management is responsible for developing procedures for implementing this policy.

6.4. Channelport Pty Ltd management maintains a list of approved mobile handheld devices and makes the list available internally.

6.5. Channelport Pty Ltd management maintains a list of authorised and unauthorised applications.

7. User awareness training

7.1 Users must be trained in order to ensure the proper use of devices and resources of the business. A focus on applications and basic security features of the business is mandatory.

7.2 The following list is not exhaustive, but contains crucial points that must be addressed during the initial training:

- Review of policies;
- Procedure implementation;
- Password protection;
- How to deal with social engineering attacks;
- Proper protection of devices;
- Locking the device;
- Preventing the use of systems by unauthorised users;
- Protecting devices from loss or theft;
- Ensuring the information on a handheld device is absolutely necessary;
- Ensuring the information on a handheld device is also stored on the business's network where it is regularly backed up;
- How to encrypt sensitive information;
- User awareness of changes in technologies and security policies should be regularly tested.

8. Inventory of mobile handheld devices

8.1. Channelport Pty Ltd management must keep inventory of handhelds in use in the business, using associating owner names and identity for network access control.

8.2. The inventory must take into account at least but not limited to the following list of identifiers:

- Device name;
- Owner's ID;
- Device serial number;
- Device IMEI;
- Device's MAC address;
- Owner's ID (user);
- User's MSISDN;
- Device capabilities (Bluetooth, IrDA, camera, etc.);
- Supplementary accessories provided.

9. Authorised services and applications

9.1. Only approved third party applications may be installed on handhelds. The approved list can be obtained by contacting Channelport Pty Ltd management.

9.2. If a desired application is not on the list, a request can be submitted Channelport Pty Ltd management. If the program meets internal testing requirements of stability and security, it will be added and at that point it may be installed.

10. Forbidden devices

10.1. Channelport Pty Ltd management must provide a list of unauthorised applications and communicate it to the users.

10.2. The list of unauthorised applications must remain available to the users via the intranet.

11. Unauthorised actions

11.1. Users must not modify security configurations without request to and approval by Channelport Pty Ltd management

11.2. Unauthorised actions:

- Installing and/or using unauthorised applications or services;
- Removing root certificates from certificate stores;
- Conducting any careless actions leading to an interruption of service;
- Disabling security features.

12. Uncovered issues

All issues that are not covered by this security policy must be brought to the attention of the Information Officer which will treat them on a case-by-case basis.

13. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

14. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

15. Change history

Date	Author	Version	Change reference

16. Policy approval

Signed: _____

Date: _____

Physical Security Policy

Policy	**Physical Security Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # G

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing all aspects related to the business's premises that include computers and other types of information technology resources which must be safeguarded against unlawful and unauthorised physical intrusion, as well as fire, flood, and other physical threats.

2. Scope

This policy addresses threats to critical IT resources that result from unauthorised access to facilities owned or leased by the business, including offices, data centres and similar facilities that are used to house such resources.

3. Purpose

All information resource facilities must be physically protected in proportion to the criticality or importance of their function. Physical access procedures must be documented, and access to such facilities must be controlled. Access lists must be reviewed at least quarterly or more frequently depending on the nature of the systems that are being protected.

3.1 Use of secure areas to protect data and information

The business must use physical methods to control access to information processing areas. These methods could include, but are not limited to, locked doors, secured cage areas, vaults, ID cards and biometrics.

3.2 Physical Access management to protect data and information

Access to facilities that holds critical IT infrastructure, systems and programs must follow the principle of least privilege access. Employees, including full and part-time staff, contractors and vendors' staff should only be granted access to facilities and systems that are necessary for the fulfilment of their job responsibilities.

The process for granting physical access to information resource facilities must include the approval of the Information Officer. Access reviews must be conducted at least quarterly, or more frequently depending on the nature of the systems that are being protected. Removal of individuals who no longer require access must then be completed in a timely manner.

Access cards and/or keys must be appropriately protected, not shared or transferred and returned when no longer needed. Lost or stolen cards/keys must be reported immediately.

The business should ensure that visitors obtain security clearance before entering the premises. This could include, but is not limited to, a sign in book, employee escort within a secure area, ID check and ID badges for visitors.

Computers, printers, and other non-portable information systems equipment belonging to the business must not be removed from the business's premises unless accompanied by an approved property pass issued by the Channelport Pty Ltd management.

Equipment and media taken off the premises should not be left unattended in public areas. Portable computers and other handheld devices must be carried as hand luggage where possible when travelling.

4. Roles and responsibilities

4.1 Channelport Pty Ltd will establish a periodic reporting requirement to measure the compliance and effectiveness of this policy.

4.2 Channelport Pty Ltd management is responsible for implementing the requirements of this policy and documenting non-compliance.

5. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

6. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

7. Change history

Date	Author	Version	Change reference

8. Policy approval

Signed: _____

Date: _____

Antivirus Policy

Policy	**Antivirus Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # H

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing all aspects related to the Anti-Virus's use and procedures within the business.

2. Purpose

The purpose of this policy is to establish minimum anti-virus requirements which must be met by all computers connected to the business's networks and to ensure effective virus detection and prevention.

3. Scope

This policy applies to all of the business's computers that are Macs, PC-based or utilise PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers.

4. Roles and responsibilities

4.1 All of the business's PC-based computers must have the business's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up to date. Virus-infected computers must be removed from the network until they are verified as virus-free. Channelport Pty Ltd management is responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into the business's networks (e.g., viruses, worms, Trojan horses, email bombs, etc.) are prohibited, in accordance with the Information Security Policy and/or Acceptable Use Policy.

4.2 Users must not attempt to remove viruses themselves. If a virus infection is detected, users must disconnect from the business's networks, stop using the infected computer immediately and notify Channelport Pty Ltd management.

4.3 Users must be cautious of email attachments from an unknown source as viruses are often hidden in attachments. If a virus is suspected the attachment must not be opened or forwarded and must be deleted immediately.

5. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

6. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

7. Change history

Date	Author	Version	Change reference

8. Policy approval

Signed: _____

Date: _____

Surveillance and Monitoring Policy

Policy	**Surveillance and Monitoring Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # I

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing all aspects related to Surveillance and Monitoring Systems and procedures within the business.

2. Purpose

The purpose of this policy is to regulate:

- the use of the surveillance and monitoring equipment;
- the safety and property of the business, its employees, and visitors; and
- the applicable legal and privacy interests of the business, its clients, and employees.

3. Scope

This policy applies to Channelport Pty Ltd, all permanent and temporary employees, contractors, consultants, including all personnel affiliated with third parties who use surveillance cameras in the business and/or conduct surveillance monitoring and recording.

4. Definitions

4.1 Surveillance camera

Any item, system, camera, technology device, communications device used alone or in conjunction with a network for the purpose of gathering, monitoring, recording or storing an image or images of the business and/or people at the premises of the business. Images captured by surveillance cameras may be real-time or preserved for review at a later date. Such devices may include, but are not limited to the following:

- Close-circuit television;
- Web cameras;
- Real-time surveillance systems;

- Computerised visual monitoring;
- Cell phone with cameras.

4.2 Surveillance monitoring or recording

Using surveillance cameras or other related technology to observe, review or store visual images for the purpose of deterring crime and protecting the safety and security of the business.

4.3 The business premises

All areas on property owned, leased or controlled by the business, both internal and external, including offices, common spaces and other areas.

5. Compliance principles

The business is committed to integrating the best security. The business's use of surveillance cameras for surveillance monitoring or recording must be:

- Conducted in a professional, ethical, and legal manner;
- Compliant with the business's policies and procedures;
- Limited to uses that does not violate a person's reasonable expectation of privacy, as defined by current legal requirements.

6. Procedures

6.1 Installation and/or placement of surveillance cameras in the business premises must be approved by the Channelport Pty Ltd management and Information Officer of the business.

6.2 Only employees designated by the Channelport Pty Ltd management and/or Information Officer will have access to the images captured by surveillance monitoring or recordings.

6.3 All existing uses of surveillance cameras and surveillance monitoring or recording, subject to this policy, must comply with this policy. A request to continue using the existing surveillance cameras will be submitted to the Information Officer. Network connectivity for surveillance monitoring or recording must comply with the business's policies.

6.4 Violations of these procedures may result in disciplinary action in accordance with the policies, contracts, rules and regulations of the business.

7. Training

The Information Officer will ensure that the designated employees will be trained on the responsible use of the information and technology. Designated employees will also be supervised by a specific supervisor, with periodic review performed by the Information Officer.

8. Retention and release of information

8.1 The business will retain images obtained through surveillance monitoring or recording for a length of time deemed appropriate for the purpose, unless such images have historical value, or are being used for a criminal investigation. Any questions regarding the retention of these images should be directed to the Information Officer.

8.2 Only Channelport Pty Ltd management and / or the Information Officer can authorise the release of information and results obtained through surveillance monitoring or recording.

8.3 Where third parties have access to Channelport Pty Ltd's Surveillance and Monitoring equipment it is the responsibility of Channelport Pty Ltd management to enter into Data Processing Agreements with these third parties to ensure data privacy protection.

9. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

10. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

11. Change history

Date	Author	Version	Change reference

12. Policy approval

Signed: _____

Date: _____

Incident Response Policy

Policy	**Incident Response Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # J

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing personal information breaches effectively.

2. Scope

This policy applies to all staff. You must be familiar with this policy and comply with its terms. This policy supplements our other policies relating to information use. We may supplement or amend this policy by additional policies and guidelines from time to time.

3. Training

All staff will receive training on this policy. New staff will receive training as part of the induction process. Further training will be provided at least every year or whenever there is a substantial change in the policies and procedures.

Training may be provided through information sessions, regular emails to all staff as well as pre-recorded online webinars, and will cover the latest subjects related to the use of Channelport Pty Ltd IT systems and applications, the applicable laws relating to data protection, and Channelport Pty Ltd's data protection, and related policies and procedures. Completion of training is compulsory.

If you have any questions or concerns about anything in this policy, do not hesitate to send your query to the Information Officer.

4. Personal information

Channelport Pty Ltd defines personal information and special personal information as stipulated in the definitions of POPIA.

5. Data breaches

Data breaches may be caused amongst other things, by employees, external parties, third party service providers and computer system errors or vulnerability. Below are a few examples of possible ways in which a data breach can occur:

5.1 Human error

- Loss of computing devices (portable or otherwise), data storage devices, or paper records containing personal information;
- Disclosing data to a wrong recipient/s;
- Handling data in an unauthorised way (downloading information owned by Channelport Pty Ltd for personal use);
- Unauthorised access or disclosure of personal information by employees (sharing passwords);
- Improper disposal of personal information (hard disk, storage media, or paper documents containing personal information sold or discarded before data is properly deleted).

5.2 Malicious activities:

- Hacking incidents / illegal access to databases containing personal information;
- Theft of computing devices (portable or otherwise), data storage devices, or paper records containing personal information;
- Scams that trick Channelport Pty Ltd staff into releasing personal information of individuals.

5.3 Computer system error:

- Errors or bugs in Channelport Pty Ltd's software platforms or websites;

6. Reporting of breaches

All members of staff have an obligation to immediately report actual, suspected or potential data protection incidents. This notification must be done on the "Form for Reporting Information Breaches" annexed hereto as "Annexure IRP 1". Immediate notification is of vital importance as it allows us to amongst other things:

- Investigate the incident and take the necessary steps if required;
- Maintain a register of any possible incidents;
- Notify the Information Regulator should this be required.

All staff must immediately and without any delay notify the Channelport Pty Ltd Data Breach Team of any possible data breaches or suspected incidents as per the reporting lines set out in the Privacy Policy:

6.1 Data Breach Team

The Data Breach Team consists of:

- The Information Officer;
- IT Service Provider.

Depending on the type of incident, the Information Officer in consultation with the other members of the Data Breach Team, will take responsibility to make all time-critical decisions on steps to contain and manage the incident.

6.2 Reporting the incident to the Information Regulator

In the case where a data breach has affected data subjects, a notification must be sent to the Information Regulator and any affected data subjects, should their identity be known. This notification must be done as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system. The notification to the Information Regulator must be done on the form prescribed by the Information Regulator "Annexure A - Form SCN1: Notification of a Security Compromise" annexed hereto as "Annexure IRP 2".

7. Responding to a data breach

Upon being notified of a (suspected or confirmed) data breach, the Data Breach Team should immediately activate the data breach management and response plan.

7.1 Channelport Pty Ltd's data breach management and response plan is:

- Confirm the breach;
- Contain the breach;
- Assess risks and impact;
- Report the incident;
- Evaluate the response & recovery to prevent future breaches;

7.1.1 **Confirm the breach**

The Data Breach Team must act as soon as it is aware of a data breach. Where possible, it must first confirm that the data breach has occurred.

7.1.2 **Contain the Breach**

The Data Breach Team must consider the following measures to contain the breach, where applicable:

- Shut down the compromised system that led to the data breach.
- Establish whether steps can be taken to recover lost data and limit any damage caused by the breach (remotely disabling / wiping a lost notebook containing personal information of individuals).
- Prevent further unauthorised access to the system.
- Reset passwords if accounts and / or passwords have been compromised.

- Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system.

7.1.3 Assess risks and impact

Knowing the risks and impact of data breaches will help Channelport Pty Ltd determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected.

7.1.3.1 Risk and impact on individuals

- How many people were affected?
- Whose personal information had been breached?
- Does the personal information belong to employees, customers, or minors? Different people will face varying levels of risk because of a loss of personal information.
- What types of personal information were involved?
- Any additional measures in place to minimise the impact of a data breach?

7.1.3.2 Risk and impact on organisations

- What caused the data breach?
- Determining how the breach occurred (through theft, accident, unauthorised access, etc.) will help identify immediate steps to take to contain the breach and restore public confidence in a product or service.
- When and how often did the breach occur?
- Who might gain access to the compromised personal information?
- Will compromised data affect transactions with any other third parties?

7.1.4 Report the incident

To comply with the notification requirement imposed on Channelport Pty Ltd should a data breach occur, the following must be considered:

7.1.4.1 How to notify

The business must notify the data subject in writing and ensure that this communication reaches the data subject in at least one of the following ways:

- mailed to the data subject’s last know physical or postal address;
- sent by email to the data subject’s last known email address;

- placed in a prominent position on the website of the business;
- published in the news media; or
- as may be directed by the Regulator.

7.1.4.2 What to notify

The business must ensure that the written notification provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including –

- A description of the possible consequences of the security compromise;
- A description of the measures that the business intends to take or has taken to address the security compromise;
- A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
- If known to the business, the identity of the unauthorised person who may have accessed or acquired the personal information.

7.1.5 Evaluate the response and recovery to prevent future breaches

After steps have been taken to resolve the data breach, Channelport Pty Ltd should review the cause of the breach and evaluate if existing protection and prevention measures and processes are sufficient to prevent similar breaches from occurring, and where applicable put a stop to practices which led to the data breach.

7.1.5.1 Operational and policy related issues

- Were audits regularly conducted on both physical and IT related security measures?
- Are there processes that can be streamlined or introduced to limit the damage if future breaches happen or to prevent a relapse?
- Were there weaknesses in existing security measures such as the use of outdated software and protection measures, or weaknesses in the use of portable storage devices, networking, or connectivity to the Internet?
- Were the methods for accessing and transmitting personal information sufficiently secure, e.g.: access limited to authorised personnel only?
- Should support services from external parties be enhanced, such as vendors and partners, to better protect personal information?

- Were the responsibilities of vendors and partners clearly defined in relation to the handling of personal information?
- Is there a need to develop new data-breach scenarios?

7.1.5.2 Monitoring

- All employees must adhere to this policy.
- The Information Officer or any duly appointed representative has overall responsibility to monitor this policy.
- The Information Officer or any duly appointed representative will review and monitor this policy regularly to make sure it is effective, relevant, and adhered to.

8. Consequences of failing to comply and enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

9. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

10. Change history

Date	Author	Version	Change reference

11. Policy approval

Signed: _____

Date: _____

“Annexure IRP 1”

FORM FOR REPORTING INFORMATION BREACHES

REPORTER DETAILS:

Name and Surname: _____

Department and Office: _____

Date of Reporting: _____

Telephone number: _____

Email address: _____

INCIDENT DETAILS:

Date of Incident: _____

Time of Incident: _____

Time of notification: _____

Provide a brief description of the suspected incident and how it was discovered: (stolen laptop, opened phishing email, etc.)

_____

_____

_____

_____

_____

Did you witness the incident yourself? _____

Did others witness the incident? (if yes, specify below)

_____

_____

_____

_____

_____

To your knowledge was any of the following involved (just indicate – Yes or No)?

Telephone: _____

Fax: _____

Photocopier: _____

Computer Hardware: _____

Email: _____

Internet download: _____

Virus: _____

Theft: _____

Fraud: _____

Unauthorised Access: _____

Third party services providers: _____

Others (specify):

_____

_____

_____

_____

_____

1. Was any of the Internal (employee) or confidential information of the business compromised? _____

2. Was any CLIENT information compromised? _____

3. Was any THIRD-PARTY information compromised? _____

4. Does the suspected incident involve paper record, electronic records or both?

_____

_____

_____

_____

Reported by: _____

Date: _____

Signature: _____

Departmental manager: _____

Date: _____

Signature: _____

"Annexure IRP 2"

ANNEXURE A

FORM SCN1

NOTIFICATION OF A SECURITY COMPROMISE IN TERMS OF SECTION 22 OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

Note:

1. Attach documents in support of the notification
2. Complete the form in full as is applicable
3. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.

A	**DETAILS OF THE RESPONSIBLE PARTY**
Name(s) and Surname/Registered name of the responsible party:	
Address:	Code ( )
Contact Number(s)	
E-mail address:	

B	**DETAILS OF THE INFORMATION OFFICER**
Full names of the Information Officer	
Registration number of the Information Officer	
Contact Number(s)	
E-mail address:	

C	DETAILS OF SECURITY COMPROMISE			
Date of incident				
Date incident reported to Information Regulator				
Explanation for delay in notification to the Regulator, if applicable				
Kindly tick applicable box ✓				
Type of Security Compromise	Loss of personal information			
	Damage to personal Information			
	Unauthorised destruction of personal information			
	Unlawful access to personal information			
	Unlawful processing of personal information			
	Other			
	If other, please explain:			
Type of personal information compromised	Personal information of children		Unique Identifiers	
	Special personal information		Other	
Number of data subjects affected				

Method of notification of affected data subjects	Mail to the data subject's last known physical or postal address;			
	Sent by e-mail to the data subject's last known e-mail address;			
	Placed in a prominent position on the website of the responsible party;			
	Published in the news media			
Does the notification provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise including -	A description of the possible consequences of the security compromise;			
	A description of the measures that the responsible party intends to take or has taken to address the security compromise;			
	A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise			
	If known, the identity of the unauthorised person who may have accessed or acquired the personal information.			
Status of the Compromise	Confirmed		Alleged	

D	**Description of the measures that the responsible party intends to take or has taken to address the security compromise and to protect the personal information of the data subjects from further unauthorised access or use**

E	Declaration
I declare that the information contained herein is true, correct and accurate.	
Signed at _____ on this the _____ day of _____ 20 ____	
_____ **Signature**	
_____ **Name**	_____ **Designation**

Information Classification Policy

Policy	Information Classification Policy
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # K

1. Introduction

This policy aims to guide Channelport Pty Ltd to classify information within the business.

2. Purpose

The purpose of this policy is to classify information to ensure that the correct standards and principles are applied to that information.

3. Responsibility

All of the business's employees share in the responsibility for ensuring that the information receives an appropriate level of protection:

- Managers of the business or information "owners" shall be responsible for assigning classifications to information according to the standard information classification system presented below: "owners" have approved management responsibility, "owners" do not have property rights.

- All employees of the business shall be guided by the information category in their security-related handling of the business's information.

- All information of the business and all information entrusted to the business from third parties fall into one of three classifications in the table below, presented in order of increasing sensitivity.

Information Description	Category	Examples
Unclassified public	Information is not confidential and can be made public without any implications for the business.	• Product brochures widely distributed. • Information widely available in the public domain, including publicly available web site areas of the business. • Sample downloads of the business's software that is for sale. • Financial reports required by regulatory authorities. • Newsletters for external transmission.
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorised access could influence the business's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedures. • Know-how used to process client information. • Standard Operating Procedures used in all parts of the business activities. • All software codes developed by the business, whether used internally or sold to clients.
Confidential data	Information collected and used by the business in the conduct of its business to employ people, to log and fulfil client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the business. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data. • Accounting data and internal financial reports. • Confidential customer business data and confidential contracts. • Non-disclosure agreements with clients\vendors company business plans.

4. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

5. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

6. Change history

Date	Author	Version	Change reference

7. Policy approval

Signed: _____

Dated: _____

Data Retention Policy

Policy	**Data Retention Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # L

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing all aspects related to data retention and procedures within the business.

2. Purpose

The purpose of this policy is to ensure that necessary records and documents of the business are adequately protected and maintained to ensure that records are not retained for longer than necessary. This Policy is also for the purpose of aiding employees of the business in understanding their obligations in retaining documents.

3. Scope

This policy applies to all documents which are collected, processed, or stored by the business and includes but is not limited to documents in hardcopy and electronic format, for example, email, web and text files, PDF documents etc.

4. Guidelines for the retention of documents

4.1 The business may suspend the destruction of any record or document due to pending or reasonably foreseeable litigation, audits, government investigations or similar proceedings. Employees will be notified of applicable documents to which they have access where the destruction has been suspended.

4.2 All documentation and personal information that is being stored by the business in accordance with this policy must be stored and guarded in compliance with all the business's policies.

4.3 The documentation and information listed below may not contain all the records and documents processed and in the possession of the business and should merely be used as a guideline.

4.4 In the event that a document and/or information is no longer required to be stored in accordance with this policy and relevant legislation, it should be deleted and destroyed in accordance with the Data Destruction Policy of the business.

4.5 The Information Officer should be consulted where there is uncertainty regarding the retention and destruction of a document and/or information.

Companies in terms of the Companies Act 71 of 2008

No.	Type of document	Retention period
1	General Rule: Documents, communication etc, not listed below.	Seven (7) years
2	Certificate of Incorporation	Seven (7) years
3	Memorandum of Incorporation and amendments	Indefinite
4	Rules	Indefinite
5	Register of Company Secretary and Auditors	Indefinite
6	Register of Beneficial Ownership greater than 5%	Indefinite
7	Documentation related to shareholder meetings	Seven (7) years
8	Reports presented at the AGM	Seven (7) years
9	Accounting records and annual financial statements	Seven (7) years
10	Securities register	Indefinite

Basic Conditions of Employment Act 75 of 1997

No.	Type of document	Retention period
1	Employee's employment contract, as well as other written records	Three (3) years after termination of employment
2	Time worked by employee	Three (3) years from last entry
3	Remuneration to be paid to each employee	Three (3) years from last entry
4	Date of birth of any employee under 18 years of age	Three (3) years after termination of employment

Labour Relations Act 66 of 1995

No.	Type of document	Retention period
1	Record regarding any applicable collective agreement, arbitration award, determination made in terms of Wage Act	Three (3) years from date of event or end of period to which they relate
2	Details of strike, lockout or protest involving employees	Indefinite
3	Records of employee disciplinary transgression, actions taken and reason therefore	Indefinite

Employment Equity Act 55 of 1998

No.	Type of document	Retention period
1	Records in respect of workforce and employment equity plan	Five (5) years after expiration of the plan
2	Annual report submitted to Director-General of the Department of Labour	Five (5) years from date of submission

Unemployment Insurance Act 63 of 2001

No.	Type of document	Retention period
1	Records of employees – Section 56(2)(c) Names, ID numbers, monthly remuneration, address of employment.	Five (5) years from date of submission

Health and Safety in terms of the Occupational Health and Safety Act 85 of 1993

No.	Type of document	Retention period
1	Annexure A1 Occupational Health and Safety Act, Act No 85 of 1993) Regulation 8 of the General Administrative Regulations	Three (3) years

2	A health and safety committee shall keep record of each recommendation made to an employer in terms of issues affecting the health of employees and of any report made to an inspector in terms of the recommendation.	Three (3) years
	Asbestos	
3	Records in terms of Regulation 23: Asbestos	Minimum of 50 years
	Hazardous Biological Agents	
4	Regulations for Hazardous Biological Agents, records of risk assessment, medical surveillance, and exposure monitoring reports	Minimum of 40 years
5	Record of examinations and repairs in terms of Regulation 12(b)	Minimum of 5 years
6	Records of training in terms of Regulation 4	Three (3) years after termination of employment
7	Self-employed persons risk assessment	Minimum of 40 years
	Hazardous Chemical Agent	
8	Records of assessment and air monitoring	Minimum of 30 years
9	Record of examinations and repairs in terms of Regulation 12(b)	Minimum of 3 years
	Lift, escalator, and passenger conveyor regulations	
10	Certificates and reports in terms of Regulation 7(1) and (2) and 6(4) and Section 24(1)(c)(iii) & (iv)	Minimum 10 years
	Noice Induced Hearing Loss	
11	Records of assessment and noise monitoring	Minimum of 40 years
12	Record of training in terms of Regulation 4(6)	Three (3) years after termination of employment
	Pressure Equipment Regulations	
13	Certificate of manufacturing, results, inspection tests, modifications and repairs	Minimum of 12 years

Credit Agreements in terms of the National Credit Act 34 of 2005

No.	Type of document	Retention period
1	Enquiries	One (1) year
2	Payment profile	Five (5) years
3	Adverse classification of enforcement action or consumer behaviour	One (1) year
4	Civil court judgements	The earlier of 5 years or until the

		judgement is rescinded by a court or abandoned
5	Maintenance judgments	Until rescinded by the court
6	Administration orders	Five (5) years or until the order is rescinded by a court
7	Sequestrations	Five (5) years or until rehabilitation order is granted
9	Rehabilitation orders	Five (5) years
10	Records to be retained in terms of Regulation 55(1)(a) – (d)	Three years from the earliest date on which the registrant created, signed, or received the document
11	Records kept in terms of Section 170	Three (3) years for date of termination of the agreement, or for a refused application, the date of such application.

Tax Records in terms of the Income Tax Act 58 of 1962 and Value Added Tax Act 89 of 1991

No.	Type of document	Retention period
	Income Tax Act	
1	EMP 201 and EMP 501	Five (5) years from date of submission required
2	Sixth Schedule, paragraph 14(a)-(d)	Five (5) years from date of submission or five years from end of tax year.
	Value Added Tax Act	
3	Where Zero rate is applied, proof to substantiate entitlement – Section 11(3)	Five (5) years from date of submission of return
4	Where vendor's basis of accounting is changed, list of debtors and creditors – Section 15(9)	Five (5) years from date of submission of return
5	Documents to be retained where a VAT vendor intends to deduct input tax – Section 16(2)	Five (5) years from date of submission of the return

6	Records to be retained – Section 55(1)(a)	Five (5) years from date of submission of the return

Financial Intelligence Centre Act 38 of 2001

No.	Type of document	Retention period
1	Information pursuant to Sections 21 to 21H	Five (5) years from termination of the business relationship
2	Transaction record – Section 22A	Five (5) years form conclusion of the transaction
3	Suspicious and unusual transactions – Section 29	Five (5) years from submitting report to the Centre

Consumer Protection Act 68 of 2008

No.	Type of document	Retention period
1	Information provided to a consumer by an intermediary	Three (3) years
2	Written disclosure of conflict of interest by an intermediary	Three (3) years
3	Record of advice given to consumer	Three (3) years
4	Written instruction given to consumer	Three (3) years
5	Details pertaining to Promotional Competitions – Section 36 and Regulation 11	Three (3) years
6	Written agreement containing terms and conditions regarding the sale of goods at auctions	Three (3) years

5. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

6. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

7. Change history

Date	Author	Version	Change reference

8. Policy approval

Signed: _____

Date: _____

Data Destruction Policy

Policy	**Data Destruction Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # M

1. Introduction

This policy aims to guide Channelport Pty Ltd in managing all aspects related to data destruction and procedures within the business.

2. Purpose

The purpose of this policy is to provide guidance to the business's employees regarding the destruction of documentation. All forms of computer equipment, digital storage media and printed or handwritten material must be disposed of securely when no longer required. Secure disposal maintains our data security and supports compliance with the business policies and procedures.

The business realises that electronic devices and media can hold vast amounts of information, some of which can linger indefinitely and sees compliance with this policy as of the utmost importance in order to ensure that restricted data and/or personal information does not find its way into unauthorised hands.

3. Scope

This policy aims to ensure secure disposal of data and personal information regardless of form, and applies to all employees of the business, it's premises and networks as well as visitors and third parties. This policy applies to all information systems owned by the business and includes personal computers, laptops, mobile phones, handheld computers, servers and external or removable storage devices and hard copy materials.

4. Secure disposal

4.1 In determining whether a document and/or information should be stored or disposed of, each employee should first refer to the Data Retention Policy and in the event of any uncertainties, to the Information Officer of the business.

4.2 Under no circumstances should paper documents or removable media (CD's, DVD's, discs, etc.) containing personal or confidential information be simply binned or deposited in refuse bins.

4.3 The business will ensure that all, electronic equipment and data on disk drives be physically removed and destructed in such a way that the data will by no means be able to be retrieved.

4.4 Employees must ensure that all paper documents that should be disposed of, must be disposed of as per the internally approve procedures and then be recycled with the minimum requirement being that the information thereon must be de-identified.

4.5 In the event that a third party is used for data destruction purposes, this third party must also comply with the regulations as stipulated in this policy and any other applicable legislation.

5. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

6. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

7. Change history

Date	Author	Version	Change reference

8. Policy approval

Signed: _____

Date: _____

Risk Management Policy

Policy	**Risk Management Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # N

1. Introduction

This Policy aims to guide Channelport Pty Ltd in managing all risk relating to Information Privacy and procedures within the business.

2. Purpose and scope

This policy establishes the process for the management of risks pertaining to personal information faced by the business. The aim of risk management is to maximise opportunities in all the business activities and to minimise risk. The policy applies to all activities relating to the processing of personal information in the business. It is the responsibility of all employees to identify, analyse, evaluate, respond, monitor, and communicate risks associated with any activity, function or process relating to the processing of personal information.

3. Definitions

3.1 **"Risk"** means risk related to processing of personal information in the business.

3.2 **"Risk control"** means taking action to first eliminate risk so far as is reasonably practicable, and if that is not possible, minimising the risks so far as is reasonably practicable.

3.3 **"Risk management"** means the application of a management system and includes identification, analysis, treatment, and monitoring.

3.4 **"Risk owner"** means the person(s) responsible for managing risks and is usually the person directly responsible for the strategy, activity or function that relates to the risk.

4. Principles

The business is proactive in its approach to risk management, balances the cost of managing risk with anticipated benefits, and undertakes contingency planning in the event that critical risks are realised. The business has the primary duty to ensure the reasonable technical and organisational measures are implemented to minimise internal and external risk.

5. Functions and delegations

The Information Officer must exercise due diligence to ensure that the business complies with the POPIA and this policy. This includes taking reasonable steps to:

- gain an understanding of the risks associated with the operations of the business; and
- ensure that the business has and uses appropriate resources and processes to eliminate or minimise risks.

All employees must contribute to the establishment and implementation of risk management systems for all functions and activities of the business. These risk management practices must align with all policies and applicable legislation.

6. Risk management principles

The business must take into consideration the following aspects in adhering to risk management compliance:

6.1 How to assess risk

A Personal Information Impact Assessment must be conducted to ensure that all internal and external risks are identified, mitigated, and addressed.

6.2 Consulting with employees

It is imperative that the employees of the business are made aware of the inherent risks when they process personal information. It is important to have regular meetings with such employees to make sure that the employees have a thorough understanding of the processes and procedures in place to minimise such risk.

6.3 How to control risks

It is important that upon identifying potential risk areas, appropriate measures be put in place to control and/or minimise those risk areas. Where it is possible for the risk to be eliminated completely, this should be done without delay. The responsible person who oversees this potential risk area must be made aware of such risk to implement appropriate safeguards.

6.4 How to review controls

It is important that the business reviews the control measures in place to eliminate and minimise the risk areas on a regular basis.

6.5 How to keep records

It is essential that the business documents and stores all applicable information regarding potential risk areas, as well as the decisions that was made and implemented to address those risk areas. These documents should be stored in accordance with the Data Retention Policy, as well as applicable legislation.

7. Role and responsibility of the Information Officer

The business must take into consideration that the elected Information Officer needs to ensure that all employees, subcontractors, representatives, agents and suppliers have a reasonable understanding of the risks associated with the day-to-day responsibilities and operations in ensuring that the business uses all appropriate resources and available processes to eliminate the business's risk element.

8. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

9. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

10. Change history

Date	Author	Version	Change reference

11. Policy approval

Signed: _____

Date: _____

Clean Desk Policy

Policy	**Clean Desk Policy**
Applicable to	All employees
Person responsible	Information Officer
Document No.	POL # O

1. Introduction

This policy aims to guide Channelport Pty Ltd to establish minimum requirements to ensure information is not left unattended at your workstation.

2. Purpose

The purpose of this policy is to establish the minimum requirements for maintaining a “clean desk” – where all personal information is used.

3. Scope

This policy applies to all Channelport Pty Ltd employees and affiliates contractors, and other individuals who have access to any information systems and/or records containing personal information processed by Channelport Pty Ltd.

4. Policy

4.1. Employees are required to ensure that all information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

4.2. Computer workstations must be locked when workspace is unoccupied.

4.3. Computer workstations must be shut down completely at the end of the workday.

4.4. Any personal information must be removed from the desk and locked in a drawer when the desk is unoccupied, and at the end of the workday.

4.5. File cabinets containing personal information must be kept closed and locked when not in use or when not attended.

4.6. Keys used for access to personal information must not be left unattended.

4.7. Laptops must be either locked with a locking cable or locked away in a drawer or office.

4.8. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

4.9. Printouts containing personal information should be immediately removed from the printer.

4.10. Upon disposal, documents containing personal information should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

4.11. Whiteboards containing restricted and/or sensitive information should be erased.

4.12. Employees must treat mass storage devices such as CDROM, DVD or USB drives as sensitive, and secure them in a locked drawer.

4.13. All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

5. Enforcement

Violation of this policy will result in disciplinary action that may include termination for employees and temporaries, termination of employment relations in the case of contractors or consultants, or dismissal for interns and volunteers. Additionally, individuals are subject to loss of the business's information resources access privileges, civil, and criminal prosecution.

6. Document control

Creation date	24 October 2024
Division name	Channelport Pty Ltd Management
Author name	Lani Botha
Author position	Information Officer
Last updated	24 October 2024
This version	V 01
Latest version approved by the directors of Channelport Pty Ltd	

7. Change history

Date	Author	Version	Change reference

8. Policy approval

Signed: _____

Date: _____