# POLICY MANUAL
# PLAYALOT

## Table of Contents

# Data Protection Policy

## 1. Introduction

Playalot is dedicated to upholding the privacy rights and protecting the personal information of individuals in accordance with the data protection laws and regulations of South Africa, including the Protection of Personal Information Act No. 4 of 2013 ("POPI"). This Data Protection Policy serves as a commitment to data protection, outlining the organization's responsibilities and principles, and providing guidelines for the collection, use, storage, and disclosure of personal information.

## 2. Purpose

The purpose of this policy is to ensure that all employees understand their roles and responsibilities in safeguarding personal information and to promote a culture of privacy and data protection throughout the organization.

## 3. Scope

This policy applies to all employees and/or contractors of Playalot and/or any other individual that makes use of Playalot's premises or facilities. This policy is effective from the date of implementation.

## 4. Roles and Responsibilities

### 4.1. Management Responsibilities

- **Senior Management:** Senior management is responsible for providing leadership and ensuring that adequate resources and processes are in place to comply with data protection laws and regulations. They are also responsible for establishing a culture of privacy and data protection within the organisation.
- **Information Officer and Deputy Information Officer(s):** The Information Officer(s) are responsible for overseeing the organisation's data protection efforts, monitoring compliance with data protection laws, providing advice, guidance and training on data protection matters, handling data subject requests in accordance with applicable laws and regulations and acting as a point of contact for data subjects and regulatory authorities.

### 4.2. Employee Responsibilities

- All employees have a responsibility to comply with this policy, handle personal information in a secure and confidential manner, and report any data protection concerns or incidents to the Information Officer(s) or Information Officer and/or Deputy Information Officer.
- Employees who collect personal information are responsible for ensuring that appropriate consent is obtained, informing data subjects about the processing activities.
- Employees who process personal information are responsible for handling personal information only as instructed/authorised, ensuring the security of the data, and reporting any breaches or unauthorised access immediately to the Information Officer or Information Officer and/or Deputy Information Officer.

## 5. Policy Statement

### 5.1. Principles of Data Protection

#### 5.1.1.Lawfulness, Fairness, and Transparency:

- Personal information shall be processed lawfully, fairly, and transparently, ensuring that individuals are informed about the purposes and processing of their data.
- Employees shall only collect personal information when necessary and for legitimate purposes.

#### 5.1.2.Purpose Limitation and Data Minimisation:

- Personal information shall be collected and processed for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes.
- Employees shall only collect and process personal information that is necessary for the intended purpose and shall avoid excessive data collection.

#### 5.1.3.Accuracy and Storage Limitation:

- Personal information shall be accurate, kept up to date, and necessary steps shall be taken to rectify inaccurate or incomplete data without undue delay.
- Personal information shall be kept in a form that permits identification for no longer than is necessary for the purposes for which it is processed.

#### 5.1.4.Security and Confidentiality:

- Appropriate technical and organisational measures shall be implemented to ensure the security and protection of personal information against unauthorised or unlawful processing and accidental loss, destruction, or damage.
- Employees shall handle personal information in a confidential manner and only disclose it to authorised individuals or organisations in accordance with applicable laws and regulations.

### 5.2. Data Subject Rights

#### 5.2.1.Access and Rectification:

- Data subjects have the right to access their personal information and request corrections or updates where necessary.
- Employees shall assist data subjects in exercising their rights to access and rectify their personal information, providing them with the necessary information and support to fulfill their requests.

#### 5.2.2.Erasure and Restriction:

- Data subjects have the right to request the erasure or restriction of processing of their personal information in certain circumstances.
- Employees shall promptly address and respond to such requests, ensuring that the necessary actions are taken to comply with the data subject's rights, while considering any legal or contractual obligations.

#### 5.2.3.Objection and Portability:

- Data subjects have the right to object to the processing of their personal information and, under certain conditions, the right to data portability.
- Employees shall handle objections and portability requests in accordance with applicable laws and regulations, providing data subjects with the necessary information and support to exercise their rights.

### 5.3. Vendor Management

- When engaging third-party service providers and/or Operators who will process personal information on behalf of the organisation, a due diligence process shall be followed to ensure their compliance with data protection laws and regulations.
- Appropriate contractual agreements, including Operator agreements, shall be in place with third-party service providers and/or Operators, outlining their responsibilities and obligations regarding data protection.

### 5.4. Breach Management

#### 5.4.1.Reporting and Investigation:

- Any actual or suspected data breaches or incidents involving personal information shall be reported immediately to the Information Officer and/or Deputy Information Officer.
- An incident response plan shall be implemented to address and investigate data breaches, including the assessment of potential risks and the implementation of mitigation measures.

#### 5.4.2.Notification and Communication:

- In the event of a data breach that poses a risk to the rights and freedoms of individuals, data subjects affected and relevant authorities shall be promptly notified in accordance with applicable laws and regulations.

### 5.5. Training and Awareness

- Regular data protection training and awareness programs shall be conducted for all employees to ensure a clear understanding of their roles and responsibilities in protecting personal information.
- Training shall cover relevant data protection laws, regulations, policies, and procedures, as well as best practices for handling personal information securely and confidentially.

### 5.6. Policy Compliance and Review

- Regular compliance assessments and audits shall be conducted to ensure adherence to this data protection policy and applicable data protection laws and regulations.
- This data protection policy shall be periodically reviewed and updated to reflect changes in applicable laws, regulations, or organizational practices.
- Employees shall be notified of any updates or revisions to the policy and shall be required to reconfirm their commitment to comply with the updated policy.

## Clean Desk Policy

### 1. Overview

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end-user workspace and locked away when the items are not in use, or an employee leaves his/her workstation. It is one of the top strategies to utilise when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

### 2. Scope

This policy applies to all parties operating within the company network environment or utilising Information Resources. It covers the data networks, servers, and personal computers (stand-alone or network-enabled), located at the company offices, employee home office, and the company production-related locations, where these systems are under the jurisdiction and/or ownership of the company or subsidiaries, and any personal computers, laptops, mobile device and or servers authorised to access the company data networks.

### 3. Policy Statement

#### 3.1. Generic Requirements

3.1.1. Employees are required to ensure that all sensitive/confidential information in hard copy or electronic form is secured in a confidential and safe place in their work area at the end of the day and when they are expected to be absent for an extended period.
3.1.2. Computer workstations must be screen locked when the workspace is unoccupied.
3.1.3. Computer workstations must be shut completely down at the end of the workday.
3.1.4. File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
3.1.5. Keys and access cards used for access to Restricted or Sensitive information must not be left unattended.
3.1.6. Laptops must be either locked with a locking cable or locked away in a drawer.
3.1.7. Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in any form in an accessible location.
3.1.8. Print outs containing Restricted or Sensitive information should be immediately removed from the printer.
3.1.9. Upon disposal, Confidential and/or Restricted documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
3.1.10. All meeting room whiteboards must be cleaned after every meeting.

3.1.11. Lock away unattended portable computing devices such as laptops and tablets.
3.1.12. Treat mass storage devices such as CDROM, DVD, or USB drives as sensitive and secure them in a locked drawer.
3.1.13. All printers and fax machines should be cleared of printed paper as soon as they are printed, this helps ensure that sensitive documents are not left on printer trays for the wrong person to pick up.

# Physical Security Policy

## 1. Introduction

### 1.1. Overview

1.1.1. The purpose of this document is to define rules for protection from fraud, vandalism, sabotage, accidents, and theft of information. These continue to increase costs for the company since the co-mingling of mobility and use of personal devices continues to grow.
1.1.2. This Physical Security document identifies how to protect the company resources from unauthorised physical access and the risks associated with environmental threats and hazards.

### 1.2. Scope

1.2.1. This document is applied to all Management, staff, and contractors.
All IT Resources, regardless of their physical location, are used to store, process, and/or transmit the company electronic information in any form. This includes, but is not limited to networks, computer hardware, mobile devices, software, applications, and associated information used in the support of the company business.

## 2. Policy

### 2.1. Physical Security Requirements

2.1.1. All Service provider's information processing facilities must be physically sound in design and consider landscaping, lighting, fencing, and closed-circuit television on the access routes to the building; that the roof, walls, and flooring are of solid construction; and that exterior access points, windows, and doors are equipped with appropriate security controls (e.g., locks, alarms, bars).

### 2.2. Physical Security Perimeter

2.2.1. Security perimeters of the building or site containing information processing facilities shall depend upon the classification of the information resources within.

### 2.3. Physical Entry Controls

2.3.1. The premises will be controlled with Physical Security Gate Access.
2.3.2. Upon dismissal of employees, access to the premises shall be immediately revoked.
2.3.3. The Access Control system shall keep a log of all activities, entry, and egress.
2.3.4. Privileges to be monitored annually.

### 2.4. Alarm

2.4.1. The premises shall maintain a Primary Alarm, to be switched on after-hours.
2.4.2. The alarm is linked to a security control room.
2.4.3. Testing must be recorded by the person receiving the signal in the control room.
2.4.4. If an alarm failed to trigger, a report must be drafted, and a corrective action plan followed.
2.4.5. Alarms to be tested monthly. When the alarm registers, the appropriate Regional Manager, Branch Manager, or Facilities Manager must be notified via SMS.

### 2.5. Maintenance

2.5.1. No air-con units to be installed above a server.
2.5.2. Air-cons must be serviced bi-annual.
2.5.3. Generator/ UPS shall be serviced.
2.5.4. Facilities Manager shall ensure enough diesel/fuel is kept on site.
2.5.5. The server room shall be cleaned.
2.5.6. Computer equipment being repaired or maintained must be protected corresponding with the sensitivity of the information it contains and the value of the equipment.
2.5.7. Maintenance of systems, hardware, or media containing information - Information Owners shall consider the sensitivity of the information stored on hardware or media when determining whether repairs will be conducted.

### 2.6. Secure Areas

2.6.1. Only authorised employees are allowed access and where relevant signage shall be placed to advise of secure areas and authorised employees entry only.

2.6.2. Access to secure areas is approved according to a specified list

2.6.3. Access to secure areas is protected with physical controls

### 2.7. Access of visitors

2.7.1. Persons who are not employed must obtain access according to the Access Control Policy.

2.7.2. Visitors may enter the secure areas and stay in those areas only in the presence of a host who shall accompany the visitor throughout their whole stay in the secure area.

2.7.3. Access from reception is controlled by a full-time receptionist.

### 2.8. Prohibited activities.

2.8.1. Within secure areas, it is not allowed to:

2.8.1.1. plug any electrical device into a power supply unless specifically authorised to do so.

2.8.1.2. touch or in any other way tamper with any equipment installed in secure areas unless specifically authorised to do so.

2.8.1.3. connect any device to a network unless specifically authorised to do so.

2.8.1.4. archive a larger amount of paper materials.

2.8.1.5. store flammable materials or equipment.

2.8.1.6. use any kind of heating devices.

2.8.1.7. smoke, eat or drink.

### 2.9. Protecting Against External and Environmental Threats

2.9.1. Service providers and their site planners and architects must incorporate physical security controls, which require protection against damage from fire, flood, and other forms of natural disasters, malicious acts, and accidents. Consideration must be given to any security threats presented by neighbouring premises or streets.

### 2.10. Cabling Security (Including Data Centres)

2.10.1. Power and telecommunications cabling carrying data or supporting information services is protected from interception interference, or damage.

### 2.11. Security of Equipment and Assets Off-Premises

2.11.1. Employees are responsible for the physical protection of mobile computing equipment and must take special care when equipment is placed in, or used in, cars or other forms of transportation, public spaces, hotel rooms, meeting places, conference centres, and other unprotected areas outside the company premises.

2.11.2. Employees must ensure that computing equipment being used offsite to access the company information is protected proportional to the sensitivity and the value of the information it contains.

2.11.3. Employees must guard against unauthorised persons reading their computer or mobile computing device's screen when in a public place.

2.11.4. Equipment designated for removal must be recorded.

3. All records must be stored in the pre-allocated location. All physical copies need to be stored in a lockable cabinet or drawer.

# Retention Policy

1. Purpose/Scope
   1.1. The purpose of this Policy is to ensure that necessary records and documents are adequately protected and maintained and to ensure that records that are no longer needed by the Company or are of no value are discarded at the proper time. This Policy is also for the purpose of aiding employees of **Playalot** in understanding their obligations in retaining documents with the objective of mitigating risk and exposure to **Playalot.**
2. Policy
   2.1. All paper or electronic documents indicated under the terms for retention below will be maintained by and subject to the directions of the Human Resources, Legal, Finance or Technical Operations departments.
   2.2. Documents (in any form or format) will be deleted in accordance with the relevant retention/destruction protocol outlined in this Policy.
   2.3.
3. Suspension Of Record Disposal in The Event Of Litigation Or Claims

   In the event **Playalot** is served with summons or request for documents or any employee becomes aware of an investigation or audit concerning **Playalot** or the commencement of any litigation against or concerning **Playalot**, such employee shall inform the Information Officer and any further disposal of documents shall be suspended until such time as the Information Officer, with the advice of counsel, determines otherwise. The Information Officer shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of documents.

4. Terms For Retention
   4.1. Most records and data will follow these timelines: permanent, 7 years, 5 years or 3 years, although specific timelines are contained in the tables provided herein. In some cases, retention may vary by different legislation and be subject to applicable laws. If legislation requires longer retention period they should be adhered to. If shorter, this policy should be followed. Key examples include:
   4.2. Retain <u>permanently</u>:
      4.2.1.1. Corporate governance records.
      4.2.1.2. Tax records.
      4.2.1.3. Stock records.
      4.2.1.4. Intellectual property records.
      4.2.1.5. Certain Financial records.
   4.3. Retain <u>for 7 years</u>:
      4.3.1.1. Certain Employee and Benefit records.
      4.3.1.2. Tax records.
      4.3.1.3. Banking documentation.
   4.4. Retain for <u>3 years</u>:
      4.4.1.1. Certain Human Resources records.
   4.5. Retain for <u>5 years</u>:
      4.5.1.1. Leases, insurance, and contract/license records.
      4.5.1.2. General correspondence and other electronic records, documents, and files.

5. Client Data And Information
   5.1. The company processes data and information about its clients and prospective clients. “Process” means any operation or set of operations that is performed by the company or on it’s, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, performance, disclosure by transmission, dissemination or making available (including making available to view), transfer, alignment, or combination, blocking, erasure or destruction. Processing may be by automated means, through Impact’s technology, or by a vendor at the company’s request. “Personal Data” means personally identifiable information or other information relating to an identified or identifiable natural or juristic person, regardless of that person’s domicile,

and excludes anonymous or anonymised information. The retention of data and information depends

5.2. upon the role that the company has in relation to the data and the relationship that the company has with the data owner.

5.3. Responsible party – The company is the responsible party of its client's personal information. This information is retained while the client is active + 5 Y after the business relationship is terminated. Requests from individuals to delete Personal Data will be processed on a case-by-case basis.

5.4. Prospective clients and other confidential information – Personal data of prospective clients and other confidential information will be retained in accordance with our privacy policy and our agreement with the prospective client or client. Unless agreed with the prospect/client otherwise this shall be active and thereafter + 5Y.

## 6. Administration

Attached as Appendix A is a Record Retention Register/Schedule that is approved as the initial maintenance, retention, and disposal schedule for physical records of Playalot and the retention and disposal of electronic documents and records. The Information Officer/Deputy Information Officer is the officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Register/Schedule is followed. The Information Officer/Deputy Information Officer will also direct any modifications to the Record Retention Register/Schedule from time to time to ensure that it remains compliant with the applicable laws and includes the appropriate document and record categories for Playalot.

The standard retention periods may also be adjusted, in keeping with the applicable laws, in the event of any dispute, audit or legal procedure that requires the relevant documentation to remain available and/or accessible for longer periods than documented in the Record Retention Register/ Schedule. All queries should be raised with the Information Officer/Deputy Information Officer.

The policy will be reviewed, and compliance audited on an annual basis.

## 7. Applicability

This Policy applies to all records, both physical and electronic, that are generated during' Playalot operation, including both original documents and reproductions.

## 8. APPENDIX A RECORD RETENTION REGISTER / SCHEDULE

| Data Records Category | Retention Period | Notes |
|---|---|---|
| ACCOUNTS PAYABLE | | |
| Check requests | 7Y | |
| Expense reports (incl. travel and entertainment) | 7Y | |
| Invoices | 7Y | |
| Journals/ledgers | 7Y | |
| Payment Documents (cc slips, petty cash receipt etc.) | 7Y | |
| Property Taxes | 7Y | |
| Purchase requisitions | 7Y | |
| ACCOUNTS RECEIVABLES | | |
| Collection notices | Superseded | |
| Collection records | 7Y | |
| Credit information / applications | 7Y | |
| Invoices | 7Y | |
| Journals/ledgers | 7Y | |
| Uncollected accounts | 7Y | |
| CAPITAL RECORDS | | |
| Acquisitions | 7Y | |
| Capital asset records | Life of asset +7Y | |
| Capital requisition/authorization requests | Life of asset +7Y | |
| Depreciation schedules | 7Y | |
| Dispositions | 7Y | |
| Journals/ledgers | 7Y | |
| Property/plan/equipment records | Life of asset +7Y | |
| GENERAL ACCOUNTING | | |
| Accounting procedures | Superseded + 7Y | |
| Financial reports - annual | Life of corporation | |
| Financial reports - monthly | 7Y | |
| Financial statements | 7Y | |

| | | |
|---|---|---|
| General ledgers | Life of corporation | |
| Journals/ledgers | 7Y | |
| Registers | 7Y | |
| PAYROLL | | |
| Garnishment records | 5Y | |
| Payroll checks | 7Y | |
| Payroll records | 7Y | |
| Payroll register | Life of corporation | |
| FINANCIAL PLANNING | | |
| Budgets | 5Y | |
| Forecasts | 5Y | |
| Strategic Plan | 5Y | |
| Backlog reports | 5Y | |
| BANKING | | |
| Bank deposits | 7Y | |
| Bank reconciliations | 7Y | |
| Bank statements | 7Y | |
| Check registers | 7Y | |
| Check stubs | 7Y | |
| Checks, cancelled | 7Y | |
| Deposit slips | 7Y | |
| Wire transfers | 7Y | |
| Forex records | 7Y | |
| INSURANCE | | |
| Certificates of Insurance | Superseded +5Y | |
| Insurance Policies | Policy expiration +5Y | |
| Insurance correspondence | Policy expiration +5Y | |
| AUDITS | | |
| External audit reports | Permanent | |
| Attorney contingent liability letters | Permanent | |
| Internal audit reports and working papers | Fiscal year + 7Y | |
| TAX | | |

| | | |
|---|---|---|
| Tax returns/filings | Permanent | |
| Tax department correspondence | Per legislation requirements | |
| CORPORATE SECRETARY | | |
| Annual reports | Life of corporation +7Y | |
| Articles/Certification of incorporation | Life of corporation +7Y | |
| Board of Director/Shareholders meeting notes/minutes | Life of corporation +7Y | |
| Bylaws | Life of corporation +7Y | |
| Dividend records | Assessment of tax +7Y | |
| Proxies, signed | Life of corporation +7Y | |
| Stock certificates | Life of corporation +7Y | |
| Stock ledgers | Life of corporation +7Y | |
| Stock records | Life of corporation +7Y | |
| Stock sales | Life of corporation +7Y | |
| Stock transfers | Life of corporation +7Y | |
| Stockholder, listing of | Life of corporation +7Y | |
| HUMAN RESOURCES | | |
| **Benefits** | | |
| Benefit plans | Superseded +3Y | |
| Disability records | Employment severance +3Y | |
| Incentive plans | Superseded +3Y | |
| Sick leave benefits accrued | 3Y | |
| **General** | | |
| Attendance records | 3Y | |
| Employee manuals | Superseded +3Y | |
| Employee performance reviews | 3Y | |
| Employee vacation requests | 3Y | |
| Job descriptions | 3Y | |
| **Salary administration** | | |
| Pay/wage rates | 3Y | |
| Payroll deductions | 3Y | |
| Payroll records | 3Y | |
| Timecards/sheets | 3Y | |

| | | |
|---|---|---|
| Personnel Actions | | |
| Employee immigrations reports | Longer of hire date + 3 years or termination + 3 year | |
| Layoff records | 3Y | |
| Personnel files | Employment +3Y | |
| Solicited applications | 3Y | |
| Unsolicited applications - rejected | 3Y. | |
| HEALTH & SAFETY | | |
| Accident reports | 5Y | |
| Emergency action plans | Superseded +5Y | |
| Employee medical complaints | 5Y | |
| Health and safety bulletins | 5Y | |
| Health insurance claims | Settlement +5Y | |
| Injury reports | 7Y | |
| Safety records | 5Y | |
| TECHNOLOGY & SECURITY | | |
| Source code | Life of corporation | |
| Design specifications | Life of corporation | |
| Engineering changes | Life of corporation | |
| Security Incident Plan | Superseded +5Y | |
| Security Incident Records | 7Y | |
| Third Party Audit of Systems & Security | Superseded +5Y | |
| Internal Audit of Systems & Security | Superseded +5Y | |
| Business Continuity & Disaster Recovery Plan | Superseded +5Y | |
| FACILITIES | | |
| Building permits | Life of ownership + 5 Y | |
| Maintenance records | Project completion + 5 Y | |
| Real estate records | Life of ownership | |
| Zoning permits | Superseded + 5 Y | |
| LEGAL | | |
| Agreements | Termination/Expiration +7Y | |
| Legal opinions | Annual review | |
| Litigation files | Settlement of all appeals + 5 Y | |

| | | |
|---|---|---|
| Settlement files/agreements | 7Y | |
| Trademark and trademark agreements | Life of corporation | |
| Copyright Records | Life of corporation | |
| CUSTOMER DATA<br>Subject to PAIA request for erasure. | | |
| Client contact info and account usage data | Active +5Y | |
| Client customer data | Active +5Y | |
| CONFIDENTIAL INFORMATION | | |
| Prospective business relationship only | Active + 90 days | |
| Business relationship | Active +5Y | |

# Exceptions Policy

## 1. Introduction

### 1.1. Overview

The purpose of this policy is to ensure that the best interests of (**Error! Reference source not found.**) are maintained. All policies and procedures are to be followed for best practice and adherence to compliance requirements. Where there may be a requirement for an exception, careful consideration must be considered to maintain the best interest and reputation of (**Error! Reference source not found.**) and keep within the legislative and compliance requirements. In such cases, an exception must be documented and approved using the process specified herein.

### 1.2. Scope

All employees, contractors, consultants, temporary workers and other workers at Playalot, including all personnel affiliated with third parties, must adhere to this policy. This policy applies to all exceptions required to implement any policy or procedure within (**Error! Reference source not found.**).

## 2. Policy Statement

### 2.1. Exception Allowances

An exception to a published policy, procedure, or process may be granted in any of the following situations (including IT or information security policies and procedures):

- Temporary exception, where immediate compliance would disrupt critical operations.
- Another acceptable solution where equivalent protection is available.
- A superior solution is available.
- A legacy system is being retired, and compliance is not possible (risk must be managed).
- Long-term exception, where compliance would adversely impact business.
- Compliance would cause a major adverse financial impact that would not be offset by the reduced risk caused by the compliance (i.e. the cost to comply offsets the risk of non-compliance).

## 3. Exception Application Requirements

1. The exception request must document:

1.1. Description of the exception required i.e. the nature of the non-compliance, i.e., specific deviation from the policy/standard

1.2. The specific policy/standard for which an exception is being requested.

1.3. The reason for the exception.

1.4. Why is an exception required, e.g., what business needs or situations exist; what alternatives were considered; and why they are inappropriate.

1.5. Assessment of the potential risk posed by non-compliance, i.e., if the exception is granted.

1.6. Plan for managing or mitigating those risks, e.g., compensating controls, alternative approaches.
1.7. Anticipated length of non-compliance; and
1.8. Any additional information is needed, including any specific conditions or requirements for approval.

## 2. Exception Approval Process

2.1. All requests for exception must be signed by the person responsible for implementing the standards or controls. If the requester is not that person, then the support staff responsible must co-sign.
2.2. All requests for exception must be reviewed and approved by the relevant executive with authority for the resource for which the exception is being requested. Appropriate consideration for information security must be considered and consultation with the IT Manager where required.
2.3. Requests for exceptions must be submitted to the Information Officer/Deputy Information Officer for submission for review for validity and are not automatically approved. Once it has been recorded as approved by the department, the exception is approved. Requests for exception that create significant risk to the infrastructure will not be approved.
2.4. Requests for exceptions must be periodically reviewed to ensure that assumptions or business conditions have not changed.
2.5. Renewals are not automatically approved. The new request for the Policy/Procedure Exception Form must be completed and the process followed again. Time should be made in advance of the
2.6. expiry of the exception to allow for the approval process to be followed should there be a need to continue with the exception.
2.7. Requests for exception may be revoked in the event of a security incident or policy violation using established incident response procedures.

## 2. Policy/Procedure Change

2.1.1. If a certain type of exception is constantly being requested and approved, it may mean that the relevant Policy or procedure needs to be adjusted to include the exception as a norm.
2.1.2. If a superior solution is available, an exception will be granted until the solution can be reviewed, and standards or procedures can be updated to allow for a better solution.
2.1.3. The exception process is intended to be a generic method that applies to all IT/information security policies and standards.

## 3. Exception Application Procedure

3.1.1. The Requester requests an exception form by contacting the Deputy Information Officer. The latest version of the form can be accessed on internal servers.
3.1.2. The Requester completes the form and obtains all required signatures.
3.1.3. The Requester emails the signed form to the Deputy Information Officer for verification. And if satisfied, they will send to the CEO for authorisation.
3.1.4. The Deputy Information Officer will gather any necessary background information, to determine if other administrative officials need to be consulted, and to make a recommendation to approve or deny the request.
3.1.5. The Compliance Officer will contact the requester if additional information is required.
3.1.6. The request will be submitted to the Governance and Compliance Committee and will receive final approval which shall be recorded in the meeting notes.
3.1.7. The Compliance Manager will approve or deny the request for an exception and notify the requester and manager in writing as to the basis for the approval or an explanation of the denial.
3.1.8. If approval is contingent upon meeting specific requirements not documented in the request form, the requester must sign and submit an updated request form.
3.1.9. Any relevant and authorised department may appeal a denial by submitting additional information or requesting a meeting to discuss the decision. After that, all decisions will be considered final.
3.1.10. All requests for exception will be documented and retained by the Compliance Officer.
3.1.11. Exceptions will be valid for a maximum of one year and thereafter reviewed on an annual basis. Duration must be specified on the request form.
3.1.12. If the conditions have substantially changed, a new request for exception must be submitted and documented

# Incident Response Plan

## 1. Introduction:

Playalot understands the importance of an effective incident response plan in addressing and mitigating data breaches and security incidents. This Incident Response Plan Policy outlines the framework and guidelines for responding to incidents promptly, efficiently, and in compliance with the data protection laws and regulations, including the Protection of Personal Information Act ("POPIA"). The purpose of this policy is to establish clear roles, responsibilities, and procedures for incident response, ensuring a coordinated and effective response to protect the confidentiality, integrity, and availability of data.

## 2. Purpose:

The purpose of this policy is to define the procedures and guidelines for responding to security incidents and data breaches within Playalot. The policy aims to provide a structured approach to incident response to minimise the impact of incidents on individuals and the organisation and ensure compliance with relevant laws, regulations, and industry best practices.

## 3. Scope

This policy applies to all employees and/or contractors of Playalot and/or any other individual that makes use of Playalot's premises or facilities. This policy is effective from the date of implementation.

## 4. Roles and Responsibilities:

### 4.1. Management Responsibilities:

- **Senior Management:** Senior management shall provide oversight and support for incident response efforts. They shall ensure that sufficient resources, including personnel, technology, and training, are allocated to effectively respond to incidents. Senior management shall be involved in decision-making processes related to incident response, including escalation and coordination with external stakeholders.
- **Information Officer and Deputy Information Officer(s):** The Information Officer, appointed by Playalot, shall have overall responsibility for incident response activities. The Deputy Information Officer(s) shall support the Information Officer in managing and coordinating incident response efforts. They shall ensure that incident response plans and procedures are regularly reviewed, updated, and communicated to relevant stakeholders. The Information Officer and Deputy Information Officer(s) shall oversee incident reporting, investigation, and the implementation of remediation measures.

### 4.2. Employee Responsibilities:

- All employees shall be responsible for promptly reporting any suspected or confirmed security incidents or data breaches to the Information Officer and/or Deputy Information Officer. Employees shall cooperate fully in incident response activities, providing accurate and timely information to support investigation and resolution efforts. They shall adhere to the incident response procedures outlined in this policy and any related guidelines or instructions provided by the Information Officer and/or Deputy Information Officer.

## 5. Policy Statement:

- For the purposes of this policy the following definitions bear reference:
    - **Incident:** An incident refers to any event or occurrence that has the potential to compromise the confidentiality, integrity, or availability of data, information systems, or the security of an organisation. Incidents can include unauthorised access, unauthorised disclosure, alteration, or destruction of data, security breaches, cyberattacks, system failures, physical breaches, or any other event that poses a risk to the security or privacy of data.
    - **Data Breach:** A data breach refers to a security incident where there is an unauthorised access, acquisition, disclosure, or loss of personal information. It involves the exposure of sensitive, confidential, or protected data to unauthorised individuals or entities. Data breaches can occur due to various reasons, such as cyberattacks, accidental loss or theft of physical devices

or documents containing personal information, insider threats, or vulnerabilities in information systems. The breach may result in potential harm or misuse of the compromised data, leading to risks such as identity theft, financial fraud, or repetitional damage. Organisations are required to report data breaches promptly to the relevant authorities and affected individuals, as mandated by applicable laws and regulations.

- Playalot is committed to maintaining the confidentiality, integrity, and availability of data and responding swiftly and effectively to security incidents and data breaches.
- Incidents shall be promptly reported, assessed, and escalated to ensure an appropriate response and minimize potential harm to affected individuals and the organisation.
- All incidents shall be reported to the Information Officer and/or Deputy Information Officer, whether it has been confirmed that the incident is a data breach or whether it is just suspected.
- Once the breach has been investigated, the affected data subjects will be informed of the data breach (or suspected data breach) and the necessary reporting will happen to the Information Regulator.
- Playalot will report any data breaches (or suspected data breaches) to the Information Regulator within 72 hours of becoming aware of the data breach. This period may be extended if there are circumstances to warrant it i.e. the breach is still under investigation.
- The reporting procedure to the data subject and the Information Regulator will follow the defined process as given by the Information Regulator.
- Incident response procedures shall be regularly reviewed, tested, and updated to reflect changing threats, technologies, and regulatory requirements.
- The organization shall take necessary actions to mitigate the impact of incidents, restore services, and prevent future occurrences.

6. Training and Awareness:
    - Regular training and awareness programs shall be conducted to educate employees about the incident response plan, their roles and responsibilities, and the importance of timely reporting and incident handling.
    - Employees shall be informed of the incident reporting channels, escalation procedures, and the contact details of the Information Officer and/or Deputy Information Officer for incident response.

7. Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the company.

## Work From Home Policy

1. Introduction
    - 1.1. This policy governs work from home to ensure ongoing optimum employee productivity while working from home, while adding to workplace risk mitigation. It caters for the health and safety of employees when work is carried out from home.
    - 1.2. The 'Work from Home Policy 'is not to be used in lieu of sick leave, family responsibility leave, maternity leave, and so forth but only within the constraints set out herein.

2. Scope
    - 2.1. This policy applies to all employees that have been designated the responsibility to carry out their duties from their place of residence and shall be reviewed annually to ensure that it meets legal requirements and reflects best industry practices while giving due consideration to and balancing employee circumstances and The Company operational requirements.

3. Policy Statement
    - 3.1. It has been determined that the Company may require or permit employees to work from home from time to time.

3.2. Working from Home is only available to eligible employees, which will be determined at the business 'sole discretion and is based on operational and/or risk mitigation and management requirements.

3.3. Employees may qualify for home-based working activities under the following conditions/circumstances:

- Control measure to combat the spreading of the COVID-19 virus or any other serious illness.
- Family responsibility emergencies.
- Medical reasons, prohibiting the employee from travelling to work.
- Any other reason which the company in its sole discretion deems necessary.

3.4. Employees that qualify for and are permitted to work from home may do so:

- On specified days.
- Occasional, temporary, or permanently, depending on the employee's nature of work and the circumstances that demand such undertaking be considered.

3.5. Temporary Home-based work arrangements may be approved for circumstances such as special projects, or business travel. These arrangements are approved on an as-needed basis only, with no expectation of ongoing continuance.

3.6. Other informal, short-term arrangements may be made for employees on family or medical leave to the extent practical for the employee and the company and with the consent of the employee's health care provider, if appropriate.

3.7. All informal Home-based work arrangements are made on a case-by-case basis, focusing first on the business needs of the company unless The Company provides communication advising otherwise.

## 4. Performance

4.1. Employees will be permitted to work from home only where the employee's work duties can be performed from home.

4.2. Employees are required to complete all duties, obligations, responsibilities, or conditions of employment in accordance with contractual requirements and in accordance with internal work standards. Employees will be measured on the outcomes they have achieved for the purpose of evaluation.

4.3. Where there are any difficulties in completing any task, the employee must immediately notify his or her manager who will assess the situation and make an appropriate recommendation.

## 5. Tools and Equipment

5.1. Employees must ensure that they have access to required tools, laptops, internet access, communication, recording facilities etc. which will be required for the proper performance of duties.

5.2. Where applicable, equipment and tools provided by the business for the successful application of the Work from Home Policy must be used. Additional resources which may be required need to be discussed with the relevant management representative.

5.3. If, while working from a designated workspace, the employee experiences technical issues with his or her computer or internet access that prevents or hinders the employee from effectively working remotely, the employee must notify his or her manager immediately.

5.4. Internal policies and procedures remain intact and are not affected by the enforcement of this policy. Employees have the responsibility of adhering to the rules and procedures enacted by any other policy when working from home.

## 6. Timekeeping

6.1. Employees are required to follow regular assigned work schedules, unless otherwise discussed with and approved by management. Employees may be asked to work on holidays and weekends if this is provided for in employment contracts.

## 7. Communication

7.1. The company will communicate with the employee on a frequency agreed on to determine and confirm the employee's wellbeing, performance and conformance to company policies and procedures.

7.2. Employees working from a designated workspace will be expected to attend all essential meetings via video conference or by phone.

7.3. Employees who fall under this policy must respond to Company and client communications within the agreed specific timeframe as required by Company standards.

8. Workspace Designation

8.1. Employees must designate a specific area where work activities will be performed at home ("workspace").

8.2. The employee ultimately remains responsible and liable for any other area at home which does not fall within the scope of the designated workspace.

9. Health and Safety Requirements

9.1. Every employee is responsible for their own health and safety and that of others who may be affected by their actions and/or omissions (Occupational Health and Safety Act of South Africa (85 of 1993 Section 14).

9.2. Where employees work from home, the Company enacts employer responsibilities towards the employee through the rules and guidelines needed to ensure a safe working environment at home as per the Health and Safety Act.

9.3. Work must be conducted in such a manner that promotes Health and Safety at home.

9.4. The employee is responsible for inspecting his/her designated workspace before work from home begins, on a periodic scheduled basis thereafter, and whenever work area changes introduce new potential workplace hazards. If any items are identified as a risk, the employee must promptly correct safety concerns before starting work from home. Reporting in respect of this must be sent to management weekly, who will retain all documentation regarding inspections, including findings and corrective actions.

9.5. Any matter that may affect the employee's health and safety at home must immediately be reported to management.

9.6. The workspace must be kept in a safe condition, free from hazards to both the employee and the equipment.

10. Injury on Duty

10.1. The business will not be responsible for any injuries to the employee or any third parties outside of the designated workspace or during the employee's non-working time.

11. Confidentiality and Security

11.1. Employees working remotely remain bound by all confidentiality and/or security agreements and policies and must therefore ensure the protection of proprietary company and customer information which is made available to them and is accessible from their home office.

11.2. Steps include required security protocols, such as maintaining updated antivirus software, regular password maintenance, locked file cabinets and desks to store sensitive information, and any other measures appropriate for the job and the environment of the designated workspace.

11.3. The Company must provide remote support where possible to ensure the employee is able to meet their obligations in respect of confidentiality and data security.

12. Compensation and Other Benefits

12.1. The compensation and benefits of the employee must be discussed with the employee before enforcement of this policy.

12.2. The business is not responsible for any expenses related to remote work during this period, except for that which has been agreed in writing.

13. Return To Office

13.1. Employees working from home may, from time to time, be required to come to their usual work site as required by business needs.

13.2. Interruptions to work caused by internet outages may require the employee to work from their regular office space for the remainder of the day, or until the outage is fixed.

13.3. The business may end the remote work assignment at any time with or without cause, and this permission to work from home may be withdrawn at any time should business needs require this.

13.4. In this instance, employees will be required to return to the workplace, or should circumstances require this, placed on unpaid leave.

13.5. The employee must upon request make themselves available to return to office and if this is not possible must provide management with immediate reasoning and justification, which reasoning will be taken under review and consideration.

14. Non-Compliance

14.1. Breach of this policy will be dealt with under the Disciplinary Procedure and may be treated as gross misconduct which could result in dismissal.

# Direct Marketing Policy

1. Introduction:

Playalot values the trust its customers place in the organisation and is fully committed to safeguarding their privacy and personal information. As part of its unwavering dedication to protecting individual rights, the company has meticulously developed a comprehensive marketing policy that strictly adheres to the requirements outlined in the Protection of Personal Information Act (POPI).

2. Purpose

The purpose of this policy is to ensure that Playalot markets to their clients and prospects in a way that respects their privacy, interests, and complies with section 69 of the POPI Act. This policy outlines the requirements and guidelines for direct marketing activities conducted by Playalot.

3. Scope

This policy applies to all employees, contractors, consultants, temporary workers, and other personnel affiliated with third parties who engage in direct marketing activities on behalf of Playalot. It pertains to clients or prospective clients of Playalot.

4. Roles & Responsibilities

1. Management Responsibilities:

- Senior Management: Senior management is responsible for establishing a culture of compliance, setting the direction for direct marketing efforts, and ensuring adherence to applicable laws and regulations.
- Information Officer and Deputy Information Officer(s): The Information Officer and Deputy Information Officer(s) are responsible for overseeing the implementation and compliance of this policy within Playalot. They provide guidance, support, and address any concerns or issues related to direct marketing.

2. Employee Responsibilities:

- All employees and personnel engaged in direct marketing activities must familiarize themselves with this policy, follow the guidelines outlined herein, and obtain necessary consent before engaging in any direct marketing communication.

5. Policy Statement

- Consent:

- The processing of personal information of a data subject for the purpose of direct marketing through electronic communication is prohibited unless:
    - The data subject has given explicit consent, and
    - The processing is in the client's best interest for existing clients/customers.
- Approaching Data Subjects:
    - Playalot may approach a data subject for direct marketing purposes under the following conditions:
    - Consent is required, and
    - The data subject has not previously withheld consent.
    - Note: Playalot may only attempt to obtain consent from a data subject once
- Obtaining Consent:
    - Consent should be obtained through the following means:
    - Opt-in on Playalot's website
    - Manual opt-in form
    - In client contracts
    - Written consent via a signed document or email.
- Opt-In Form/Consent Requirements:
    - Each opt-in form must clearly state that the consent is for the purpose of direct marketing to the data subject. Without this statement, Playalot cannot process the information for direct marketing purposes.
- Processing Personal Information for Direct Marketing:
    - Processing personal information for direct marketing purposes is allowed if:
    - Contact details were obtained during a sale of a product or service.
    - Marketing is for similar products within the client's best interest.
    - Marketing is solely for the primary purpose of marketing.
    - The client or data subject has not refused to receive communication or previously opted out.
- Direct Marketing Message Requirements:
    - All direct marketing communications must contain the following:
    - Details and identity of the sender (or the person on whose behalf the communication has been sent).
    - An address or contact details to request the cessation of such communication.
    - Optionally, an opt-out button that directly links to Playalot's CRM system.

# Information Security Policy

1. Introduction

Playalot recognises the importance of protecting the confidentiality, integrity, and availability of its information assets. This Information Security Policy establishes the framework for implementing security measures to safeguard sensitive data and maintain compliance with applicable laws and regulations, including the Protection of Personal Information Act (POPI). This policy outlines the roles and responsibilities of employees and management in ensuring the security of information within Playalot.

2. Purpose:

The purpose of this policy is to ensure the protection of information assets from unauthorised access, disclosure, alteration, destruction, and disruption. It aims to establish a secure environment, promote responsible information handling practices, and mitigate risks associated with the storage, transmission, and processing of sensitive data.

3. Scope:

This policy applies to all employees, contractors, and third-party vendors who have access to Playalot's information assets, regardless of the medium or format in which the information is stored.

4. Roles and Responsibilities:

1. Management Responsibilities:

- Senior Management: Senior Management, including the CEO and department heads, are responsible for providing adequate resources and support for implementing and maintaining information security measures, setting the overall direction and objectives for information security, approving security policies, standards, and procedures, ensuring compliance with applicable laws and regulations, and monitoring and regularly reviewing the effectiveness of information security controls.
- Information Officer and Deputy Information Officer(s): The Information Officer and Deputy Information Officer(s) are responsible for overseeing the implementation and enforcement of information security measures, developing and maintaining information security policies, standards, and procedures, conducting risk assessments and ensuring appropriate risk treatment measures are implemented, promoting a culture of security awareness and providing training to employees, coordinating incident response and conducting investigations into security breaches, and serving as the point of contact for information security-related matters.

2. Employee Responsibilities:

- All employees have a responsibility to adhere to information security policies, standards, and procedures, safeguard sensitive information in their custody, use information assets and systems responsibly and ethically, report any security incidents, breaches, or vulnerabilities promptly, and participate in security awareness and training programs.

5. Policy Statement:

- Playalot is committed to maintaining a robust information security posture to protect the confidentiality, integrity, and availability of its information assets. We will implement appropriate technical, administrative, and physical safeguards to ensure the security of sensitive information throughout its lifecycle. Information security is a shared responsibility, and all employees must actively contribute to maintaining a secure environment.

## Acceptable Use Policy

1. Introduction:

Playalot recognises the importance of responsible and secure use of its information resources. This Acceptable Use Policy establishes guidelines and expectations for the appropriate use of company-owned technology, systems, and networks. It aims to protect the integrity, confidentiality, and availability of data and ensure compliance with relevant laws and regulations.

2. Purpose

The purpose of this policy is to define acceptable and prohibited activities when accessing, using, or transmitting Playalot's information resources. It promotes a safe and productive working environment by outlining the responsibilities and obligations of all employees regarding the use of technology resources.

3. Scope

This policy applies to all employees, contractors, and authorised users who have access to Playalot's information resources. It covers the use of company-owned devices, systems, networks, email services, internet access, and any other technology resources provided by Playalot. Compliance with this policy is mandatory and failure to adhere to its provisions may result in disciplinary action.

4. Roles & Responsibilities

4.1. Management Responsibilities

- Senior Management: Provide support and allocate resources to enforce and maintain compliance with this policy. Communicate and promote the importance of acceptable technology use to all employees.

- **Information Officer and Deputy Information Officer(s):** Oversee the implementation and enforcement of this policy. Monitor and assess compliance with acceptable use guidelines.

### 4.2. Employee Responsibilities

- All employees shall use Playalot's technology resources in a responsible and professional manner.
- Protect the confidentiality, integrity, and availability of information.
- Comply with all applicable laws, regulations, and policies when using technology resources.
- Report any suspected or actual security incidents or policy violations promptly.
- Attend and participate in training and awareness programs related to acceptable technology use.

## 5. Policy Statement

- Playalot is committed to ensuring the appropriate and lawful use of its information resources.
- Employees are expected to use technology resources responsibly and for legitimate business purposes only.
- Prohibited activities include, but are not limited to:
    - Violating any local or international laws, regulations, or policies.
    - Engaging in unauthorised access, modification, or disclosure of data or systems.
    - Using technology resources to harass, intimidate, or defame others.
    - Installing unauthorised software or engaging in software piracy.
    - Engaging in activities that may result in the transmission of malware or viruses.
    - Accessing or distributing inappropriate, offensive, or discriminatory material.
    - Unauthorised sharing or disclosure of confidential or sensitive information.
    - Using technology resources for personal gain or engaging in unauthorised commercial activities.
    - Unauthorised use of another individual's credentials or impersonating others.

# Data First Touch Policy

## 1. Introduction:

This policy outlines the guidelines and procedures for the safe and secure handling of data at Playalot. It ensures compliance with the Protection of Personal Information Act (POPI) and incorporates international best practices in data protection. This policy applies to all employees and departments involved in the receipt, collection, transfer, and storage of data.

## 2. Purpose

The purpose of this policy is to establish a framework for the proper handling of data from the moment it is first received or accessed. It aims to ensure data is handled securely, accurately, and in compliance with relevant legislation and regulations. By following this policy, Playalot aims to protect the confidentiality, integrity, and privacy of all data.

## 3. Scope

This policy applies to all forms of data, including electronic data, hard copies, hard drives, and verbal information transcribed into written or electronic format. It covers the entire data lifecycle, including receipt, collation, transit, handover, storage, archiving, retrieval, and discarding. All employees, departments, and systems involved in data handling must adhere to this policy.

## 4. Roles & Responsibilities

### 4.1. Management Responsibilities

- **Senior Management:** Senior management is responsible for promoting a culture of data protection, ensuring compliance with relevant legislation and regulations, and allocating necessary resources for data protection measures.

- **Information Officer and Deputy Information Officer(s):** The Information Officer and Deputy Information Officers are responsible for overseeing data protection efforts, ensuring compliance with applicable laws, and acting as points of contact for data-related queries and incidents.

### 4.2. Employee Responsibilities

- All employees must familiarize themselves with this policy, understand their role in data protection, and comply with the guidelines and procedures outlined herein.
- Employees who handle data must receive appropriate training to ensure they understand the importance of data protection, the procedures to follow, and their responsibilities in safeguarding data.

## 5. Policy Statement

- Playalot is committed to the secure and responsible handling of data throughout its lifecycle.
- The individual giving data and the individual receiving data are jointly responsible to adhere to the below principles.
- We adhere to the following principles:
    - **Data Classification:** All data will be classified based on its sensitivity and handled accordingly.
    - **Consent / Permission:** Written consent or permission from the data subject is required before accepting, transferring, or storing confidential, personal, or private information.
    - **Data Accuracy and Completeness:** All collected data must be accurate, complete, and up to date. Verification from the data subject is recommended.
    - **Data Storage, Transfer, and Discarding:** Proper storage facilities, access controls, and data registration procedures must be in place to safeguard data. Data should be stored in electronic format whenever possible, and physical documents should be minimised.
    - **Data Transfer Requirements and Protocol:** During data transfer, measures must be taken to prevent data breaches, including limiting exposure, using secure containers, and maintaining constant control over the data.
    - **Data Discarding:** When data is no longer needed, it must be properly discarded or archived as per internal policy.
    - **Data Archiving:** Annual assessments will be conducted to determine which documents should be archived and which should be purged based on the internal retention policy.
    - **Data Retrieval:** Data must be stored in a manner that allows for easy tracking, tracing, and retrieval by authorised users only.
    - **Data Revisit and Continuous Update**: Data custodians are responsible for ensuring the accuracy and currency of the data they handle.
    - **Data Breach:** Any suspected data breaches must be reported following internal policy.

# Minimum Access Policy

## 1. Introduction:

The purpose of this policy is to establish rules and requirements for connecting personal computers, laptops, mobile devices, and servers to the company network. These rules aim to minimise potential risks and unauthorised use of company resources, ensuring the protection of sensitive and confidential data, intellectual property, and critical internal systems. Compliance with this policy is crucial to avoid financial liabilities, damage to the company's reputation, and loss of data.

## 2. Scope

This policy applies to all individuals accessing the company network environment or utilising information resources. It includes personal computers, laptops, mobile devices, and servers located at the company offices, production sites, and authorised devices accessing the company data networks.

## 3. Roles & Responsibilities

### 3.1. Management Responsibilities

- **Senior Management:** Senior management is responsible for endorsing and supporting the implementation of this policy, allocating necessary resources for its enforcement, and ensuring its alignment with applicable laws and regulations.
- **Information Officer and Deputy Information Officer(s):** The Information Officer and Deputy Information Officers are responsible for overseeing the implementation of this policy, ensuring compliance, and acting as points of contact for any data-related queries or incidents.

### 3.2. Employee Responsibilities

- All employees must familiarise themselves with this policy, understand their role in complying with it, and adhere to the guidelines and requirements outlined herein.
- Employees accessing the company network from personal devices are responsible for preventing unauthorised access to company resources and data.
- Employees must refrain from engaging in any illegal activities through the company network and understand that they are liable for any misuse of their access privileges.

## 4. Policy Statement

### 4.1. General Requirements

- All employees, contractors, vendors, and agents with access privileges to the company network must ensure that their personal devices comply with the standards outlined in this policy. It is their responsibility to prevent unauthorised access to company computer resources or data. Illegal activities through the company network are strictly prohibited, and users will be held responsible for any misuse of their access privileges.

### 4.2. Operational Procedures

Before connecting personal devices to any company resource, the device owner must request an authorization from management. The assessment will evaluate compliance with the requirements specified below.

### 4.3. Minimum Requirements

- Operating System Updates
  - All Windows devices must have critical and security updates installed and up to date. Before connecting to the corporate network, devices with pending updates must be updated to ensure the latest security measures.
- Anti-Virus Software
  - Devices must have up-to-date anti-virus software installed. If no antivirus software is present, an IT representative will install a free or trial version to scan for malicious applications or files.
- Mobile Device Management Software
  - Employees may be required to install mobile device management software to allow organisation monitoring and enforcement of security protections.
- Prohibited Applications
  - Employees are prohibited from using proxy applications, peer-to-peer file transfer applications, file transfer software other than those approved by the IT department, and network monitoring software without IT approval.
- Data Segregation
  - Employees must segregate personally owned data from company-owned data as much as possible.
- Data Backup Responsibility
  - The device owner is responsible for backing up personally owned data on the device to prevent loss in case of device wiping.
- Liability for Damages
  - The device owner assumes liability for any damages caused by malfunctions, viruses, or other incidents related to their device.

- Access to Confidential and Personal Information
    - Only authorised individuals requiring access to confidential and/or personal information for their job responsibilities will be granted access.

# Removeable Media Policy

## 1. Introduction:

The purpose of this policy is to minimise the risk of loss or exposure of sensitive information and prevent malware infections using removable media within Playalot and its associates' environment.

## 2. Scope

This policy applies to all computers and servers operating within Playalot's environment.

## 3. Roles & Responsibilities

### 3.1. Management Responsibilities

- **Senior Management:** Senior management is responsible for endorsing and supporting the implementation of this policy, allocating necessary resources for its enforcement, and ensuring its alignment with applicable laws and regulations.
- **Information Officer and Deputy Information Officers(s):** The Information Officer and Deputy Information Officers are responsible for overseeing the implementation of this policy, ensuring compliance, and acting as points of contact for any data-related queries or incidents.

### 3.2. Employee Responsibilities

- All employees must familiarise themselves with this policy, understand their role in complying with it, and adhere to the guidelines and requirements outlined herein.
- Employees must only use Playalot removable media on their work computers and obtain explicit permission from the IT Department before using removable media on non-company computers.
- When storing sensitive information on removable media, employees must ensure encryption is applied.
- Employees should dispose of removable media after its intended use, following the guidelines specified in the Disposal and Destruction Policy.
- Employees must cooperate with authorised personnel during monitoring and auditing activities to maintain security and compliance.

## 4. Policy

- Removable media Usage
    - Playalot staff may only use Playalot removable media in their work computers. Removable media should not be connected to or used in computers not owned or leased by Playalot without explicit permission from the IT Department. Prior to connecting removable media to a corporate computer or server, it must be scanned for malware infections.
- Storage of Sensitive Information
    - Sensitive information should only be stored on removable media when necessary for the performance of assigned duties or when providing client information directly to the client. When storing sensitive information on removable media, encryption is required.
- Disposal of Removable Media
    - Information stored on removable media must be destroyed after its intended use and should not be kept for backup purposes. The disposal of removable media must comply with internal policy.
- Monitoring and Auditing
    - Authorised personnel may monitor and audit equipment, systems, and network traffic for security, compliance, and maintenance purposes, in accordance with internal policy.

# Technology Disposal Policy

## 1. Introduction

Playalot recognises the importance of proper technology disposal to safeguard sensitive information and protect individual privacy. This policy establishes guidelines and procedures for the secure and responsible disposal of technology assets, including hardware and electronic media. It aims to ensure compliance with the Protection of Personal Information Act (POPI) and best international practices in data protection.

## 2. Purpose:

The purpose of this policy is to outline the requirements and responsibilities associated with the disposal of technology assets to minimise the risk of data breaches, unauthorised access, and the potential exposure of sensitive information. By adhering to this policy, Playalot aims to protect the privacy and confidentiality of individuals' personal information and maintain compliance with applicable laws and regulations.

## 3. Scope:

This policy applies to all employees, contractors, and third parties who handle or have access to Playalot's technology assets, including but not limited to computers, laptops, mobile devices, storage media, servers, and any other electronic devices that store or process data.

## 4. Roles & Responsibilities:

### 4.1. Management Responsibilities:

- **Senior Management:** Senior management is responsible for ensuring that this policy is implemented effectively throughout the organisation. They must allocate appropriate resources to support technology disposal activities and promote a culture of data protection.
- **Information Officer and Deputy Information Officer(s):** The Information Officer and Deputy Information Officer(s) are responsible for overseeing the implementation of this policy, ensuring compliance with POPI and international best practices. They must monitor technology disposal practices and provide guidance and support to employees.

### 4.2. Employee Responsibilities:

- Employees are responsible for adhering to the procedures outlined in this policy when disposing of technology assets. They must ensure that all sensitive data is removed or securely deleted from the devices before disposal, following the specified guidelines and procedures.

## 5. Policy Statement

### 5.1. Disposal Process:

- When technology assets reach the end of their useful life, employees should send them to the IT Team office for proper disposal. The IT Team will handle the secure disposal of equipment in accordance with the procedures outlined in this policy.

### 5.2. Secure Data Erasure:

- To safeguard sensitive data, the IT Team will securely erase all storage media before disposal. This process includes using disk sanitizing software that cleans each disk sector of the machine with zero-filled blocks. Electronic drives, such as hard drives, will either be degassed or overwritten with a commercially available disk cleaning program. In cases where the memory or storage technology is non-functioning, the memory or storage device will be physically removed and destroyed to ensure data cannot be accessed.

# Backup and Restore Policy

## 1. Introduction

Playalot recognises the critical importance of protecting its data and ensuring business continuity. This Backup and Restore Policy establish guidelines and procedures for the systematic backup and restoration of data assets.

## 2. Purpose

The purpose of this policy is to:

- Ensure the availability, integrity, and confidentiality of Playalot's data.
- Establish procedures for regular backups and secure storage of data.
- Define roles and responsibilities for backup and restore activities.
- Provide guidelines for data restoration in the event of data loss or system failures.
- Ensure compliance with relevant legal and regulatory requirements, including POPI.

## 3. Scope

This policy applies to all employees, contractors, and third-party service providers who handle or have access to Playalot's data. It encompasses all data assets, including but not limited to customer information, employee records, financial data, intellectual property, and any other sensitive or confidential information.

## 4. Roles and Responsibilities

### 4.1. Management Responsibilities

- **Senior Management:** Provide support and resources necessary for the implementation of backup and restore procedures. Approve backup and restore strategies and associate budgetary requirements.
- **Information Officer and Deputy Information Officer(s):** Oversee the implementation and compliance with backup and restore policies, ensure adequate backup systems and processes are in place, monitor the effectiveness and efficiency of backup and restore activities and review and update backup and restore procedures as necessary.

### 4.2. Employee Responsibilities

- Follow backup and restore procedures as outlined in this policy and related documentation.
- Report any data loss or system failures promptly to the relevant Management.
- Protect backup media and storage locations from unauthorised access or damage.
- Comply with data classification and handling guidelines to ensure appropriate backup and restore measures are applied to different data types.

## 5. Policy Statement

### 5.1. General Requirements

- At Playalot, we recognise that despite implementing best practices, there is always a risk of systems or procedures failing, which could result in the loss of access to information, data, and systems. To mitigate these risks, we have established the following steps to ensure the secure backup and restoration of Playalot information and data in the most efficient manner possible.

### 5.2. Data Backups (One Drive)

- The Playalot IT team is responsible for providing system support and conducting data backup tasks. They must ensure that adequate backup and system recovery practices, processes, and procedures are followed.
- All IT backup and recovery procedures must be documented, regularly reviewed, and made available to trained personnel who are responsible for performing data and IT system backup and recovery.
- All infrastructure data on servers, including servers, networking, and supporting system configuration files, must be systematically backed up in the event of system re-installation and/or configuration.

- Backup media must be encrypted and appropriately labeled with dates and codes/markings that enable easy identification of the original source of the data and the type of backup used. Encryption keys should always be securely stored.
- Backup media retained on-site before being sent for storage at a remote location must be stored securely. Playalot must ensure that both the original and backup copies are stored in separate physical locations.
- Access to the original and backup locations must be restricted to authorised personnel only.
- All backups identified for long-term storage must be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media.
- Important paper files should be scanned and stored electronically to create digital copies that can be backed up by Playalot's Information and Communications Technology systems. If scanning is not possible, photocopies of paper files must be made and stored in a secure location.
- Regular tests must be conducted to evaluate the effectiveness of Playalot's backup and restore procedures. This includes restoring data/software from backup copies and analysing the results. Any issues that arise during testing should be promptly reported to the IT Team.
- The IT Team should be notified when backups fail, providing detailed information such as backup job details and reasons for the failure. A record must be maintained, documenting backup job failures and any actions taken.
- Backup data/media no longer required must be clearly marked and recorded for secure disposal, with due consideration for environmental impact.

### 5.3. User Responsibilities

- Users also have a responsibility to ensure that Playalot data is securely maintained and available for backup.
- Users must not store any data/files on the local drive of a computer, excluding the normal functioning of the Windows operating system and other authorised software that requires local file caching. Instead, users must save data (files) in their allocated areas. Storing data (files) locally puts them at risk of exposure, damage, corruption, or loss since they will not be backed up.
- If the company network becomes unavailable, users may need to save data (files) locally on the computer being used or on approved storage media, such as a company-owned encrypted Data stick (USB storage). Once the Playalot network becomes available again, users should immediately transfer the data (files) to the company network for safe backup. Local copies of data on the computer or portable storage media must be deleted to avoid duplicate copies and maintain data availability and integrity.
- Mobile phones can be used to store sensitive, business, or personally identifiable information, but users must comply with applicable processing of personal information laws.

### 5.4. Data Restores

- Data (file) restores are carried out by the Playalot IT Team, who will make every effort to restore files from the specified date or the nearest backed-up date.
- Users must request data (files) to be restored by contacting the IT Team. Only files that the user is authorised to access will be provided from the restore.
- The IT Team will verify that the user has permission and/or authorization to view or obtain restored copies of files and/or folders.
- Users requesting a restore must provide necessary information about the data (files), including:
    - The reason for the restoration.
    - The name of the file(s), folder(s), or system(s) to be restored.
    - The date, day, or time of deletion/corruption or the nearest approximation.
    - The last date, day, or time when the user recalls the data (files) being intact and successfully accessed/used.
- All backup and recovery (restoration) procedures must be documented and made available to the Playalot IT Team for performing data (file) restores.
- Requests from third-party software/hardware vendors for file or system restores, for the purpose of system support, maintenance, testing, or other unforeseen circumstances, should be made under the

supervision of the IT Manager, CEO, or a designated Playalot representative appointed by the IT Manager or CEO.

- Personnel accessing backup media for the purpose of restoring must ensure that any media used is returned to a secure location when no longer required.

# Password Policy

## 1. Introduction:

Passwords play a crucial role in computer security, and choosing a strong password is essential to protect Playalot's resources. This policy outlines the guidelines and requirements for selecting and securing passwords to prevent unauthorised access and exploitation of Playalot's assets.

## 2. Scope

This policy applies to all employees, contractors, consultants, temporary workers, and personnel affiliated with third parties who have access to Playalot's systems or devices connected to Playalot's network. This policy outlines the guidelines and requirements for selecting, changing, and securing passwords manually, without the use of a password management system. All individuals covered by this policy are responsible for adhering to these guidelines to maintain the security and confidentiality of Playalot's resources and sensitive information.

## 3. Purpose

The purpose of the Password Policy is to establish guidelines and requirements for the selection, management, and protection of passwords used within Playalot. This policy aims to ensure the security and confidentiality of Playalot's resources and sensitive information by promoting strong and unique passwords, minimising the risk of unauthorised access, and preventing potential exploitation of accounts.

## 4. Roles & Responsibilities

### 4.1. Management Responsibilities

- **Senior Management:** Endorse and support the implementation of this policy, allocate necessary resources, and ensure alignment with applicable laws and regulations.
- **Information Officer and Deputy Information Officer(s):** Oversee the policy's implementation, ensure compliance, and serve as points of contact for data-related queries or incidents.

### 4.2. Employee Responsibilities

- All employees must familiarise themselves with this policy, understand their role in compliance, and adhere to the guidelines and requirements.
- Use only Playalot's approved passwords and follow the password construction guidelines.
- Report any suspected password compromise to Management.
- Safeguard and protect passwords and avoid sharing them with anyone.
- Comply with all password-related policies and guidelines.

## 5. Policy Statement

- **Password Creation**
  - All user-level and system-level passwords must adhere to the "Password Construction Guidelines" specified in this policy.
  - Users should not use the same password for Playalot accounts as for personal or other access (e.g., personal ISP account, internet banking, social media).
  - Users should avoid reusing the same password for different access needs within Playalot.
- **Password Change**
  - All user-level passwords must be changed manually at least every ninety calendar days.
  - Employees must change their password immediately if they suspect a compromise or unauthorised access to their account.
- **Password Protection**
  - Avoid sending plaintext passwords over networks or email to maintain security.
  - Passwords must not be shared with anyone and should be treated as restricted information.

- If passwords need to be shared electronically, they must be encrypted, and the encryption key should be shared through a separate medium.
- Do not reveal passwords on questionnaires or security forms.
- Avoid hinting at the password format, such as using personal information.
- Do not share passwords with anyone, including administrative assistants, secretaries, managers, co-workers, or family members.
- Do not write passwords down or store them in your workspace.
- Do not store passwords in files on computer systems or mobile devices.
- Avoid using the "Remember Password" feature of applications.
- If a user suspects their password has been compromised, they must report the incident to Playalot's Management immediately and request a password change for all user access accounts.
- The use of password managers is allowed, subject to pre-authorised software list approval by InfoSec and IT departments.

- Password Construction Guidelines
  - Pass-phrases are recommended for increased security. A passphrase is a longer version of a password, typically composed of multiple words.
  - A strong password should be relatively long and include a combination of upper and lowercase letters, numbers, and special characters.
  - Passwords listed in the password blacklist are prohibited.
  - Playalot passwords must meet at least three of the following four characteristics:
    - Contain at least 12 alphanumeric characters.
    - Include both upper- and lowercase letters.
    - Contain at least one number (0-9).
    - Contain at least one special character ($%^&*()_+|~-¬-=`{}[]:";'<>?,/).
- Password Examples
  - Examples of weak passwords to avoid:
    - Single dictionary words (e.g., "Password").
    - Personal information (e.g., birthdate, family names, pet names).
    - Work-related information (e.g., building names, system commands, sites, companies, hardware, or software).
    - Number patterns (e.g., ababa, qwerty, zyxwvuts, or 123321).
    - Common words spelled backwards or combined with numbers (e.g., terces, secret1, or 1secret).
    - Variations of common passwords like "Welcome123," "Password123," or "Changeme123."
- Mobile Phone Passwords
  - Mobile phones used to access company information must comply with the Minimum Access Policy and have a password set.
  - Passwords for mobile phones must meet the following requirements:
    - Minimum Password Length - Set to a minimum of 5 characters.
    - Password Complexity - Numeric patterns or consecutive numbers (e.g., "1111" or "1234") are not allowed.
    - Maximum Inactivity Time Before Password Required - Set to 5 minutes

## Server Policy

1. Introduction:

   The purpose of this Server Policy is to establish standards and guidelines for the configuration, management, and security of servers within Playalot. This policy aims to ensure the proper ownership, registration, and maintenance of server infrastructure, as well as adherence to security best practices to mitigate risks associated with server vulnerabilities.

## 2. Purpose

The purpose of this policy is to define the requirements and procedures for the deployment, configuration, and monitoring of servers owned, operated, or leased by Playalot. It aims to safeguard critical systems and sensitive information by implementing appropriate security measures and maintaining an accurate inventory of servers. This policy ensures the consistent application of server installation, ownership, and configuration management practices throughout Playalot.

## 3. Scope

This policy applies to all employees, contractors, consultants, temporary workers, and other personnel affiliated with Playalot. It encompasses all server equipment owned, operated, or leased by Playalot or registered under the company's internal network domain.

## 4. Roles & Responsibilities

### 4.1. Management Responsibilities

- **Senior Management:** Senior management is responsible for supporting the implementation and enforcement of this policy, setting a positive example by adhering to the policy and encouraging compliance among their teams, and ensuring that appropriate resources are allocated to meet the requirements of this policy.
- **Information Officer and Deputy Information Officer(s):** The Information Officer and Deputy Information Officer(s) are responsible for overseeing the implementation and compliance of this policy, providing guidance and support to management and employees regarding server security and best practices, and periodically reviewing and updating the Server Policy to align with regulatory requirements and industry best practices.

### 4.2. Employee Responsibilities

- Complying with this Server Policy and related procedures.
- Reporting any suspected security incidents or vulnerabilities related to servers to the IT department.
- Using servers and associated services responsibly and in accordance with authorised access and usage policies.
- Cooperating with server audits, monitoring, and security assessments.

## 5. Policy Statement

### 5.1. General Requirements

- All internal servers deployed at Playalot must be owned by an operational group responsible for system administration.
- Approved server configuration guides must be established and maintained, based on business needs and approved by IT and Security.
- Servers must be registered within the corporate enterprise management system, providing accurate and up-to-date information for each server.

### 5.2. Configuration Requirements

- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall.
- The most recent security patches must be installed promptly, with exceptions made only when business requirements necessitate delay.
- Secure channel connections, such as encrypted network connections using SSH or IPSec, must be used for privileged access when available.
- Servers should be physically located in access-controlled environments and are prohibited from operating from uncontrolled areas.

### 5.3. Monitoring

- All security-related events on critical or sensitive systems must be logged, and audit trails should be retained for a specified duration.

- Security-related events, including port-scan attacks, unauthorised access to privileged accounts, or anomalous occurrences, should be reported to the IT and/or Security departments for review and appropriate action.
- All records must be stored in a designated location with proper security measures, including lockable cabinets or drawers.

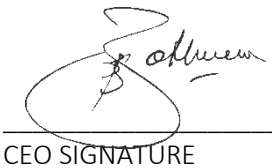
## Enforcement

An employee found to have violated this policy manual may be subject to disciplinary action, up to and including termination of employment. A violation of this policy manual by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Playalot.

FRANCOIS BOTHMA

_____

CEO NAME



_____

CEO SIGNATURE

19/11/2025

_____

DATE

# PAIA & POPIA MANUAL PLAYALOT

This manual sets out Playalot's compliance with the Promotion of Access to Information Act (PAIA) and the Protection of Personal Information Act (POPIA), including procedures for accessing information and data subject rights.

This manual has been prepared in terms of the section 51 of the Promotion of Access to Information Act 2 of 2000 and to address the requirements of the Protection of Personal Information Act 4 of 2013.

## Table of Contents



*Although we have used our best endeavors to supply a list of applicable legislation, it is possible that this list may be incomplete. Whenever it comes to our attention that existing or new legislation allows a Requester access on a basis other than as set out in PAIA, we shall update the list accordingly. If a Requester believes that a right of access to a record exists in terms of other legislation listed above or any other legislation, the Requester is required to indicate what legislative right the request is based on, to allow the Information Officer the opportunity of considering the request in light thereof

## 1. DEFINITIONS

| | |
|---|---|
| Client | Any natural or juristic person that received or receives services from the Company. |
| Conditions for Lawful Processing | The conditions for the lawful processing of Personal Information as fully set out in chapter 3 of POPI and in paragraph 12 of this Manual. |
| Data Subject | The person to whom Personal Information relates. |
| Information Officer | The individual who is identified in paragraph 3 of this manual. |
| Manual | This manual. |
| PAIA | The Promotion of Access to Information Act 2 of 2000. |

| | |
|---|---|
| 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 –<br>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.<br>b. Information relating to the education or the medical, financial, criminal or employment history of the person.<br>c. Any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other assignment to the person.<br>d. The biometric information of the person.<br>e. The personal opinions, views or preferences of the person.<br>f. Correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.<br>g. The views or opinions of another individual about the person; and<br>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. |
| Personnel | Any person who works for or provides services to or on behalf of the Company, and receives or is entitled to receive remuneration and any other person who assists in carrying out or conducting the business of the Company, which includes, without limitation, directors (executive and non-executive), all permanent, temporary and part-time staff as well as contract workers. |
| POPI | The Protection of Personal Information Act 4 of 2013. |
| POPI Regulations | The regulations promulgated in terms of section 112(2) of POPI. |

| | |
|---|---|
| Private Body | Means –<br>a. A natural person who carries or has carried on any trade, business or profession, but only in such capacity.<br>b. A partnership which carries or has carried on any trade, business or profession; or<br>c. Any former or existing juristic person but excludes a public body. |
| Processing | Means any operation or activity or any set of operations, whether by automatic means, concerning personal information, including –<br>a. The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;<br>b. Dissemination by means of transmission, distribution or making available in any other form; or<br>c. Merging, linking, as well as restriction, degradation, erasure or destruction of information. |
| SAHRC | The South African Human Rights Commission. |

Any other terms not described herein will have the meaning as ascribed to it in terms of PAIA or POPI.

## 2. INTRODUCTION

2.1. To POPI and PAIA, the Company is defined as a private body. In accordance with the Company's obligations in terms of POPI and PAIA, the Company has produced this manual.
2.2. This manual sets out all information required by both PAIA and POPI.
2.3. This manual also deals with how requests are to be made in terms of PAIA.
2.4. This manual also establishes how compliance with POPI is to be achieved.

## 3. CONTACT DETAILS

| | |
|---|---|
| Business Name | Playalot (Pty) Ltd – 2018/076829/07<br>Playalot 101 (Pty) Ltd – 2019/592325/07<br>Playalot 103 (Pty) Ltd – 2020/090850/07 |
| Registered Office | Pinehurst, 3 Tanzanite Cres, Durbanville, Cape Town, 7550, South Africa |
| Postal Address | Pinehurst, 3 Tanzanite Cres, Durbanville, Cape Town, 7550, South Africa |
| Contact Number | 087 138 7529 |
| Information Officer | Salome Els |
| Email address/es | salome@playalot.co.za |

**4.**

Background information of how the Company processes information can be found at: www.playalot.co.za

## 4. GUIDE OF INFORMATION REGULATOR

4.1. A guide to PAIA and how to access information in terms of PAIA has been published pursuant to section 10 of PAIA.
4.2. The guide contains information required by an individual who may wish to exercise their rights in terms of PAIA.
4.3. Should you wish to access the guide you may request a copy from the Information Officer by submitting **ANNEXURE A**, attached hereto, to the details specified above.
4.4. You may also inspect the guide at the Company's offices during ordinary working hours.
4.5. You may also request a copy of the guide from Information Regulator at the following details:

**Information Regulator:**

| | |
|---|---|
| Postal Address: | P O Box 31533, Braamfontein, Johannesburg, 2017 |
| Telephone: | +27 (10) 023-5200 |
| Website: | www.justice.gov.za |
| Email: | PAIAComplaince.IR@justice.gov.za |

## 5. LATEST NOTICES IN TERMS OF SECTION 52(2) OF PAIA

5.1. At this stage no Notice(s) has/have been published on the categories of records that are available without having to request access to them in terms of PAIA.

## 6. AVAILABILITY OF CERTAIN RECORDS IN TERMS OF PAIA

6.1. The Company holds and/or processes the following records for the purposes of PAIA and POPI.
6.2. The following records may be requested; however, it should be noted that there is no guarantee that the request will be honored. Each request will be evaluated in terms of PAIA and any other applicable legislation.

**Products and/or Services:**

- All products and/or services are available freely on the Company's website as set out above.

Human Resources:

- Employment Contracts
- Employee Benefits
- Personnel Records and Correspondence
- Training Records
- Internal Policies
- Information pertaining to share options, share incentives, bonus or profit-sharing agreements of each employee

Legal:

- Agreements with Clients
- Agreement with Suppliers
- Shareholder Agreements
- Licenses and Permits
- Sale Agreements
- Lease Agreements

Company Secretarial:

- Memorandum of Incorporation
- Secretarial Records
- Tradename Registrations
- Trademark Registrations
- Company Registration Documents
- Statutory Registers
- Minutes of Shareholder's meetings
- Minutes of Director's meetings
- Register of Directors
- Share Certificates

Financial:

- Accounting Records
- Annual Reports
- Interim Reports
- Auditor Details and Reports
- Tax Returns
- Insurance Records

Client:

- Client Database
- Credit Applications
- Correspondence with Clients
- Documentation prepared for Clients.
- Invoices, receipts, credit and debit notes

Marketing:

- Published Marketing Material

Miscellaneous:

- Internal Correspondence
- Information Technology Records
- Domain Name Registrations
- Website Information
- Asset Registers
- Title Deeds

## 7. RECORDS AVAILABLE IN TERMS OF OTHER LEGISLATION

7.1.1. Basic Conditions of Employment Act, No. 75 of 1997
7.1.2. Companies Act, No. 71 of 2008
7.1.3. Compensation for Occupational Injuries and Diseases Act, No. 130 of 1993
7.1.4. Consumer Protection Act, No. 68 of 2008
7.1.5. Constitution of the Republic of South Africa Act, No. 108 of 1996
7.1.6. Electronic Communication and Transactions Act, No. 25 of 2002
7.1.7. Employment Equity Act, No. 55 of 1998
7.1.8. Identification Act, No. 68 of 1997
7.1.9. Income Tax Act, No. 58 of 1962
7.1.10. Insolvency Act, No. 24 of 1936
7.1.11. Machinery and Occupational Safety Amendment Act No. 181 of 1993
7.1.12. National Payment Systems Act No. 78 of 1998
7.1.13. Occupational Health and Safety Act No. 85 of 1993
7.1.14. Patents, Designs and Copyright Merchandise Marks Act, No. 17 of 1941
7.1.15. Promotion of Access to Information Act, No. 2 of 2000
7.1.16. Protection of Personal Information Act, No. 4 of 2013
7.1.17. Skills Development Levies Act, No. 9 of 1999
7.1.18. The Labour Relations Act, No. 66 of 1995
7.1.19. Trademark Act No. 194 of 1993
7.1.20. Value Added Tax Act, No. 89 of 1991

**Although we have used our best endeavors to supply a list of applicable legislation, it is possible that this list may be incomplete. Whenever it comes to our attention that existing or new legislation allows a Requester access on a basis other than as set out in PAIA, we shall update the list accordingly. If a Requester believes that a right of access to a record exists in terms of other legislation listed above or any other legislation, the Requester is required to indicate what legislative right the request is based on, to allow the Information Officer the opportunity of considering the request in light thereof.*

## 8. REQUEST PROCESS

8.1. An individual who wishes to place a request must comply with all the procedures laid down in PAIA.
8.2. The requester must complete ANNEXURE B, which is attached hereto, and submit it to the Information Officer at the details specified above.
8.3. The prescribed form must be submitted as well as payment of a request fee and a deposit, if applicable to the information officer at the postal or physical address, fax number or electronic mail as is stated herein.
8.4. The prescribed form must be completed with enough particularity to enable the information officer to determine:
  8.4.1. The record(s) requested.
  8.4.2. The identity of the requestor.
  8.4.3. What form of access is required; and
  8.4.4. Postal address or fax number of the requestor.
8.5. The requestor must state that the records are required for the requestor to exercise or protect a right and clearly state what the nature of the right is so to be exercised or protected. An explanation of why the records requested is required to exercise or protect the right.
8.6. The request for access will be dealt with within 30 days from date of receipt, unless the requestor has set out special grounds that satisfies the Information Officer that the request be dealt with sooner.

8.7. The period of 30 days may be extended by not more than 30 additional days, if the request is for a large quantity of information, or the request requires a search for information held at another office of the Company and the information cannot be reasonably obtained within 30 days. The information officer will notify the requestor in writing should an extension be necessary.

8.8. The Information Officer must communicate a response to the request for access using "Annexure E", this communication shall inform the requestor of:

8.8.1. The decision.

8.8.2. Fees payable in terms of paragraph 11.

8.9. If the Information Officer is of the opinion that the searching and preparation of the record for disclosure would amount to more than 6 hours, he/she shall inform the requestor to pay a deposit not exceeding one third of the amount payable.

8.10. Should the requestor have any difficulty with the form or the process laid out herein, the requestor should contact the Information Officer for assistance.

8.11. An oral request can be made to the Information Officer should the requestor be unable to complete the form due to illiteracy or a disability. The Information Officer will complete the form on behalf of the requestor and provide a copy of the form to the requestor.

## 9. GROUNDS FOR REFUSAL

9.1. The following are grounds upon which the Company may, subject to the exceptions in Chapter 4 of PAIA, refuse a request for access in accordance with Chapter 4 of PAIA:

9.1.1. Mandatory protection of the privacy of a third party who is a natural person, including a deceased person, where such disclosure of Personal Information would be unreasonable.

9.1.2. Mandatory protection of the commercial information of a third party, if the Records contain:

9.1.2.1. Trade secrets of that third party.

9.1.2.2. Financial, commercial, scientific or technical information of the third party, the disclosure of which could likely cause harm to the financial or commercial interests of that third party; and/or

9.1.2.3. Information disclosed in confidence by a third party to The Company, the disclosure of which could put that third party at a disadvantage in contractual or other negotiations or prejudice the third party in commercial competition.

9.1.3. Mandatory protection of confidential information of third parties if it is protected in terms of any agreement.

9.1.4. Mandatory protection of the safety of individuals and the protection of property.

9.1.5. Mandatory protection of Records that would be regarded as privileged in legal proceedings.

9.1.6. Protection of the commercial information of the Company, which may include:

9.1.6.1. Trade secrets.

9.1.6.2. Financial/commercial, scientific or technical information, the disclosure of which could likely cause harm to the financial or commercial interests of the Company.

9.1.6.3. Information which, if disclosed, could put the Company at a disadvantage in contractual or other negotiations or prejudice the Company in commercial competition; and/or

9.1.6.4. Computer programs which are owned by the Company, and which are protected by copyright and intellectual property laws.

9.1.7. Research information of the Company or a third party, if such disclosure would place the research or the researcher at a serious disadvantage; and

9.1.8. Requests for Records that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources.

## 10. REMEDIES SHOULD A REQUEST BE REFUSED

10.1. The Company does not have an internal appeal procedure considering a denial of a request, decisions made by the information officer is final.

10.2. The requestor may in accordance with sections 56(3) (c) and 78 of PAIA, apply to a court for relief within 180 days of notification of the decision for appropriate relief.

## 11. FEES

11.1. The following fees shall be payable upon request by a requestor:

| | |
|---|---|
| Request fee<br>(Payable on every request) | R140.00 |
| Photocopy of an A4 page or part thereof | R2.00 |
| Printed copy of an A4 page or part thereof | R2.00 |
| Hard copy on flash drive<br>(Flash drive to be provided by requestor) | R40.00 |
| Hard copy on a compact disc<br>(Compact disc to be provided by requestor) | R40.00 |
| Hard copy on a compact disc<br>(Compact disc to be provided by the Company) | R60.00 |
| Transcription of visual images per A4 page | As per quotation of service provider |
| Copy of visual images | As per quotation of service provider |
| Transcription of an audio record per A4 page | R24.00 |
| Copy of an audio record on flash drive<br>(Flash drive to be provided by requestor) | R40.00 |
| Copy of an audio on a compact disc<br>(Compact disc to be provided by requestor) | R40.00 |
| Copy of an audio on a compact disc<br>(Compact disc to be provided by the Company) | R60.00 |
| To search for and prepare the record for disclosure for each hour or part of an hour, excluding the first hour, reasonably required for such search and preparation | R145.00 |
| To search for and prepare the record for disclosure for each hour or part of an hour, excluding the first hour, reasonably required for such search and preparation<br>(Cannot exceed total cost) | R435.00 |

| | |
|---|---|
| Postage, email or any other electronic transfer | Actual expense, if any |

11.2.

## 12. POPI

12.1. Conditions for lawful processing:

12.1.1. POPI has eight conditions for lawful processing and includes:

12.1.1.1. Accountability
12.1.1.2. Processing limitation
12.1.1.3. Purpose specification
12.1.1.4. Further processing limitation
12.1.1.5. Information quality
12.1.1.6. Openness
12.1.1.7. Security safeguards
12.1.1.8. Data subject participation

12.1.2. The Company is involved in the following types of processing:

12.1.2.1. Collection
12.1.2.2. Recording
12.1.2.3. Organization
12.1.2.4. Structuring
12.1.2.5. Storage
12.1.2.6. Adaptation or alteration
12.1.2.7. Retrieval
12.1.2.8. Consultation
12.1.2.9. Use
12.1.2.10. Disclosure by transmission
12.1.2.11. Dissemination or otherwise making available
12.1.2.12. Alignment or combination
12.1.2.13. Restriction
12.1.2.14. Erasure
12.1.2.15. Destruction

12.1.3. The Company processes information for the following purposes:

12.1.3.1. To fulfil agreements in relation to its employees.
12.1.3.2. to provide services to its clients in accordance with terms agreed to by the Clients.
12.1.3.3. to undertake activities related to the provision of services, such as
12.1.3.3.1. to fulfil domestic legal, regulatory and compliance requirements.
12.1.3.3.2. to verify the identity of Customer representatives who contact the Company or may be contacted by The Company.
12.1.3.3.3. for risk assessment, information security management, statistical, trend analysis and planning purposes.
12.1.3.3.4. to monitor and record calls and electronic communications with the Client for quality, training, investigation and fraud prevention purposes.
12.1.3.3.5. to enforce or defend the Company or the Company affiliates' rights.
12.1.3.3.6. to manage the Company's relationship with its clients, which may include providing information to its clients and its clients affiliates about the Company's and the Company affiliates' products and services.
12.1.3.4. the purposes related to any authorised disclosure made in terms of agreement, law or regulation.
12.1.3.5. any additional purposes expressly authorised by the Company's client.
12.1.3.6. any additional purposes as may be notified to the Client or Data Subjects in any notice provided by the Company.

12.2. The Company processes personal information the following categories of Data Subjects:

12.2.1. Juristic persons –

12.2.1.1. Corporate Clients

12.2.1.2. Suppliers

12.2.2. Natural persons –

12.2.2.1. Individuals

12.2.2.2. Staff

12.2.2.3. Clients

12.2.2.4. Suppliers

12.3. The Company process the following categories personal information:

12.3.1. Client profile information.

12.3.2. Bank account details.

12.3.3. Payment information.

12.3.4. Client representatives.

12.3.5. Names.

12.3.6. Email addresses.

12.3.7. Telephone numbers.

12.3.8. Facsimile numbers.

12.3.9. Physical addresses.

12.3.10. Tax numbers.

12.3.11. Identity numbers.

12.3.12. Passport numbers.

12.4. Recipients of Personal Information.

12.4.1. The Company, the Company's affiliates, their respective representatives.

12.5. When making authorised disclosures or transfers of personal information in terms of Section 72 of POPI, personal information may be disclosed to recipients in countries that do not have the same level of protection for personal information as South Africa does.

12.6. The following Security measures are implemented by the Company:

12.7. The Company implements numerous Security measures to protect personal information that is stored electronically and physically.

12.7.1. The Company ensures that appropriate security measures are taken and updates these measures on a regular basis.

12.7.2. The Company have also implemented various policies for additional security for personal information stored both physically and electronically.

12.8. The personal information that is stored physically is protected as follows:

12.8.1. Where physical records of the data exist, such records will be stored in a secure area that can be 'locked-away' as to avoid a breach of the personal information.

12.8.2. Such physical data records will be 'locked-away' and secured when not in use.

12.9. The Company may share personal information with third parties and in certain instances this may result in cross border flow of the personal information. The personal information will always be subject to protection, not less than the protection it is afforded under the Protection of Personal Information Act No.4 of 2013.

12.10. Objection to the processing of personal information by a data subject:

12.10.1. Section 11(3) of POPI and regulation 2 of the POPI regulations provides that a data subject may, at any time object to the processing of their personal information in the prescribed form attached to this manual as **ANNEXURE "B".**

12.11. Request for correction or deletion of personal information:

12.11.1. Section 24 of POPI and regulation 3 of the POPI regulations provides that a data subject may request for their personal information to be corrected and/or deleted in the prescribed form attached hereto as **ANNEXURE "C"**.

12.11.2. Regulation 8 of the POPI regulations provides for requests the outcomes of requests and of fees payable in the prescribed form attached hereto as **ANNEXURE "E"**.

SIGNATURE INFORMATION

OFFICER : _____

DATE : _____

# ANNEXURE A

## FORM 1

### REQUEST FOR A COPY OF THE GUIDE
[Regulations 3]

**TO:** The Information Officer

_____

_____

I,

| | | | | |
|---|---|---|---|---|
| Full Names: | | | | |
| In my capacity as *(mark with "X")*: | Information Officer: | | Other: | |
| Name of Public/Private Body (if applicable): | | | | |
| Postal Address: | | | | |
| Street Address: | | | | |
| E-mail Address: | | | | |
| Facsimile: | | | | |
| Contact Numbers: | Tel. (B): | | Cellular: | |

Hereby request the following copy(ies) of the Guide:

| Language *(mark with "X")*: | No of Copies | Language *(mark with "X")*: | No of Copies |
|---|---|---|---|
| Sepedi | | Sepedi | |
| Setswana | | Setswana | |
| Tshivenda | | Tshivenda | |
| Afrikaans | | Afrikaans | |
| isiNdebele | | isiNdebele | |
| isiZulu | | isiZulu | |

Manner of Collection *(mark with "X")*:

| Personal Collection | Postal Address | Facsimile | Electronic Communication (Please Specify) |
|---|---|---|---|
| | | | |

Signed at _____ this _____ day of _____ 20 ____.

_____

Signature of Requester

# ANNEXURE B

## FORM 2

### REQUEST FOR ACCESS TO RECORD

[Regulations 7]

**NOTE:**

1. *Proof of identity must be attached by the requester.*
2. *If requests made on behalf of another person, proof of such authorization, must be attached to this form.*

**TO:** The Information Officer

_____

_____

_____

_____

*(Address)*

E-mail Address: _____

Fax Number: _____

*Mark with an" X"*

☐ Request is made in my own name ☐ Request is made on behalf of another person

| PERSONAL INFORMATION | |
|---|---|
| Full Names: | |
| Identity Number: | |
| Capacity in which request is made *(when made on behalf of another person):* | |
| Postal Address: | |
| Street Address: | |

| | | | | |
|---|---|---|---|---|
| E-mail Address: | | | | |
| Contact Numbers: | Tel. (B): | | Facsimile: | |
| | Cellular: | | | |
| Full Name of person on whose behalf request is made *(if applicable)*: | | | | |
| Identity Number: | | | | |
| Postal Address: | | | | |
| Street Address: | | | | |
| E-mail Address: | | | | |
| Contact Numbers: | Tel. (B): | | Facsimile: | |
| | Cellular: | | | |

PARTICULARS OF RECORD REQUESTED

*Provide full details of the record to which access is requested, including the reference number if that is known to you, to enable the record to be located. (If the provided space is inadequate, please continue a separate page and attach it to this form. All additional pages must be signed.)*

| | |
|---|---|
| Description of record or relevant part of the record: | |
| | |
| | |
| | |
| | |
| Reference number, if available: | |
| Any further particulars of record: | |
| | |
| | |

| | |
|---|---|
| | |
| | |

| TYPE OF RECORD<br>*(Mark the applicable box with an "X")* | |
|---|---|
| Record is in written or printed form | |
| Record comprises virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc.)* | |
| Record consists of recorded words or information which can be reproduced in sound | |
| Record is held on a computer or in an electronic, or machine-readable form | |

| FORM OF ACCESS<br>*(Mark the applicable box with an "X")* | |
|---|---|
| Printed copy of record *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)* | |
| Written or printed transcription of virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc.)* | |
| Transcription of soundtrack *(written or printed document)* | |
| Copy of record on flash drive *(including virtual images and soundtracks)* | |
| Copy of record on compact disc drive *(including virtual images and soundtracks)* | |
| Copy of record saved on cloud storage server | |

| MANNER OF ACCESS<br>*(Mark the applicable box with an "X")* | |
|---|---|
| Personal inspection of record at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)* | |
| Postal services to postal address | |
| Postal services to street address | |
| Courier service to street address | |
| Facsimile of information in written or printed format *(including transcriptions)* | |
| E-mail of information *(including soundtracks if possible)* | |
| Cloud share/file transfer | |
| Preferred language<br>*(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)* | |

| PARTICULARS OF RIGHT TO BE EXERCISED OR PROTECTED<br><br>*If the space provided is inadequate, please continue on a separate page and attach it to the Form. The requester must sign all the additional pages.* | |
|---|---|
| Indicate which right is to be exercised or protected | |
| | |
| | |

| | |
|---|---|
| Explain why the record requested is required for the exercise or protection of the aforementioned right: | |
| | |
| | |

| FEES | |
|---|---|
| *a) A request fee must be paid before the request is considered.*<br>*b) You will be notified of the amount of the access fee to be paid.*<br>*c) The fee payable for access to a record depends on the form in which access is required, and the reasonable time required to search for and prepare a record.*<br>*d) If you qualify for exemption of the payment of any fee, please state the reason for exemption.* | |
| Reason | |
| | |
| | |

You will be notified in writing whether your request has been approved or denied and if approved the costs relating to your request, if any. Please indicate your preferred manner of correspondence:

| Postal Address | Facsimile | Electronic Communication (Please Specify) |
|---|---|---|
| | | |

Signed at _____ this _____ day of _____ 20 ____.

_____

Signature of Requester / Person on whose behalf request is made

_____

*FOR OFFICAL USE*

| | |
|---|---|
| *Reference Number:* | |
| *Request received by:*<br>*(State Rank, Name and Surname of Information Officer)* | |
| *Date Received:* | |
| *Access Fees:* | |
| *Deposit (if any):* | |

_____

*Signature of Information Officer*

## ANNEXURE C

### FORM 1

**OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION**
**IN TERMS OF SECTION 11(3) OF THE**
**PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)**

**REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017**
[Regulation 2(1)]

**Note:**

1. *Affidavits or other documentary evidence in support of the objection must be attached.*
2. *If the space provided for in this Form is inadequate, submit information as anAnnexure to this Form and sign each page.*

Reference Number _____

| DETAILS OF DATA SUBJECT | |
|---|---|
| Name and Surname of Data Subject | |
| Residential, postal or business address | |
| Contact number(s) | |
| Fax number: | |
| E-mail address: | |

| DETAILS OF RESPONSIBLE PARTY |
|---|

| | |
|---|---|
| Name and Surname of Responsible Party (if the Responsible Party is a natural): | |
| Residential, postal or business address | |
| Contact number(s) | |
| Fax number: | |
| E-mail address: | |
| | |
| Name of Public Body or Private Body (if Responsible Party not a natural person): | |
| Business address: | Code ( ) |
| Contact number(s): | |
| Fax number: | |
| e-mail address: | |

| |
|---|
| REASONS FOR OBJECTION<br>*(Please provide detailed reasons for the objection)* |

Signed at _____ this _____ day of _____ 20 ____.

_____

*Signature of Data Subject (Applicant)*

ANNEXURE D

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2017
[Regulation 3(2)]

NOTE:

1. *Affidavits or other documentary evidence in support of the request must be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to thisForm and sign each page.*

Reference Number _____

Mark the appropriate box with an "x"

1. **Request For:**

☐ Correction or deletion of personal information about the data subject which is in possession or under the control of the party responsible.

☐ Destroying or deleting a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

| DETAILS OF DATA SUBJECT | |
|---|---|
| Name and Surname of Data Subject | |
| Residential, postal or business address | |
| Contact number(s) | |
| Fax number: | |
| E-mail address: | |

| DETAILS OF RESPONSIBLE PARTY | |
|---|---|
| Name and Surname of Responsible Party (if the Responsible Party is a natural): | |
| Residential, postal or business address | |
| Contact number(s) | |
| Fax number: | |
| E-mail address: | |
| | |
| Name of Public Body or Private Body (if Responsible Party not a natural person): | |
| Business address: | Code ( ) |
| Contact number(s): | |
| Fax number: | |
| e-mail address: | |

REASONS FOR

*CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT/

*DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT WHICH IN IN THE POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY
*(Please provide detailed reasons for the objection)*

Signed at _____ this _____ day of _____ 20 ____.

_____
*Signature of Data Subject*

## ANNEXURE E

FORM 3

OUTCOME OF REQUEST AND OF FEES PAYABLE
[Regulation 8]

1. *If your request is granted –*
   (a) *Amount of the deposit, if any, is payable before your request is processed; and Requested record/ portion of the record will only be released once proof of full payment is received.*
2. *Please use the reference number hereunder in all future correspondence.*

Reference number: _____

TO: _____
_____
_____
_____

Your request dated_____ refers

## 1. You Requested

| | |
|---|---|
| Personal Inspection of information at registered address of public/private body *(including listening to recorded words, information which can be reproduced in sound, or information held on computer or in an electronic or machine-readable form)* is free of charge. You are required to make an appointment for the inspection of the information and to bring this Form with you.<br><br>If you then require any form of reproduction of the information, you will be liable for the fees in Annexure B | |

OR

## 2. You Requested

| | |
|---|---|
| Printed copies of the information *(including copies of any virtual images, transcriptions and information held on computer or in an electronic or machine-readable form)* | |
| Written or printed transcription or virtual images *(this includes photographs, slides, video recordings, computer-generated images, sketches, etc.)* | |
| Transcription of soundtrack *(written or printed document)* | |
| Copy of information on flash drive *(including virtual images and soundtracks)* | |
| Copy of information on compact disc drive *(including virtual images and soundtracks)* | |
| Copy of record saved on cloud storage server | |

3.

## 3. To be Submitted

| | |
|---|---|
| Postal services to postal address | |
| Postal services to street address | |
| Courier service to street address | |
| Facsimile of information in written or printed format *(including soundtracks if possible)* | |
| Cloud share/file transfer | |
| Preferred language:<br>*(Note that if the record is not available in the language you prefer, access may be granted in the language in which the record is available)* | |

4.

Kindly note that your request has been:

☐ Approved

☐ Denied, for the following reasons:

| |
|---|
| |

5. Fees are payable with regard to your request:

| Item | Cost per A4-size page or part thereof /item | Number of pages /items | Total |
|---|---|---|---|
| Photocopy | | | |
| Printed copy | | | |
| For a copy in a computer-readable form on:<br>(i) Flash drive<br>• To be provided by requestor<br>(ii) Compact disc<br>• If provided by requestor<br>• If provided to the requestor | R40.00<br>R40.00<br>R60.00 | | |
| For a transcription of visual images per A4-size page | Service to be outsourced. Will | | |
| | depend on the quotation of the | | |
| Copy of visual images | | | |
| | service provider | | |
| Transcription of an audio record, per A4-size | R24.00 | | |
| Copy of an audio record | | | |
| (i) Flash drive | | | |
| • To be provided by requestor | R40.00 | | |
| (ii) Compact disc | | | |
| • If provided by requestor | R40.00 | | |
| • If provided to the requestor | R60. 00 | | |
| Postage, e-mail or any other electronictransfer: | Actual costs | | |
| **TOTAL:** | | | |

6.

**1.** **Deposit payable (if search exceeds six hours):**

☐ Yes

☐ No

| | | | |
|---|---|---|---|
| Hours of search | | Amount of deposit *(calculated on one third of total amount per request)* | |

The amount must be paid into the following Bank account:

Name of Bank:

Name of account holder:

Type of account:

Account number:

Branch Code:

Reference Nr:

Submit proof of payment to:

Signed at_____this_____day of_____20 _____

_____

Information officer