



Access Management Control Policy and Procedure

1. SCHEDULE	2
2. INTRODUCTION	2
3. OBJECTIVE.....	2
4. SCOPE	2
5. DOCUMENTS	3
6. POLICY.....	3
7. PROCEDURE REGARDING ACCESS CONTROL.....	3
8. RIGHTS RESERVED BY THE ORGANISATION.....	4
9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS	4
10. POLICY AWARENESS AND UPDATE.....	4

Initial
SS
Initial

1. SCHEDULE

1.1	The Organisation	Insight Business Accounting
1.2	Registration number	20/07/2022
1.3	VAT registration number	4670306416
1.4	Physical address	
1.5	Email address	shane@insightba.co.za

2. INTRODUCTION

- 2.1. The organisation set out in item 1 of the Schedule (“**Organisation**”) is committed to, and is responsible for, ensuring the confidentiality, integrity and availability of the data and information stored on its systems.
- 2.2. Access management to information and information processing facilities are important aspects to consider in order to ensure the confidentiality, integrity and availability of the information of the Organisation.
- 2.3. When capitalised terms are used in the policy and procedure document (“**Policy**”), they are given the meanings ascribed to them either (i) in the Policy itself, or (ii) in the Protection of Personal Information Act 4 of 2013 (“**POPIA**”).
- 2.4. The provisions set out in this Policy ensure that the Organisation complies with its obligations under POPIA insofar as the security of information regulated and protected by POPIA is concerned.

3. OBJECTIVE

- 3.1. The objective of this Policy is to formalise the access control management process for the Organisation. When reference is made to “access control” in this Policy, it effectively means that access to the Organisation’s information and information processing facilities is limited through access control measures, such as usernames and passwords. Access control will be further enhanced by two factor authentication such as one-time pins where deemed necessary.
- 3.2. This Policy sets out the processes to be followed by the Organisation to:
 - 3.2.1. limit the access to information and information processing facilities;
 - 3.2.2. ensure authorised user access and to prevent unauthorised access to the Organisation’s systems and services;
 - 3.2.3. make employees, contractors, visitors, or other persons authorised to access and use the Organisation’s systems (“**Users**”) accountable for safeguarding their authentication information; and
 - 3.2.4. prevent unauthorised access to the Organisation’s systems and applications.
- 3.3. Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important and valuable asset of the Organisation which must be managed with care at all times. All information has a value to the Organisation. However, not all of this information has an equal value, or requires the same level of protection. The Organisation will determine in its sole discretion which information requires a greater degree of protection, depending on the:
 - 3.3.1. nature of the information in question; and
 - 3.3.2. the Organisation’s obligations in relation to such information, as regulated by the provisions of POPIA.
- 3.4. Access controls are put in place to protect information by:
 - 3.4.1. controlling who has the right to use different information resources; and
 - 3.4.2. guarding against unauthorised use of information.
- 3.5. Formal procedures must be followed to control how access to information is granted, changed and revoked.

4. SCOPE

- 4.1. This Policy is applied to all Users that use devices that relate to the Organisation’s business operations where data is processed.
- 4.2. This Policy covers all servers, workstations, network devices, operating systems, applications and other information assets of the Organisation.

Initial
SS Initial

5. DOCUMENTS

- 5.1. This Policy should be read in conjunction with the following related policies and procedures of the Organisation:
- 5.1.1. Information Security Policy;
 - 5.1.2. Acceptable Use Policy;
 - 5.1.3. Clean Desk and Clear Screen Policy; and
 - 5.1.4. Password Policy.

6. POLICY

- 6.1. The Organisation understands the importance of protecting its information and information processing facilities from unauthorised access.
- 6.2. Access to information and information processing facilities are provided by the information asset owners, as identified in the information asset register. The information asset register (“**IAR**”) is an inventory of information assets that include information, software and hardware of the Organisation. The IAR also allocates information asset owners (“**IAO/s**”) to the specific assets set out in the IAR. The IAO's have a responsibility to only provide access to people where their role requires them to have access to the specific information or information asset. In smaller organisations it could be the chief operating officer (“**CEO**”) that provides access to information assets.

7. PROCEDURE REGARDING ACCESS CONTROL

7.1. User Access Management

- 7.1.1. User registration will only occur where the User's role within or in relation to the Organisation requires them to have access to the information or information processing facilities in question.
- 7.1.2. The User must complete the system access request form in order to gain access to the information or information processing facilities in question.
- 7.1.3. The access request by the User will be considered by the IAO and will be approved or declined by the IAO based on the need to obtain access to the information in question.
- 7.1.4. The Organisation has designated some Users as “privileged Users”, and such Users will have access to root and administration functions. In such cases, the IAO may either decline or recommend access, but if access is recommended, the CEO of the Organisation will make the final decision as to whether access of the User in question is approved or declined.
- 7.1.5. Where the User activation has been approved in terms of this Policy, the relevant activation will be done within 48 (Forty-Eight) hours.

7.2. Passwords

- 7.2.1. Password protection standards must be maintained in line with the Organisation's password policy.

7.3. User Responsibilities

- 7.3.1. Users are responsible for ensuring that they gain access to the Organisation's information and information processing facilities only for work that is in line with their role within, or in relation to, the Organisation. Users must do the following at all times:
 - 7.3.1.1. protect their username and password and never share them with anyone else;
 - 7.3.1.2. ensure that they log out of any Organisation system when they are not using the system in question;
 - 7.3.1.3. comply with the Organisation's Acceptable Use policy, and all other policies and procedures of the Organisation that regulate the processing of information in terms of POPIA; and
 - 7.3.1.4. make sure that their screen is cleared and use the lock function when they are not at their desks.

7.4. User Deactivation

- 7.4.1. Deactivation of a User's access will take place in the following circumstances:
 - 7.4.1.1. when the User is an employee and has resigned from the Organisation;
 - 7.4.1.2. when the User has been authorised to assist on an Organisation project and the project in question has been finalised; and
 - 7.4.1.3. where the User is an employee has been suspended from the Organisation due to a forensic investigation.
- 7.4.2. Deactivation of access will take place as soon as possible, but not longer than 24 (Twenty-Four) hours from the time that a decision has been made by the Organisation to deactivate a User.

7.5. Access Reviews and Reconciliation

- 7.5.1. Periodic auditing of the accounts of Users will be performed by the IAO in order to:
 - 7.5.1.1. identify and revoke non-active, unused or non-authorised Users; or
 - 7.5.1.2. perform the reallocation or revocation of the privileges of Users.

Initial

SS

Initial

7.5.2. Access reviews will take place as often as necessary, but will occur at least once every month.

7.6. Privilege Management

7.6.1. Assignment of account privileges of Users is based on the principal of minimum privilege. Thus, an authorised User will be provided with access sufficient for their role at, or in relation to, the Organisation and the User in question will not be afforded any greater level of access than that strictly required.

7.6.2. If an authorised User's role within, or in relation to, the Organisation changes at any time, such User's access rights to information and / or information processing facilities may also change to reflect the circumstances and requirements of their new role.

7.7. Network Access Control

7.7.1. The use of modems on the Organisation-owned personal computers connected to the Organisation's network can seriously compromise the security of the network. Specific approval must be obtained from the Chief Executive Officer before connecting any equipment to the Organisation's network. Where sensitive and / or confidential information, including Special Personal Information, are in transit over the network, such information will be encrypted in transit.

7.8. Operating System Access Control

7.8.1. Access to the Organisation's operating systems is controlled by a secure login process. The access control management procedure defined in clause 7.1 must be applied. The login procedure must also be protected by:

7.8.1.1. not displaying any previous login information (for example, the username in question);

7.8.1.2. limiting the number of unsuccessful attempts and locking the account if exceeded;

7.8.1.3. the password characters being hidden by symbols; and

7.8.1.4. displaying a general warning notice that only authorised Users are allowed.

7.8.2. All access to the Organisation's operating systems will be via a unique login identity ("ID") that will be audited and can be traced back to each individual User. The login ID must and will not give any indication of the level of access that it provides the User in question to the system (such as administration rights, for example).

7.8.3. System administrators must have individual administrator accounts that will be logged and audited. The administrator account must not be used by individuals for normal day to day activities.

8. RIGHTS RESERVED BY THE ORGANISATION

The Organisation reserves the right to monitor, audit, screen, and preserve Organisation information as the Organisation deems necessary, in its sole discretion, in order to maintain compliance with this Policy and, by extension, all relevant provisions of POPIA. Any dissemination, unauthorised use or benefit from any Organisation information by a User in contravention of this Policy may result in disciplinary action being taken against such User by the Organisation. Furthermore, the use of any account or system in such a way that breaches any of the provisions of this Policy will be reported to the appropriate supervisor or manager within the Organisation, which may lead to further disciplinary action being taken.

9. ENFORCEMENT AND POTENTIAL DISCIPLINARY ACTIONS

Any violation of this Policy may result in disciplinary action being taken against the User in question. Such disciplinary action will be taken in accordance with the Organisation's applicable disciplinary code and may include the (i) termination of employment in relation to employees of the Organisation, or (ii) cancellation or termination of contractual relations in the case of other Users, such as contractors or consultants. Notwithstanding the foregoing, should any authorised User fail to adhere to this policy, the individual will be dealt with as prescribed by the Organisation's disciplinary code and procedures.

10. POLICY AWARENESS AND UPDATE

10.1. **Training and awareness:** The (i) requirement for, and (ii) a User's obligation in terms of, this Policy will be explained in detail in the Organisation's induction program, in the case of employees of the Organisation. Further training and additional awareness regarding the Policy will be offered from time to time by the Organisation. The Organisation will specifically make Users who are not employees of the Organisation aware of the Policy.

10.2. **Dissemination:** This Policy will be made available on the Organisation's network, intranet or similar portals.

10.3. **Review:** This Policy will be reviewed from time to time in order to ensure ongoing compliance with POPIA, but such revisions will take place at least annually. More frequent review may be required in response to (i) exceptional circumstances, (ii) organisational change, or (iii) relevant changes in legislation or guidance.

Initial
SS
Initial