HGDA Farmers Market, Erf 2226, Portion 27 Ellerton Farm, Ixopo,
Tel:039 834 2470/ 039 834 1362

ICT POLICY

Approved Date: 31/03/2023	**Effective Date:** 01/04/2023
Review Date: 06/01/2023	**Signature:**

TABLE OF CONTENTS

CONTENTS	PAGE
1. INTRODUCTION.	3
2. LEGISLATIVE FRAMEWORK.	3
3. OBJECTIVE OF THE POLICY.	4
4. AIM OF THE POLICY.	4
5. SCOPE.	4-5
6. BREACH OF POLICY.	5
7.ADMINISTRATION OF POLICY	5
8. DELAGATION OF RESPONSIBILITY.	6
9. PROCESS FOR NEW USER REGISTRATION.	6
10. PROCESS OF USER TERMINATION AND INACTIVE ACCOUNTS.	6-7
11. PROCESS OF RESETTING OF PASSWORDS.	7
12. PROCESS OF USER PERMISION/ROLE CHANGE IN USER ACCESS REQUEST.	7
13. GENERAL USER ACCESS RIGHTS ASSIGNEMENT	7-8
14. NETWORK USER ACCESS RIGHTS ASSIGNMENT	8
15. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT	8-9
16. APPLICATION USER ACCESS RIGHTS ASSIGNMENT	9
17. DATABASE USER ACCESS RIGHTS ASSIGNMENT	9
18. REVIEWING USER ACCESS AND PERMISSIONS	9-10

1. INTRODUCTION

Information security is becoming increasingly important to the Agency, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that ICT systems, data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction or loss data, as well as unauthorised disclosure or incorrect processing of data.

2. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well to leverage internationally recognised ICT standards.

The following legislation, amongst others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa Act, Act No.108 of 1996.
- Copyright Act, Act No. 98 of 1978.
- Electronic Communications and Transactions Act, Act No. 25 of 2002.
- Minimum Information Security Standards, as approved by Cabinet in 1996.
- Municipal Finance Management Act, Act No. 56 of 2003.
- Municipal Structures Act, Act No. 117 of 1998.
- Municipal systems Act, Act No.32 of 2000.
- National Archives and Record Service of South Africa Act, Act No. 43 of 1996.
- Promotion of Access to Information Act, Act No. 2 of 2000
- Protection of Personal Information Act, Act No. 4 of 2013.
- Regulation of interception of Communications Act, Act No. 70 of 2002.
- Treasury Regulations for departments, trading entities, constitutional institutions and public entities, Regulation 17 of 2005

The following internationally recognised ICT standards were leveraged in the development of this policy:

- Control Objectives for Information Technology (COBIT) 5, 2012;
- ISO 27002: 2013 Information technology- Security techniques- Code of practice for information security controls and;
- King Code of Governance Principles, 2009.

3. OBJECTIVE OF THE POLICY

The objective of the policy is to define the user access management control measures for the Agency's ICT systems, information and infrastructure where it would apply to both the Agency's users and Service Providers. This policy seeks to further ensure that it protects the privacy, security and confidentiality of the Agency's information.

The main objective of this policy is to provide the Agency with the best practice User Access Management controls and procedures to assist the Agency in securing their user access management procedure.

4. AIM OF THE POLICY

The aim of this policy is to ensure that the Agency conforms to standard user access management controls in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that risks associated to the management of user access are mitigated. This policy supports the Agency's Corporate Governance of ICT Policy. The policy also aims to outline the process for the creation, amending, resetting, deletion and deactivation of VIP, Sage Evolution, Caseware, Email, Teams, Active Directory, Network and other application, so as to increase system security and eliminate possible threats associated with security of user accounts.

5. SCOPE

The ICT User Access Management Policy has been developed to guide and assist agencies to be aligned with internationally recognised best practice User Access Management controls and procedures. This policy further recognizes that agencies are diverse and therefore adopts the approach of establishing principles and practises to support and sustain the effective control of user access management in the Agency. The policy applies to everyone in the agency, including its service providers/vendors. This policy is regarded as being crucial to the operation and security of ICT systems of the Agency. Agencies must develop their own User Access Management controls and procedures by adopting the principles and practices put forward in this policy.

The policy covers the following elements of User Access Management:

- New user registration
- Approval of request
- Resetting password
- Terminated user removal
- User permission/ role to Change request/change of access
- User access rights assignment for networks, operating systems, databases and applications
- Reviewing user access permissions and,
- Users and administrator's activity monitoring.

Aspects relating to ICT security and operating system security controls are contained in the ICT security and ICT Operating System Security Controls policies.

6. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the Agency and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but not limited to:

- Revocation of access to Agency systems and ICT services;
- Disciplinary action in accordance with the Agency policy;
- Civil or criminal penalties e.g. violations of the Copyright Act, Act No.98 of 1978; or.
- Punitive recourse against the service provider/vendors as stated in the service provider/ vendor's SLA with the Agency.

7. ADMINISTRATION OF POLICY

The delegated I T authority within the agency is responsible for maintaining this policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and recommended changes must be approved by Board.

8. DELAGATION OF RESPONSIBILITY

In accordance with the ICT Governance Policy, it is the responsibility of the *HGDA* CEO to determine the delegation of authority, personnel responsibilities and accountability to Management with regards to the Corporate Governance of ICT.

9. PROCESS FOR NEW USER REGISTRATION

a) A formalised user registration process must be implemented and followed in order to assign access rights.

b) All user access requests must be formally documented, along with the access requirements and approved by authorised personnel by making use of the user access request form.

c) User access requests must be obtained from HR on registration of a new employee. The form must be sent to the service provider/line manager for access requirements to be requested. Once the requirements have been requested and signed off by the departmental manager, the form must be sent to the ICT section for approval following which the activation of the employee based on the specified requirements will be completed.

d) User access must only be granted once approval and ICT user awareness has been obtained.

c) The username created by the ICT System Administrator will be in accordance with the approved naming convention policy. All users must be assigned unique user IDs in order to ensure accountability for actions performed, should shared accounts be required to fulfil a business function, this account must be approved and documented by the Internal Audit & Risk Management Committee.

10. PROCESS OF USER TERMINATION AND INACTIVE ACCOUNTS

a) A formalised user termination process must be implemented and followed in order to revoke access rights.

b) All user termination requests must be formally documented and approved by duly authorized personnel. Access must be disabled immediately, with accounts being removed after 6 months.

c) Terminated user requests must be obtained from HR on the termination of an employee. Form must be sent to the ICT section or approval and deactivation of employee based on specified requirements. ICT section must file a form for record keeping purposes.

11. PROCESS OF RESETTING OF PASSWORDS

a) Applicant will complete and sign the Password Reset Request Form.

b) The ICT System Administrator will then reset the user on the relevant system.

c) Once the applicant has been reset on the system, the System Administrator will then sign and file the form for audit purposes.

12. PROCESS OF USER PERMISION/ROLE CHANGE IN USER ACCESS REQUEST

a) A formalised user access management process must be implemented and followed in order to adjust user access rights.

b) All user access change requests must be formally documented along with their access requirements, and approved by dully authorised personnel.

c) Access must only be granted once approval has been obtained by the respective line manager.

d) User access change requests must be obtained form HR on change of an employee's role or permissions. The template for this type of request can be found attached to this policy in Annexure B. once the access requirements have been signed off, the form must then be sent to the ICT department for approval and adjustment of employee's access rights based on specified requirements. The form must then be filed by ICT for record keeping purposes.

e) User access rights that are no longer required must be removed immediately.

13. GENERAL USER ACCESS RIGHTS ASSIGNEMENT

a) Access rights include, but are not limited to: General office applications (E-mail, Microsoft Office, SharePoint, etc.), Department specific applications and/or databases, Network shares, administrative tasks, RASNPN Access; Wi-Fi and BYOD

b) Access must follow a "principle of least-privilege" approach, whereby all access is revoked by default and users are only allowed access based on their specific requirements.

c) The levels or degrees of access control to classified information must be restricted in terms of legislative prescripts.

d) Access rights must be assigned to a group/role. A user must then be assigned to that group. Access rights must not be assigned to individual users.

14. NETWORK USER ACCESS RIGHTS ASSIGNMENT

a) Access to the *Agency*'s network must be only allowed once a formal user registration process has been followed.

b) Access to Wi-Fi must only be provided to users who require access to the network throughout the Agency, to fulfil their business function.

c) Best practice states that RAS access must only be granted to employees who require remote access to a system in order to administer the environment.

d) Best practice states that VNP access must only be granted to employees who:

- Work remotely (Not at the office);
- Work overtime, or not within regular office hours.

e) it is the responsibility of the ICT Steering committee to ensure all users must be made aware of the security risks and obligations.

f) All reviews must be formally documented and signed off by the *ICT Administrator/Specialist/*. Documentation must be kept for record keeping purposes.

g) The *ICT Administrator/Specialist* must approve all hardware and software, owned by *HGDA* employees and service providers/vendors, if it is to be used for official purposes (BYOD).

h) The ICT team must ensure that all mobile devices must be protected with PIN.

15. OPERATING SYSTEM ACCESS RIGHTS ASSIGNMENT

a) Each system administrator must be given their own accounts within the administrator group. Should shared accounts be required to fulfil a business function,

then this account must be approved and documented by the Internal Audit & Risk Management Committee.

b) The default guest must be removed or renamed and disabled.

16. APPLICATION USER ACCESS RIGHTS ASSIGNMENT

a) Segregation of duties must be practised, in such a way that application administrators cannot perform general tasks on an application. This is to prevent any fraudulent activity from taking place.

b) Applications administrators must remain independent of the department utilising the application, with the exception of the ICT department.

17. DATABASE USER ACCESS RIGHTS ASSIGNMENT

a) The ICT Administrator/Specialist must limit full access to databases (e. g. sysadmin server role, db owner database role, etc.) to ICT staff who need this access. *HGDA* employees who use applications may not have these rights to the application's database.

b) The ICT Administrator/Specialist must ensure that *HGDA* employees who access databases directly (e.g. through ODBC) only have read access.

c) The ICT Steering Committee must approve all instances where *HGDA* employees have edit or execute access to databases.

d) The ICT Administrator/Specialist must review database rights and permissions on a quarterly basis (every 3 months). Excessive rights and permissions must be removed.

18. REVIEWING USER ACCESS AND PERMISSIONS

a) User access and user permissions must be reviewed every quarter (3 months) by the system ICT Administrator/Specialist.

b) Administrators' permission must be reviewed every quarter (3 months) by independent person/ HOD.

c) On a monthly basis, ICT checks a list of all terminated employees for that month to the ICT section This list must be used to ensure that all terminated users have had

their access revoked. Should one or more terminated users still have access to the environment, an investigation into the finding must be conducted.

a) On a monthly basis, the ICT Administrator/Specialist must review all users with administrative access to the environment and assess their rights for appropriateness. Should a user be found with excessive rights, a user access change request must be performed.

b) All reviews must be formally documented and signed off by the ICT Administrator/Specialist. Documentation must be kept for record keeping purposes.