HARRY GWALA DEVELOPMENT AGENCY (PTY) LTD

[REG. No: 2011/001221/07]

POLICY: ICT SECURITY CONTROLS

Administrative Responsibility:	Office of the Chief Executive Officer
Implementing Department / Departmental Unit	Corporate Services Department

POLICY DOCUMENT CONTROL

POLICY NUMBER	HGDA 011
CUSTODIAN	Corporate Services
STATUS	Final
VERSION (NO./YEAR)	V1 – 2024
APPROVED BY	
EFFECTIVE DATE	
REVISION DATE	
ROUTING	MANCO – 02 February 2024
	HGDA Policy Retreat- 13 February 2024
	Portfolio Committee/s- 06 March 2024
	HGDA Board- 19 March 2024
	HGDM Council- Not Applicable

Summary of Amendments:

Version	Author	Date	Revised Date
V1	Corporate Services Manager	02 February 2024	13 February 2024

TABLE OF CONTENTS

PREAMBLE

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

1. INTERPRETATION OF THE POLICY

1.1. Except to the extent to which the context may otherwise require, this Policy shall be construed in accordance with the following provisions of this sub-paragraph:

1.1.1. Any word or expression importing any gender shall include the other gender.

1.1.2. Words importing the singular also include the plural, and *vice versa*, where the context requires.

1.1.3. The following words shall have the meanings hereby assigned to them –

"CEO" shall mean the Chief Executive Officer of the Harry Gwala Development Agency (Pty) Ltd

"Executive and Senior Managers" Includes Executive and Non-Executive Directors of the Board

"HGDA" means the Harry Gwala Development Agency (Pty) Ltd, a company duly incorporated in terms of the laws of the Republic of South Africa with registration number: 2011/001221/07, in which the Harry Gwala District Municipality, as Parent Municipality, holds a sole interest. (referred to as "the Agency")

"HGDM" means the Harry Gwala District Municipality, a Category C Municipality established in terms of Section 155(1)(c) of the Constitution of the Republic of South Africa, 1996 and in terms of Section 12(1) of the Municipal Structures Act, 32 of 2000 (as amended) and its successors in title. Includes duly authorised officials of the Municipality who have been delegated any powers, functions, and duties necessary to give effect to this Policy and decide upon and administer the matters referred to herein.

2. PRIMARY LEGISLATIVE AND REGULATORY PROVISIONS

The policy was drafted bearing in mind the legislative conditions, as well as to leverage internationally recognised ICT standards. The following legislation, among others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa Act, 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
- National Archives Regulations and Guidance
- 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.

Including the following internationally recognised ICT standards:

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

3. AIM

The aim of this policy is to ensure that HGDA conforms to a standard set of security controls for information security 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 Information Security are mitigated. This policy supports the Agency's Corporate Governance of ICT Policy.

4. OBJECTIVES

The objective of the policy is to reduce the risk of harm that can be caused to HGDA's ICT systems, information and infrastructure. This policy also seeks to outline the acceptable use of ICT resources by Officials and 3rd party service providers, to ensure that the investment in modern technology is applied to the best advantage of the Agengy. This policy defines the collective controls to prevent Information Security related risk from hampering the achievement of the Agency's strategic goals and objectives.

5. SCOPE

This ICT Security Controls Policy has been developed to guide and assist Harry Gwala Development Agency to be aligned with internationally recognised best practice ICT Security Controls. This policy recognizes that municipal entities are diverse in nature, and therefore adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of information security. The policy applies to everyone in the Agency, including its 3rd party service providers and consultants.

This policy is regarded as being critical to the security of ICT systems of the Agency. The policy covers the following elements of information security:

- Ownership and classification of information
- Security incident management
- Physical security
- Application security
- Network security
- Database security
- Change control; and

- Software authorisation and licensing Aspects relating to user access, server security and data backup are covered in the ICT User Access Management, ICT Operating System Security Controls and the ICT Data Backup and Recovery 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 HGDA and evaluated on its level of severity. The appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy. Actions include, but are not limited to:

- Revocation of access to Municipal systems and ICT services.
- Disciplinary action in accordance with the Municipal policy, or
- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978) Punitive recourse against a service provider in terms of the contract

7. ADMINISTRATION OF THE POLICY

The relevant ICT Official as delegated by the CEO is responsible for maintaining the policy. The policy must be reviewed by the ICT Steering Committee on an annual basis and any changes approved by the Board.

8. PROTECTION OF PUBLIC RECORDS

8.1. The ICT Officials must work with the Records Departmental Unit to ensure that public records in electronic form are managed, protected and retained for as long as they are required.

8.2. Information security plays an important role in records management as a means to protect the integrity and confidentiality of public records. The ICT Official must_ensure that systems used for records management of electronic public records and e-mails are configured and managed as follows:

8.2.1. Systems must capture appropriate metadata (background and technical information about the data).

8.2.2. The systems must establish an audit trail to log all attempts to alter or edit electronic records and their metadata.

8.2.3. The system must protect the integrity of records until they have reached their approved retention. Integrity of records can be accomplished through procedures such as backup test restores, media testing, data migration controls and capturing the required audit trails.

8.2.4. Access controls must protect records against unauthorized access and tampering.

8.2.5. Systems must be free from viruses.

8.2.6. The system must ensure that electronic records, that have to be legally admissible in court and carry evidential weight, are protected to ensure that they are authentic, not altered or tampered with, auditable and produced in systems which utilise security measures to ensure their integrity.

8.2.7. Access to server rooms and storage areas for electronic records media must be restricted to ICT staff only with specific duties regarding the maintenance of the hardware, software and media.

8.2.8. Systems technical manuals and systems procedures manuals must be designed for each system.

8.2.9. A systems technical manual include information regarding the hardware, software and network elements that comprise the electronic record keeping system and how they interact. Details of all changes to a system must also be documented.

8.2.10. A system procedure manual include all procedures relating to the operation and use of the system, including input to, operation of and output from the system. A systems procedures manual should be updated when new releases force new procedures.

8.2.11. The ICT Official must ensure that the suitability of new system for records management is assessed during its design phase. The Records departmental unit must be involved during the design specification.

9. <u>PREESERVATION OF RECORDS TO PRESERVE LEGALITY</u>

9.1. The Electronic Communications and Transactions Act, Act. No. 25 of 2002, prescribes information security controls to preserve the evidential weight of electronic records and e-mails.

9.2. The evidential weight of electronic records and e-mails is a continuum, where the weight of the evidence increases with the number of information security controls applied. The following lists examples of such specific information security controls:

- Restrict access to records.
- Encrypt records.
- Store records on write once, read many times, media
- Apply records management principles
- Store records in a database management system
- Apply change control to the records management system
- Backup data
- Use digital certificates to confirm the identities of senders and receivers of messages

10. GENERAL CONTROL ENVIRONMENT

10.1. To ensure reliability of ICT services and to comply with legislation, all HGDA systems and infrastructure must be protected with physical and logical security measures to prevent unauthorised access to Agency data.

10.2. Physical and logical security is a layered approach that extends to user access, application security, physical security, database security, operating system security and network security.

10.3. Refer to the ICT User Access Management Policy and the ICT Operating System Security Controls Policy for the requirements relating to user access, applications and operating system security.

11. PHYSICAL SECURITY

11.1. The ICT Official must ensure that reasonable steps are taken to protect all ICT hardware from natural and man-made disasters to avoid loss and ensure reliable ICT service delivery. ICT hardware under control of the ICT function must be hosted in server rooms or lockable cabinets. Server rooms must be of solid construction and locked at all times.

11.2. The ICT department must retain an access control list for the server room. Access_must be reviewed quarterly by the ICT Official.

11.3. All server rooms must be equipped with air-conditioning, UPS and fire detection and suppression.

11.4. A maintenance schedule must be created and maintained for all ICT hardware under the control of the ICT department. Maintenance activities must be recorded in a maintenance register.

11.5. Server rooms must be kept clean to avoid damage to hardware and reduce the risk of fire.

11.6. Cabling must be neat and protected from damage and interference.

11.7. No ICT equipment may be removed from the server room or offices without authorisation from the ICT Official.

11.8. Officials of the Agency must be made aware of the acceptable use of ICT_hardware.

11.9. All hardware owned by the Agency must be returned by employees and service providers on termination of their contract.

11.10. All data and software on hardware must be erased prior to disposal or re-use by authorised ICT technicians only.

11.11. The data on any hardware that can be carried offsite will be the responsibility of the user.

11.12. ICT hardware and software must be standardised as far as possible to promote fast, reliable and cost-effective ICT service delivery to the Agency.

11.13. The off-site location, used to store backup data media, must be protected with the following physical security measures:

- Building of solid construction.
- Physical access control.
- Fire detection and suppression, and
- Environmental conditions adhere to vendor recommendations for storage of media

12. DATABASE SECURITY

All HGDA databases are managed by the relevant systems service providers. The ICT Official must ensure that the security and user management is included in current signed service level agreements.

13. NETWORK SECURITY

13.1. The ICT Official must ensure that the network structure and configuration including IP addresses, location, make and model of all hubs, switches, routers and firewalls are documented.

13.2. The ICT Official must ensure that a firewall between the Municipal network and other networks is implemented.

13.3. The ICT Official must ensure limited administrator access to the firewall and user accounts must have strong passwords of at least 8 characters with a combination of alpha-numeric characters and symbols. Remote firewall administration is only allowed using SSHv2 from the internal network.

13.4. The ICT Official must ensure that firewall upgrades and patches are checked and installed on a quarterly basis. An obsolete firewall (one that is not supported by the vendor any longer and / or has known security vulnerabilities) must be replaced.

13.5. The ICT Official must ensure that firewall rulesets and configuration settings are documented. The rulesets and configuration settings must be reviewed quarterly to ensure that it remains current (i.e. remove unused services) and that services that expose the Agency to security risk are reviewed continuously.

13.6. The ICT Official must ensure that the firewall is configured to block all incoming ports, unless the service is required to connect to a server on the internal network (e.g. port 80 and port 443 for web servers).When an incoming port is allowed, the service may only connect to the specific servers on the internal network. Internal IP addresses may not be visible outside of the internal network.

13.7. The ICT Steering Committee must approve all open incoming ports. The ICT Steering Committee must only approve requests that are absolutely necessary and with consideration of the associated security risks.

13.8. The system administrators must set the firewall to block intrusion attempts and to alert the ICT Official when additional action needs to be taken. The ICT Official must ensure that an incident is raised and that the root causes of the event is dealt with.

13.9. The ICT Official must ensure that infrastructure, user devices (e.g. personal computers) and servers facing externally are placed on separate network domains.

13.10. The ICT department must scan the entire network with security software on a monthly basis to detect security vulnerabilities. The scans must be performed from the Internet, as well as from the internal network.

13.11. Officials must remove all modems from the internal network to avoid intruders by passing the firewall.

13.12. System administrators must install personal firewalls on laptops and personal computers. Officials may not disable these firewalls. Officials must choose to deny a specific address when prompted by the personal firewall, unless approved by ICT.

13.13. The ICT department must ensure that all inactive network points are disabled.

14. EMAIL AND INTERNET

14.1. The ICT Official must ensure that all users are made aware of the safe and responsible use of e-mail and Internet services. E-mail and Internet should only be used for official use. Personal usage can be permitted if it does not interfere with job functions. E-mail and Internet may not be used for any illegal or offensive activities.

14.2. Officials and the ICT department may not use other Internet cloud services (e.g. Google drive, Gmail, Dropbox etc.) for official purposes unless approved by the ICT Steering Committee.

14.3. The official cloud storage through the Microsoft365 being one-drive must be used by officials and ICT department.

15. WIRELESS NETWORKS

15.1. System administrators must configure all wireless networks to the following standard:

- WPA2 security protocol or better.

- Password strength of at least 8 characters with a combination of alpha-numeric characters and symbols.

- The latest firmware must be installed, and

- Default system usernames and passwords must be removed.

15.2. Officials may not establish wireless networks attached to the internal network without the consent of the ICT Official. All wireless networks must adhere to the secure configuration standard.

16. MOBILE DEVICE AND OWN HARDWARE

16.1. No personal owned devices will be allowed on the internal network of HGDA.

16.2. Employees may connect with personal devices to Cellular or private networks to access e-mail, calendars, contacts and all other internet based solutions offered by HGDA.

17. TRANSFER OF INFORMATION

17.1. The ICT Official must ensure that official information may only be transmitted over secured external networks using encryption.

17.2. Officials may not use personal storage devices (e.g. USB memory sticks or portable hard drives) to store Municipal data. When required for official purposes, and the data is of a confidential nature, these devices must be encrypted by the ICT Official.

18. MONITORING

18.1. The CEO authorises the monitoring of Municipal systems by the ICT Official.

18.2. Municipal officials must be made aware that the network is being monitored to ensure network security, to track the performance of the network and systems, and to protect the network from viruses.

18.3. E-mail, Internet and other network service may be monitored.

19. SECURITY INCIDENT MANAGEMENT

19.1. All Municipal users must report actual or suspected security breaches or security weaknesses to the ICT Official or the delegated authority.

19.2. The ICT Official must ensure that all information regarding security incidents are recorded. The ICT Official must ensure that all the information relating to security incidents are reviewed on a quarterly basis to ensure that the root cause of the problems is addressed.

19.3. Investigations into security incidents may only be carried out by the ICT Official or a nominated person.

19.4. The Protection of Personal Information Act, Act No. 4 of 2013 prescribes that the Regular and the person affected by the breach must be notified in the event of a breach of personal information.

20. CHANGE CONTROL

20.1. All changes to Municipal applications and infrastructure must be managed in a controlled manner to ensure fast and reliable ICT service delivery to the Agency, without impacting the stability and integrity of the changed environment.

a. Corrections, enhancements and new capabilities for applications and infrastructure will follow a structured change control process.

b. An emergency change must follow a structured change control process.

c. Recurring change requests from users (e.g. user access requests, a password reset, an installation, move or change of hardware and software etc.) must follow the help-desk processes designed to deliver ICT services in the most effective way.

d. Recurring operational tasks are excluded from the structured change control process.

e. Only formal and feature controlled system updates must be allowed to be implemented.

20.2. The ICT Official must ensure that a formal change control process is established.

20.3. The ICT Official must ensure that a Portfolio of Evidence (POE) is created which lists all of the not approved change requests, active changes requests, cancelled change requests and completed change requests. The Portfolio of Evidence (POE) must be reviewed, and actions taken, to ensure that:

- Change requests receive sufficient attention.
- The change control process is being followed for all known changes, and
- Trends across change requests, that indicate systemic problems in the ICT environment, are identified and require more permanent fixes.

21. SOFTWARE AUTHORISATION AND LICENSING

21.1. The ICT Official must ensure that a record is retained of all licenses owned by the Agency.

21.2. The ICT Official must ensure that all ICT resources are scanned on an annual basis_to verify that only authorised software is installed.

21.3. The ICT Steering Committee must approve all software being used in the Agency._An approved software list must be maintained by the ICT Section and approved by_the ICT Steering Committee.

21.4. The ICT Steering Committee may only authorise software from known, reputable sources to reduce the likelihood of introducing errors or security risks into the environment.

21.5. Officials may not install or change the software on their computers.

22. COMPLIANCE AND ENFORCEMENT

22.1. This Policy will come into effect on the date of adoption by the Board of Directors of the Harry Gwala Development Agency (Pty) Ltd.

22.2. Violation of or non-compliance with this policy will give a just cause for disciplinary steps to be taken.

23. AMMENDMENT AND/OR ABOLITION OF THIS POLICY

This policy may be amended or repealed by the Board as it may deem necessary.

APPROVED BY:

NAME	SIGNATURE	DESIGNATION	DATE
MS ACR Whyte		Chief Executive Officer	25 April 2024

HARRY GWALA DEVELOPMENT AGENCY (PTY) LTD

[REG. No: 2011/001221/07]

INDUCTION POLICY

Administrative Responsibility:	Chief Executive Officer
Implementing Department / Departmental Unit	Corporate Services Department

INDUCTION POLICY

POLICY DOCUMENT CONTROL

POLICY NUMBER	HGDA 030
CUSTODIAN	Corporate Services Department
STATUS	Final
VERSION (NO./YEAR)	V1 – 2024
APPROVED BY	
EFFECTIVE DATE	
REVISION DATE	
ROUTING	MANCO – 02 February 2024
	HGDA Policy Retreat 11 April 2024
	Portfolio Committee/s- 18 April 2024
	HGDA Board- 24 April 2024
	HGDM Council Not Applicable

Summary of Amendments:

Version	Author	Date	Revised Date
V1	Corporate Services Manager	02 February 2024	11 April 2024

TABLE OF CONTENTS

PREAMBLE

1.1. To integrate new permanent/contract employees into the Agency.

1.2. To acquaint employees with details and requirements of the job.

1.3. To familiarize new employees with the physical environment of the Agency.

1.4. To introduce new permanent/contract employees to the organisational culture of the Agency i.e. norms and values of the Strategic goals, Agency legislation, Agency Policies as well as co-workers, activities, and tasks of the employees.

1.5. To familiarize employees with the applicable employment laws, policies, and collective agreements.

1.6. To introduce recreational and sports amenities and activities to employees.

1.7. To introduce employees to the strategic corporate governance tools like PMS, Budget, Agency structures, legislative environment, and the broader decision-making processes.

1.8. To deliver a comprehensive induction package to employees.

1.9. To create a culture of knowledge and value inculcation.

2. PRINCIPLES OF ORIENTATION AND INDUCTION

2.1. A positive and warm reception environment for a newly appointed employee shall be created.

2.2. An effective office familiarization environment shall be created for employees.

2.3. Direct support from the HR division shall be solicited for the achievement of this policy.

2.4. Direct assistance from the line Manager or Supervisor shall be rendered for ensuring seamless integration and absorption of new employees into the ranks of staff.

2.5. Direct and positive co-operation shall be expected from the co-workers or colleagues of the employee.

3. STAFF ORIENTATION

3.1. The newly appointed employee will report for duty at the HR offices.

3.2. The new employee will be introduced to the CEO and Departmental staff on the first day of work.

3.3. This the new employee will be introduced to the Corporate Services Department and the rest of the Agency and the Board.

3.4. After the introduction of the employee to all Departments including workstations, the employee will be taken through his/her letter of appointment or contract of employment line by line.

3.5. The new employee will provide all required documents to the HR division.

3.6. The new employee will complete and sign all forms required in terms of the applicable procedure.

3.7. The new employee will be free to ask any question for clarity. The new employee will be given a copy of the job description, conditions of service, grievance procedure, code of conduct and HR policies by HR.

3.8. After this exercise, the new employee will be handed over to the Manager for further orientation.

3.9. The Manager will take the employee through the Job description.

3.10. The employee will be given and shown all work resources and other facilities in the office where applicable.

3.11. Office supplies like stationery needed for execution of duties will be made available to the employee at his/her convenience.

3.12. The employees will be introduced to Health and Safety measures in the operational work environment.

3.13. The work expectations of the employee shall be discussed within five days of the employee having assumed duties.

3.14. The employee will formally be informed about his/her probation conditions.

3.15. The employee will be reasonably expected to comply with all work orders and safety requirements.

3.16. Induction workshops for all new employees will be held four times per year probably on a quarterly basis.

3.17. The workshop shall be organised according to the staff induction manual of the Agency.

3.18. The workshops will be conducted strictly according to a predetermined programme over one or two days.

3.19. An annual budget for the induction of employees on all strategic and crucial information pertaining to the Agency affairs.

3.20. The induction shall amongst things cover the following items:

3.20.1. Spheres of government in South Africa and their interrelations
3.20.2. Agency Organogram
3.20.3. HGDA Board
3.20.4. Agency Integrated Development Plan
3.20.5. Performance Management System
3.20.6. Budget

4. COMPLIANCE AND ENFORCEMENT

4.1. Violation of or non-compliance with this policy will give just cause for disciplinary steps to be taken.

4.2.

4.3. It will be the responsibility of all Managers, to enforce compliance with this policy.

5. COMMENCEMENT

5.1. This Policy will come into effect on the date of adoption by the Board of Directors of the Harry Gwala Development Agency (Pty) Ltd.

APPROVED BY:

NAME	SIGNATURE	DESIGNATION	DATE
MS ACR Whyte		Chief Executive Officer	25 Apnl 2024