EDEN

DISTRICT MUNICIPALITY
UMASIPALA WESITHILI
DISTRIKSMUNISIPALITEIT

ICT SECURITY CONTROLS POLICY

Council Approved: 05/12/2017

Council Resolution Nr: C.5

TABLE OF CONTENTS

Glossary of Abbreviations

Abbreviation	Definition
BYOD	Bring Your Own Device
COBIT	Control Objectives for Information and Related Technology
ICT	Information and Communication Technology
IP	Internet Protocol
ISO	International Organization for Standardisation
ODBC	Open Database Connectivity
PIN	Personal Identification Number
SSH	Secure Shell
UPS	Uninterrupted Power Supply
USB	Universal Serial Bus
WPA2	Wi-Fi Protected Access 2

Glossary of Terminologies

Terminology	Definition
Administrative rights	Access rights that allow a user to perform high level/administrative tasks on a device/application such as adding users, deleting log files, deleting users.
Biometric information	Personal information obtained through biometric measurements, such as finger prints, retina, DNA, etc.
Internal system processes	Processes that are performed by the system with no human intervention. Part of the internal working of the system or application.

1. INTRODUCTION

Information security is becoming increasingly important to the Municipality, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that the Municipality's ICT systems, data and infrastructure are protected from risks such as unauthorised access (see ICT User Access Management Policy for further detail), manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

2. LEGISLATIVE FRAMEWORK

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, 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
- 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.

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

- Western Cape Municipal Information and Communication Technology Governance Policy Framework, 2014
- 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. OBJECTIVE OF THE POLICY

The objective of the policy is to reduce the risk of harm that can be caused to the Municipality'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 Municipality.

This policy defines the collective controls to prevent Information Security related risk from hampering the achievement of the Municipality's strategic goals and objectives.

4. AIMS OF THE POLICY

The aim of this policy is to ensure that the Municipality 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 Municipality's Corporate Governance of ICT Policy.

5. SCOPE

This ICT Security Controls Policy has been developed to guide and assist municipalities to be aligned with internationally recognised best practice ICT Security Controls. This policy recognizes that municipalities 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 Municipality, including its 3rd party service providers and consultants.

This policy is regarded as being critical to the security of ICT systems of the Municipality.

Municipalities must develop their own Security controls and procedures by adopting the principles and practices presented in this policy.

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 the Municipality 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 POLICY

The ICT Manager or delegated authority 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 Council.

8. PROTECTION OF PUBLIC RECORDS

8.1 The ICT Manager must work with the Records Manager 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 Manager must ensure that systems used for records management of electronic public records and e-mails are configured and managed as follows:

(a) Systems must capture appropriate metadata (background and technical information about the data);

(b) The systems must establish an audit trail to log all attempts to alter or edit electronic records and their metadata;

(c) 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;

(d) Access controls must protect records against unauthorized access and tampering;

(e) Systems must be free from viruses;

(f) 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.

(g) 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.

(h) Systems technical manuals and systems procedures manuals must be designed for each system.

(i) 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.

(j) 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.

(k) The ICT Manager must ensure that the suitability of new system for records management is assessed during its design phase. The Records Manager must be involved during the design specification.

9. PROTECTION OF RECORDS TO PRESERVE LEGALITY

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 Municipal systems and infrastructure must be protected with physical and logical security measures to prevent unauthorised access to Municipal 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 Manager must take reasonable steps 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 Manager.

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 Manager.

11.8 Officials of the Municipality must be made aware of the acceptable use of ICT hardware.

11.9 All hardware owned by the Municipality 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 Any hardware that carry data that can be carried off-site (e.g. laptop computers, removable hard disks, flash drives etc.) must be protected with encryption.

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 Municipality.

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

12.1 The ICT Manager must limit full access to databases (e.g. sysadmin server role, db_owner database role, sa built-in login etc.) to ICT staff who need this access. Officials who use applications may not have these rights to the application's databases.

12.2 The ICT Manager must ensure that Officials who access databases directly (e.g. through ODBC) only have read access.

12.3 The ICT Steering Committee must approve all instances where Officials have edit or execute access to databases.

12.4 The ICT Manager must review database rights and permissions on a quarterly basis. Excessive rights and permissions must be removed.

13. NETWORK SECURITY

13.1 The ICT Manager must document the network structure and configuration including IP addresses, location, make and model of all hubs, switches, routers and firewalls.

13.2 The ICT Manager must implement a firewall between the Municipal network and other networks.

13.3 The ICT Manager must limit 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 Manager must check and install firewall upgrades and patches 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 Manager must document the firewall rulesets and configuration settings. 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 Municipality to security risk are reviewed continuously.

13.6 The ICT Manager must configure the firewall 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 Manager when additional action needs to be taken. The ICT Manager must raise an incident and deal with the root causes of the event.

13.9 The ICT Manager must place infrastructure, user devices (e.g. personal computers) and servers facing externally 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 and the ICT Manager must remove all modems from the internal network to avoid intruders bypassing 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. E-MAIL AND INTERNET

14.1 The ICT Manager must make all users 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 Internet cloud services (e.g. Google drive, Gmail, Dropbox etc.) for official purposes unless approved by the ICT Steering Committee.

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 Manager. All wireless networks must adhere to the secure configuration standard.

16. MOBILE DEVICES AND OWN HARDWARE (BYOD)

16.1 No personal owned devices will be allowed on the network of Eden District Municipality.

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 Eden District Municipality.

17. TRANSFER OF INFORMATION

17.1 The ICT Manager must ensure that official information may only be transmitted over 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 Manager.

18. MONITORING

18.1 The Municipal Manager authorises the monitoring of Municipal systems by the ICT Manager.

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 Manager or the delegated authority.

19.2 The ICT Manager must record all information regarding security incidents. The ICT Manager must review all the information relating to security incidents 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 Manager 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 Municipality, 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.

20.2 The ICT Manager must establish a formal change control process (Refer ICT Control Charter).

20.3 The ICT Manager must create a Portfolio of Evidence (POE) 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 Manager must retain a record of all licenses owned by the Municipality.

21.2 The ICT Manager must scan all ICT resources 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 Municipality. An approved software list must be maintained by the ICT Manager 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.