6.
ICT SYSTEMS SECURITY POLICY

2/B
C Johnson Systems Development Manager
16 September 2020 (028) 313 8190

1. Executive Summary

The purpose of this report is to recommend to Council the approval of the Information and Communication Technology (ICT) Systems Security Policy.

2. Service Delivery and Budget Implementation Plan - IGNITE

Directorate: Management Services
Department: Information and Communication Technology

3. Compliance with Strategic Priorities

Provision of democratic, accountable and ethical governance
Provision and maintenance of municipal services

4. Delegated Authority

None

5. Legal Requirements

Local Government: Municipal Systems Act, 2000 (Act 32 of 2000);
Local Government: Municipal Finance Management Act, 2003 (Act 56 of 2003) [MFMA]

6. Background/Discussion/Evaluation/Conclusion

Background

To comply with the provision of democratic, accountable and ethical governance it is important to have an ICT Data Backup and Recovery Policy for the Municipality. The policy was approved for adoption by the ICT Steering Committee on 12 November 2019.

Discussion

The policy outlines the Systems Security Policy within ICT covering all its core Systems, Servers and Applications within the Overstrand Municipality. Information security ensures that the Municipality's ICT systems, data and infrastructure are protected from risks related to unauthorised access, manipulation, destruction or loss of data, as well as unauthorised disclosure or incorrect processing of data.

7. Financial Implications

None

8. Staff Implications

None

9. Comments from other Departments, Divisions and Administrations

None

10. Annexures

Annexure A: ICT Systems Security Policy

RECOMMENDATION TO THE COUNCIL:

that the ICT Systems Security Policy **be approved**.

RESPONSIBLE OFFICIAL : C JOHNSON

TARGET DATE FOR IMPLEMENTATION : SEPTEMBER 2020

Annexure A
1/16

Overstrand Municipality

Information, Communication and Technology
ICT SYSTEMS SECURITY POLICY

Abstract
This document outlines the Systems Security Policy within ICT covering all its Systems, Workstations, Users and Applications within the Overstrand Municipality

2|16

TABLE OF CONTENTS

3|16

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
CIS	Centre for Internet Security
COBIT	Control Objectives for Information and Related Technology
HR	Human Resources
ID	Identifier
KB	Kilobytes
Mb	Megabytes
OS	Operating System
USB	Universal Serial Bus
VPN	Virtual Private Network

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.
Baseline	A set of agreed upon configuration settings defined for all devices with the environment. Baselines are often derived from best practice standards and customised for the environment. CIS standards are recommended by best practice.
Business case	A formal requirement in order for a specific business function to perform its required task.

4/16

Terminology	Definition
Clear Screen Policy	A clear screen policy directs all users to lock their computers when leaving their desk and to log off when leaving for an extended period of time. This ensures that the contents of the computer screen are protected from prying eyes and that the computer is protected from unauthorised use.
Devices	Consists of, but is not limited to: Desktops; Laptops; Printers; Switches; Routers; Member Servers; Database Servers; Application Servers; Firewalls; Intrusion Prevention Systems; etc.
End Point OS Firewall	Default software Firewall found on all windows operating systems.
Exception	A rule or configuration setting that does not adhere to the normal settings or rules defined within the environments baseline.
Malware	Software that is specifically designed and developed to disrupt or damage a device.
Virtual Private Network	A virtual private network (VPN) is a network that is constructed using public wires — usually the Internet — to connect remote users or regional offices to a company's private, internal network.

5|16

1. INTRODUCTION

Information security is crucial to the Municipality, driven in part by changes in both the regulatory environment and advances in technology. Information security ensures that the Municipality's ICT systems, data and infrastructure are protected from risks related to unauthorised access, 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

6|16

3. OBJECTIVE OF THE POLICY

The objective of the policy is to reduce and/or prevent the risk of damage that can be caused to the Municipality's ICT systems, information and infrastructure. This policy seeks to outline operating system security controls for Municipal employees to ensure that the controls are applied correctly to all devices and are in line with best practice.

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 AND PURPOSE OF THE POLICY

The aim of this policy is to ensure that the Municipality conforms to a standard set of security controls for System security in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service efficiency and that the risks associated to the management of Systems Security are mitigated. This policy supports the Municipality's Corporate Governance of ICT Policy.

The purpose of the Information Security Policy is to:

- Establish and maintain management and staff accountability for the protection of information resources.
- Promulgate the policy regarding the security of data and information technology resources.
- Define the minimum security standards for the protection of information resources.

5. SCOPE

This ICT System Security Controls Policy guides and assists the municipality to be aligned with internationally recognised best practice. This policy recognises 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 system security.

The policy applies to everyone in the Municipality, including its service providers/vendors. This policy is regarded as being critical to the successful operation and security of ICT systems of the Municipality. The Municipality will develop its own System Security controls and procedures by adopting the principles and practices put forward in this policy.

The policy covers the following elements of system security:

- Physical access and utilisation of Computers, Network, Workstations / Laptop, Access Points, Off-line media and Computer resources
- Network Access in terms of Access Management, Passwords, Utilisation, Authentication, Time restrictions and Transaction logs

7|16

- Email and the Internet
- Malware, Anti-Virus and End Point Firewalls
- Security updates, patches and hot fixes

Aspects relating to user access, server security and data backup are covered in the ICT User Access Management, and the ICT Data Backup and Recovery policies.

6. BREACH OF POLICY

Failure to comply with the rules and standards set out herein may 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 may 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 Systems Development Manager (ICT Manager) is responsible for maintaining the policy. The policy must be reviewed by the ICT Steering Committee when there is a change and any required changes approved by Council.

8. MANAGEMENT AND STAFF RESPONSIBILITIES

8.1 Although precautions are taken to safeguard all the systems and data in the Municipality, functional requirements make it impossible to prohibit all access to it. The owner or user of the data must therefore take the necessary precautions to ensure that the integrity, confidentiality and availability of all data, systems and equipment are not compromised.

8.2 To achieve this the following standards should be adhered to:

8.2.1 Each manager must see to it that all his or her employees take note of the Policy regarding the implementation and maintenance of data and system security.

8.2.2 Each manager is responsible for assuring an adequate level of security for all the data and resources that form part of his or her component or team.

8.2.3 An employee may only access and or use the information that he or she is authorised to access/use.

8.2.4 No information/images/data that may be offensive to any person, group or organisation may be stored on any of the official computer systems or transported across any official network or system.

8.2.5 As official messages sent via the e-mail system can have a major impact on the image of the Municipality, employees should see to it that such messages contain only authorised information and that it is in the format prescribed by the Correspondence and Publication Corporate Standards of the Municipality.

8.2.6 All the data and information on the Municipality's systems is the property of the Municipality. The Municipality retains the right to access any information (e-mail etc.) that is stored on or transported across any of the resources in use and to utilise it for whatever reason it deems necessary.

8.2.7 Employees must report any form of misuse of data, systems and equipment that comes to their attention to their respective managers or the IT management.

9. PHYSICAL ACCESS AND UTILISATION

9.1 COMPUTERS

9.1.1 In order to limit exposure to security risks, access to all computer related hardware and other resources must be controlled.

9.1.2 All the domain controllers and all other critical file servers must be kept in a secure (locked) environment and only authorised employees or supervised service representatives should be permitted to enter the room.

9.1.3 Console devices (connected to the servers or domain controllers) must be located in a secure location. Other devices such as external hard disks and tape drives must also be located in secure areas.

9.1.4 Workstations must be kept in a secure environment. Only authorised employees should be allowed to use them.

9.1.5 Printers used to print sensitive documents should be placed in a location not accessible to unauthorised personnel.

9.1.6 No sensitive information should be stored on computers located in an insecure environment.

9.1.7 Sensitive material/data should not be stored on any system without prior consultation with the Data Security Manager: IT.

9.2 NETWORK

9.2.1 Network devices such as routers, firewall, bridges, hubs and servers should be treated as computers and should be located in a secure environment.

9.2.2 Cables, although less of an immediate security exposure than other computer devices should be placed in either secure or not readily accessible locations.

9.2.3 Employees must not make any unauthorised changes to the physical layout and connection points of the network.

9|16

9.2.4 Users must not attach any device to the network without prior authorisation from the manager: IT.

9.3 WORKSTATIONS AND LAPTOPS

9.3.1 The workstations / laptop should not be generally available to non-employees or unauthorised users.

9.3.2 Sensitive output from printers should either be destroyed or placed in a secure location.

9.3.3 If employees work on sensitive information the visual access to the screens should be controlled.

9.3.4 No unauthorised changes may be made to the system configuration of workstations / laptop.

9.3.5 Employees are not allowed to insert/remove any devices into/from any official workstation / laptop without prior authorisation from the manager: IT. (E.g. Processors, memory modules, controller cards etc.)

9.3.6 Employees are not allowed to install any program on any official computer / workstation without the prior authorisation from the manager: IT.

9.3.7 No sensitive or classified information should be stored on workstations / laptop that are not located in a secure environment. Please note that data stored on workstations is not secured through the normal network security measures and the necessary precautions to safeguard such data should be taken.

9.4 MODEMS OR ACCESS POINTS

9.4.1 No modems and or related devices may be attached to and or used on any official telephone line, computer, workstation, laptop and or network device without the prior authorisation by the Manager: IT.

9.5 CLEAR SCREEN POLICY

9.5.1 All devices must be locked if unattended. All users must be informed of this requirement and how they can manually implement the clear screen policy requirement.

9.5.2 Where possible the ICT division should implement procedures or systems to automatically lock devices after 5 minutes of inactivity.

9.6 OFF-LINE MEDIA

9.6.1 Backup media (e.g. tapes, disks or CD's), where they are permitted, must be secured against unauthorised use and tampering.

9.7 UNINTERUPTABLE POWER SUPPLY PROTECTION

9.7.1 Critical systems (*servers, domain controllers, network equipment and workstations*) should be provided with an uninterrupted power supply (UPS).

9.7.2 The operation and functionality of UPS's must be tested regularly according to prescribed testing procedures.

9.8 Unauthorised access to the computer and network related resources are not allowed.

10. NETWORK ACCESS

10.1 ACCESS MANAGEMENT

10.1.1 Every account must have an owner, that is, a delegated person who is responsible for account usage and password changes.

10.1.2 A record should be maintained showing each user's profile. All modifications to user accounts should be recorded.

10.1.3 A new user may be registered on the system by submitting a written application with a list of services, programs and or data to which access is required. This application has to be recommended by the applicant's supervisor and approved by the Manager: IT. After approval has been granted, the network administrator/s will register the new user.

10.1.4 Temporary employees (for example students and external contractors/auditors) will be registered on the system with an account expiry date. (Maximum of 30 days)

10.1.5 Only one login at any time will be allowed per user. Exceptions will only be allowed with prior authorisation.

10.1.6 The system will not allow anybody to use the "GUEST". Where possible, the default guest account must be disabled or completely removed.

10.1.7 The system will not allow anybody to use "ADMINISTRATOR" logins unless specifically authorised by the manager: IT.

10.1.8 File and directory permissions or equivalent will be granted to specific users or groups. This will allow the user to use a file or directory in a particular way (i.e. only for reading).

(a) The network administrator will set the appropriate rights to assign to users or groups in each directory or file.

(b) File and directory permissions, or equivalent, automatically grant users the right to see to the root of a directory. Unless otherwise instructed subdirectories of this root directory are also accessible.

(c) Users can only use rights that they have been granted in permission assignments.

10.1.9 Accounts within a group should perform a similar function and should not possess vastly different privileges. For example an account used only for data entry should not share the same group as an account used for system management.

11|16

10.1.10 All groups must be periodically examined by the Manager: IT to verify each member's function and privileges. Where appropriate, privileges should be adjusted.

10.1.11 A user may only perform authorised activities on the system.

10.2 PASSWORDS

10.2.1 Passwords are required to gain access to all the domain controllers and file servers. No one will be allowed to access any system without a valid password.

10.2.2 Users will be forced to change passwords on the domains and servers. Exceptions to this rule must be authorised by the manager: IT.

10.2.3 Passwords will be encrypted by the system.

10.2.4 The minimum password length is set to five characters and must contain alpha as well numerical characters. Care should be taken that passwords are not easily guessed (E.g. names, month etc.)

10.2.5 The use of a screensaver password is recommended

10.2.6 General Password Attributes to be implemented by systems. Exceptions and specific configurations of systems should be defined in the User Access Management Procedure of the system

Attribute	Details
Minimum Password length	at least 6 characters
Expiration frequency	30 days
Password Complexity	Should be enabled in systems that have the capability
Password Composition	Letters and numbers. Where the system allows, special characters should be used
Password history	A password must be unique from passwords used in the past. Users should not be allowed to use any of their previous passwords
Invalid Account login attempts	Users will be allowed 3 login attempts before the account will be locked. This lock will remain in effect until a request is lodged to open by the network administrator.
Account Timeout	Where the system allows it, idle sessions should lock or disconnect from network resources after a specified period of inactivity (30 minutes).

10.2.7 Passwords that expire must be changed immediately.

12|16

10.3 UTILISATION

10.3.1 Users may not leave workstations unattended while still logged onto systems. If a user has been logged onto the File server and there has been no activity on that workstation for period of time, (for example) 10 minutes or more, the user must either log out or lock their workstation.

10.4 NETWORK SHARED DIRECTORIES OR DRIVE MAPPINGS

10.4.1 The facility to use shared directories must only be utilised for official purposes.

10.4.2 Private information may not be made available on the network through shared directories and/or resources such as CD-ROMs and/or files

10.4.3 Where possible, shares must be made available from a hierarchical structure, where the root shares must only be accessible by the ICT division and system administrators.

10.4.4 Where applicable and possible, shares must be named or renamed to identify its use, function or owner.

10.4.5 To prevent unauthorised access to information shared in through the use of shared directories, users should as best practise endeavour to secure their information with password controls.

10.5 AUTHENTICATION

10.5.1 Critical systems (HR and Financial) may require further authentication by means of user log-on (ID and password) to the applicable system. The specific system administrator must control this through the User Access Policy.

10.6 TIME RESTRICTION

10.6.1 All the users will be granted access from 07:00 to 18:00 from Monday to Friday.

10.6.2 Exceptions to the above will only be allowed if the function is shift based or needs access on a continual basis.

10.6.3 Remote access via Virtual Private Network (VPN) is exempted, where access is implicitly granted at all times. VPN access requires prior authorisation from the Manager: IT and director: Management Services.

10.7 BACKUP

10.7.1 It is the responsibility of the specific user to ensure that his/her data is backed up regularly. Files containing static information should be protected from unauthorised modification.

10.7.2 All day-to-day municipal data used as part of execution of a user's duty, must be stored on official File servers, so as to ensure that they are backed up.

10.7.3 Critical applications and or data files should be backed up and stored off-site, the details of which is covered in the backup policy.

13/16

11. E-MAIL AND INTERNET

11.1 EMAIL

11.1.1 The official e-mail system may not be misused for private purposes.

11.1.2 Electronic mail messages are not encrypted and the e-mail system can therefore not be used to transmit sensitive and/or classified material.

11.1.3 The Municipality retains the right to access and monitor any information sent via the e-mail system.

11.1.4 No private information/images/data that may be offensive to any person, group or organisation may be sent to any destination via the official e-mail system.

11.1.5 As messages sent via the official e-mail system can have a major impact on the image of the Municipality, employees must see to it that such messages contain only authorised information and that it is in the format prescribed by the Correspondence and Publication Corporate Standards of the Municipality.

11.1.6 Officials may not use Internet cloud storage or file sharing services (e.g. Google drive, Gmail, Dropbox, etc.) unless explicitly approved by the manager: IT.

11.2 INTERNET

11.2.1 The connection of any network to an external network (internet) must be protected by appropriate security measures (for example: firewall restrictions).

11.2.2 Outside of the work environment and functions permitted, Internet access is provided on a limited basis for research and communication purposes only. The procedures set out in the network access and authorisation must be followed to gain access to this service.

11.2.3 No access other than that that officially authorised, to the Internet via the Municipality's infrastructure (network, telephones etc.) will be allowed.

11.2.4 Employees are not allowed to download and execute software from the Internet without the appropriate authorisation by the Manager: IT.

11.2.5 No material that may be deemed offensive may be downloaded through the official systems and networks.

11.2.6 Due to bandwidth constraints and management no live streaming of video and or audio signals over the Internet will be allowed, unless it is explicit in the application and functions permitted (e.g. video conference) or without the appropriate authorisation by the Manager: IT.

12. MALWARE AND ANTI-VIRUS

12.1 All devices must be protected from malware and viruses.

12.2 Anti-virus applications must be kept up to date and where possible daily scans must automated on all devices, alternatively threat notifications must be sent to the user or ICT division.

12.3 Anti-virus application settings must be managed by the ICT team and must not be editable by users.

12.4 Where possible the Anti-virus must perform scans on all foreign devices, such as USB flash drives, on connection to a department device.

12.5 Users must be educated on how Malware and Viruses are deployed on devices and how they can prevent infection.

12.6 Users should take care not to distribute virus infected documents, programs and or data through the network or e-mail system.

12.7 All instances of virus infections should be reported to the manager: IT **immediately**.

13. [NETWORK AND] END POINT OS FIREWALL

13.1 [Network Firewall systems must be operational and enabled at all times].

13.2 [The event log of the Network Firewall systems must retain log activities for at least 6 months, with a preference for 12 months should the system be capable thereof. If the system does not allow it, this must be stipulated in the Network Firewall Service Operating Procedure.]

13.3 [That the firewall rules be checked on an annual basis, as well as checked for consistency on rule operations; adding, removing or amending.]

13.4 [A sample of the event log of the Network Firewall systems must be reviewed on an ad-hoc basis, to determine any anomalous activity.]

13.5 [The Network Firewall administrator activities must be reviewed on a quarterly basis, Service Operating Procedure].

13.6 End point Operating System firewalls, or third party Operating System firewalls, must be enabled at all times, exceptions must be noted to the ICT Administrators.

13.7 Notwithstanding any hardware or software Firewall at the perimeter of the network, Operating System software firewalls, prescribed in 13.1, must still be enabled.

13.8 Firewall settings must be managed by the ICT team and must not be editable by users.

14. SECURITY UPDATES, PATCHES AND HOT FIXES

15/16

14.1 Devices and applications must be kept updated on a regular basis to prevent vulnerabilities from being exploited.

14.2 Updates, patches and hot fixes must only be obtained from the vendor of the software in question.

14.3 Where applicable, System administrators must monitor the release of vendor patches.

14.4 Deployment of patches must follow a formalised release schedule where this is feasible, or via the authorised regular maintenance period.

14.5 Patches must be classified according to the risk of not deploying the patch within the environment. Critical patches must be released as a matter of urgency, while non-critical patches may be released during the next patch release schedule (14.4).

15. ANNEXURE A: REFERENCES

- *BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls.* (2013). Geneva: BSI Standards Limited.
- Constitution of the Republic of South Africa. (1996). Republic of South Africa.
- *Control Objectives for Information Technology (COBIT) 5.* (2012). Illinois: ISACA.
- Copyright Act No. 98. (1978). Republic of South Africa.
- King Code of Governance for South Africa. (2009). Institute of Directors in Southern Africa.
- Local Government: Municipal Finance Management Act, No. 53. (2003). Republic Of South Africa.
- Local Government: Municipal Structures Act 117. (1998). Republic of South Africa.
- Local Government: Municipal Systems Act 32. (2000). Republic of South Africa.
- Minumum Information Security Standards. (1996, December 4). Cabinet.
- Promotion of Access to Information Act 2. (2000). Republic of South Africa.
- Protection of Personal Information Act, No. 4. (2009). Republic of South Africa.
- Regulation of Interception of Communications and Provision of Communication-Related Information Act 70. (2002). Republic of South Africa.

16|16

POLICY SECTION:	ICT
CURRENT UPDATE:	12 November 2019
PREVIOUS REVIEW:	Initial Version
APPROVAL BY COUNCIL:	__ JUNE 2019