OVERBERG

DISTRICT MUNICIPALITY

ICT OPERATING SYSTEM SECURITY CONTROLS POLICY

Reviewed 2022/2023

TABLE OF CONTENTS

Glossary of Abbreviations

Abbreviation	Definition
CIS	Centre for Internet Security
COBIT	Control Objectives for Information and Related Technology
HR	Human Resources
ICT	Information and Communication Technology
ID	Identifier
ISO	International Organization for Standardisation
KB	Kilobytes
Mb	Megabytes
OS	Operating System
USB	Universal Serial Bus

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.
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.

Terminology	Definition
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.
Segregation of duties	The principle of dividing a task up based on varying levels of authority in order to prevent fraud and error by requiring more than one person to complete a task.

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 developed with the legislative environment in mind, as well as 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; and
- 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; and
- Center for Internet Security – Security Benchmarks, 2014.

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.

4. AIM OF THE POLICY

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

5. SCOPE

This ICT Operating System Security Controls Policy has been developed to guide and assist municipalities to be aligned with internationally recognised best practice. 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 operating system security.

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

The policy covers the following elements of operating system security:

- Baselining device security configuration;
- Password and account lockout policy;
- Audit and event logs;
- Clear screen policy;
- Network shares;
- Management of administrator accounts;
- Guest accounts;
- Malware and anti-virus;
- End point OS firewall;
- Security updates, patches and hot fixes; and
- Password reset procedures.

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. 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;
- Termination of Service Level Agreement and/or contract of service provider/s;
- Disciplinary action in accordance with the Municipal policy;
- Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978); or
- Punitive recourse against the service provider/vendor as stated in the service provider/vendor's SLA with the Municipality.

7. ADMINISTRATION OF POLICY

The ICT Management or delegated authority within the municipality 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 Council.

8. DELEGATION OF RESPONSIBILITY

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

9. BASELINING DEVICE SECURITY CONFIGURATION

9.1 A secure baseline, stating device security configuration settings, must be defined for all devices within the environment and approved by the ICT Steering Committee.

9.2 Should a business case exist that prevents specific baseline settings from being applied to a device, an exception must be documented and approved by the ICT Steering Committee.

9.3 Exceptions must be reviewed on an annual basis to ensure the relevance and acceptance of the risk within the environment by the ICT Steering Committee.

9.4 Version baselines must be reviewed on an annual basis to ensure relevance and applicability within the environment by the ICT Steering Committee.

10. PASSWORD AND ACCOUNT LOCKOUT POLICY

(a) Refer to Annexure B

11. AUDIT AND EVENT LOGS

11.1 All devices and applications must have auditing/logging enabled.

11.2 All accounts, at a minimum, must conform to the following audit configuration:

(a) Account logon events for failures;

(b) Account management for success and failures;

(c) Logon events for failures;

(d) Policy change for success and failures;

(e) Privilege use for success and failures; and

(f) System events for failures.

11.3 All accounts, at a minimum, must conform to the following event log configuration:

(a) Application event log maximum log size of 32 768 KB (32Mb);

(b) Security event log maximum log size of 81 920 KB (80Mb);

(c) System event log maximum log size of 32 768 KB (32Mb); and

(d) All event logs must be set to override as required.

11.4 Logs must be reviewed once a month for any suspicious and malicious activities by system administrators. A template for the reviewing of audit logs can be found in Appendix C of this Policy.

11.5 All reviews must be formally documented and signed off by the ICT Management. Documentation must be kept for record keeping purposes. Records of audit and event log reviews must be stored for a minimum of 10 years.

12. CLEAR SCREEN POLICY

12.1 All devices must be locked if unattended. It is the responsibility of the ICT Steering Committee that all users are educated in the need for a clear screen policy and how they can adhere to the policy.

12.2 All devices must automatically lock after 10 minutes of inactivity.

13. NETWORK SHARES

13.1 Network shares must be secured and access granted in line with the ICT User Access Management Policy.

13.2 Where possible, shares must be made available from a hierarchical structure, where the root shares (E:, F:, G:) must only be accessible by administrators.

13.3 Shares must be renamed to identify its use.

13.4 Access to shares must be reviewed on a quarterly basis (every 3 months) by system administrators and access revoked if found to be inappropriate.

14. MANAGEMENT OF ADMINISTRATOR ACCOUNTS

14.1 Each administrator must be given their own accounts within the administrator group. Should shared accounts be required to fulfil a business function, this account must then be approved and documented by the Risk Committee.

14.2 Application access must be controlled in similar fashion with segregation of duties being practiced. Application administrators must not be able to perform general user tasks on an application to prevent any fraudulent activities from taking place.

15. GUEST ACCOUNTS

15.1 Where possible, the default guest account must be removed or renamed and disabled.

16. MALWARE AND ANTI-VIRUS

16.1 All devices must be protected from malware and viruses.

16.2 Anti-virus applications must be kept up to date and weekly scans must be automated on all devices.

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

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

16.5 It is the responsibility of the ICT Steering Committee that all users must be educated on how Malware and Viruses are deployed on devices and how they can prevent infection.

17. END POINT OS FIREWALL

17.1 End point OS firewalls must be enabled at all times.

17.2 Although most environments have at least one hardware Firewall at the perimeter of their network, Operating System software firewalls must still be enabled.

17.3 All firewall rules must have a defined description.

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

17.5 Firewall rules and settings must be reviewed quarterly by system administrators.

17.6 All reviews must be formally documented and signed off by the ICT Management. Documentation must be kept for record keeping purposes. Records of reviews must be stored for a minimum of 10 years, as stated in the ICT Backup and Recovery Policy.

18. SECURITY UPDATES, PATCHES AND HOT FIXES

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

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

18.3 System administrators must monitor the release of vendor patches.

18.4 Updates, patches and hot fixes must be tested by system administrators within a separate environment, such as Development, Test or Quality Assurance, before being deployed in the Production environment.

18.5 The below diagram depicts the formal patch management process to be followed.

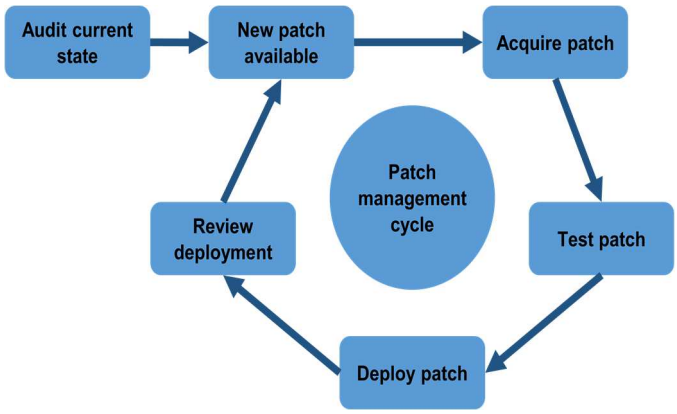

Figure 1: Patch management process

18.6 Deployment of patches must follow a formalised release schedule.

18.7 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.

19. PASSWORD RESET PROCEDURE

19.1 Should a user's password become compromised, a formal request must be sent to the System Administrator in order to reset the password.

19.2 The new temporary password must be communicated directly to the user, on validation of their identity.

19.3 The user must be forced to change their temporary password on first log on.

19.4 All documentation must be kept for record keeping purposes. Documentation must be kept for record keeping purposes. Records must be stored for a minimum of 10 years, as stated in the ICT Backup and Recovery Policy.

20. SECURITY AWARENESS AND TRAINING

20.1 As per point nr 6 on the implementation roadmap, management to provide updated security awareness training to users annually by means of information emails or training courses

20.2 IT should send through emails on how to identify phishing emails and the process to follow if such emails are received

20.3 Such processes be included in the induction course presented to new users.

21. CHANGE CONTROL AND NOTIFICATIONS

Management should ensure that Change notifications to the administrators' group be sent for all devices, operating systems, databases, and applications to which permissions are allowed. All changes made on administrator groups or accounts should be flagged and a notification or change log is sent to the relevant people.

22. MONITOR AND MANAGEMENT OF REMOTE USERS

22.1 A virtual private network (VPN) is a network that is constructed using the Internet to connect remote users or regional offices to a company's private, internal network. Remote access via Virtual Private Network (VPN) is exempted, where access is implicitly granted at all times. VPN access requires prior authorisation from ICT Management and the Director: Corporate Services.

22.2 Access to VPN is monitored on a quarterly basis through the change control log that is submitted to the ICT Steering Committee.

23. ANNEXURE D: REFERENCES

BS ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. (2013). Geneva: BSI Standards Limited.

Control Objectives for Information Technology (COBIT) 5. (2012). Illinois: ISACA.

24. ANNEXURE A: IMPLEMENTATION ROADMAP

No	Action	Month 1	Month 2	Month 3	Month 4 - 6
1	Review current operating system security controls against selected standard				
2	Train employees on policy procedures				
3	Produce baseline standard based on your specific environment				
4	Implement security controls				
5	Perform internal audit to determine conformance towards baseline				

25. ANNEXURE B: OPERATING SYSTEM SECURITY SETTINGS

Security Configuration	Setting
Password Policy - General User Accounts	
Minimum password length	8 characters
Maximum password age	30 days
Password history	5 passwords remembered
Password complexity	Enabled
Password Policy - Administrative/Super User Accounts	
Minimum password length	12 characters
Maximum password age	30 days
Password history	12 passwords remembered
Password complexity	Enabled
Account Lockout Policy - General User Accounts	
Account lockout duration	60 minutes
Account lockout threshold	5 attempts
Account lockout counter threshold	30 minutes
Account Lockout Policy - Administrative/Super User Accounts	
Account lockout duration	60 minutes
Account lockout threshold	5 attempts
Account lockout counter threshold	60 minutes
Audit Policy	
Account logon events	Failure
Account management	Success, Failure
Logon events	Failure
Policy change	Success, Failure
Privilege use	Success, Failure
System events	Failure
Event Logs	

Application Log: Maximum log size (KB)	32 768
Application Log: When maximum event log is reached	Overwrite events as needed
Security Log: Maximum log size (KB)	81 920
Security Log: When maximum event log is reached	Overwrite events as needed
System Log: Maximum log size (KB)	32 768
System Log: When maximum event log is reached	Overwrite events as needed
Additional Settings	
Screen saver	Enable
Screen saver: Wait	15 minutes
On resume, display logon screen	Enabled
Accounts: Rename administrator account	Not Administrator or admin
Accounts: Rename guest account	Not Guest
Accounts: Guest account status	Disabled
Windows Firewall: Firewall state (Domain)	Enabled (1)
Windows Firewall: Firewall state (Private)	Enabled (1)
Windows Firewall: Firewall state (Public)	Enabled (1)

26.ANNEXURE C: AUDIT/EVENT LOG REVIEW TEMPLATE

Reviewer:			
Month/Year	____/20___		
System/Application	**Day of review**	**Signature**	**Notes**
Active Directory			
Exchange			
Member Server 1			
Member Server 2			
Member Server 3			
Member Server 4			
Finance Application			
HR Application			
Comms Application			
Document Management System			

ICT Manager

Signature: _____

Date: ___/____/20__