POLICY 041/2016 RAADSBELEID

MUNICIPALITY DAWID KRUIPER MUNISIPALITEIT

SUBJECT/ONDERWERP: **IT OPERATING SYSTEM SECURITY CONTROLS POLICY**

REFERENCE/VERWYSING: **6.1.3.B**

RESOLUTION NR/BESLUIT NO: **17.9/11/2016 (CM)** DATE/DATUM: **25 November 2016**

PURPOSE: 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.

POLICY PHILOSOPHY AND PRINCIPLE

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.

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.

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.
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. SCOPE

This ICT Operating System Security Controls Policy 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.

2. 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.

3. SYSTEM ACCESS POLICY

3.1 All personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Dawid Kruiper Municipality facility, has access to the Dawid Kruiper Municipality network, or stores any Dawid Kruiper Municipality information must be assigned unique accounts that require passwords to allow access to the environment.

3.2 Users must protect password against unauthorized use thereof. Where a password was used to access any password protected system, program, information or facility it will be deemed to be done by the account holder.

3.3 Sharing logon usernames with or disclosing passwords to any third person(s).

3.4 Access to Dawid Kruiper Municipality networks via remote access is to be controlled by:

3.4.1 Using either a one-time password authentication or a public/private key system with a strong passphrase.

3.4.2 Only the Municipal Manager or Information Technology Manager may approve such access.

4. PASSWORD AND ACCOUNT LOCKOUT POLICY

4.1 User accounts must conform to the following password configuration:

4.1.1 **Minimum password length of 8 characters or more;**

4.1.2 **A combination of upper and lower case letters, numbers and special characters;**

4.1.3 **Maximum password age of 90 days or less; and**

4.1.4 **Password history of 4 passwords or more remembered.**

4.2 User accounts must conform to the following account lockout configurations:

4.2.1 **Account lockout duration of 60 minutes or more;**

4.2.2 **Account lockout threshold of 3 attempts or less;**

5. PASSWORD RESET PROCEDURE

5.1 Should a user's password become compromised, a formal request must be sent to the system administrator in order to reset the password.

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

5.3 All documentation must be kept for record keeping purposes. Documentation must be kept for record keeping purposes.

6. AUDIT AND EVENT LOGS

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

6.2 All accounts, at a minimum, must log sign on failure events.

6.3 Logs must be reviewed once a month for any suspicious and malicious activities by system administrators.

6.4 All reviews must be formally documented and signed off by the IT Manager. Documentation must be kept for record keeping purposes.

7. CLEAR SCREEN POLICY

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

7.2 All devices must automatically lock after 15 minutes of inactivity.

7.3 Users must log-off from systems or use screen savers with passwords in times of absence from a computer terminal to avoid improper and/or illegal use.

8. NETWORK SHARES

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

8.2 Shares must be renamed to identify its use.

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

9. MANAGEMENT OF ADMINISTRATOR ACCOUNTS

9.1 Each administrator must as far as permissible by the system be given their own accounts within the administrator group.

9.2 Application access must be controlled in similar fashion with segregation of duties being practiced. Application administrators must only be able to perform general user tasks on an application in accordance with their job description.

9.3 Where possible, the default administrator account must be renamed and a password must be randomly generated, sealed in an envelope and kept in a safe.

10. GUEST ACCOUNTS

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

11. MALWARE AND ANTI-VIRUS

11.1 All devices must be protected from malware and viruses.

11.2 Anti-virus applications must be kept up to date and daily scans must automate on all devices.

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

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

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

12. END POINT OS FIREWALL

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

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

12.3 All firewall rules must have a defined description.

12.4 Firewall settings must be managed by the IT team and must not be editable by users.

12.5 Firewall rules and settings must be reviewed every six months by system administrators.

12.6 All reviews must be formally documented and signed off by the IT Manager. Documentation must be kept for record keeping purposes.

13. SECURITY UPDATES, PATCHES AND HOT FIXES

13.1 Devices and applications must be kept updated in accordance with Council Patch Management policy.

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

13.3 System administrators must monitor the release of vendor patches.

ROLES

System Developers.
Administrator.
User.

RELATED POLICIES

Electronic Communication Policy, User account management Policy.

REPEALS

Any previous policy or procedure prior to this policy is hereby recalled.