POLICY 043/2016 RAADSBELEID

MUNICIPALITY DAWID KRUIPER MUNISIPALITEIT

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

REFERENCE/VERWYSING: **6.1.3.B**

RESOLUTION NR/BESLUIT NO: **17.11/11/2016 (CM)** DATE/DATUM: **25 November 2016**

PURPOSE: This policy defines the collective controls to prevent Information Security related risk from hampering the achievement of Council strategic goals and objectives.

POLICY PHILOSOPHY AND PRINCIPLE

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.

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
MISS	Minimum Information Security Standard
ODBC	Open Database Connectivity
PIN	Personal Identification Number
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 SCOPE

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 in the Municipality.

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 IT User Access Management, IT Operating System Security Controls and the IT Data Backup and Recovery policies.

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. The appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this policy.

3 PROTECTION OF CLASSIFIED INFORMATION

The Municipal Systems Act, Act No. 32 of 2000, Schedule 1: Code of Conduct for Councillors and Schedule 2: Code of Conduct for Municipal Staff Members require Councillors and Officials to employ a strict level of self-discipline in order to prevent communication of sensitive or classified information. Councillors and Officials may not disclose any privileged or confidential information to an unauthorised person.

All Municipal data must be classified in accordance with the Minimum Information Security Standards, as approved by Cabinet in 1996. Therefore all official matters requiring the application of security measures must be classified either as "Restricted" or "Confidential”. By default, Municipal data has been classified as Restricted.

Classification	Description
Restricted	Information that may be used to hamper Municipal activities.
Confidential	Information that may be used to harm the objectives and functions of the Municipality.

Table 1: Data classification in accordance with the MISS

Access to classified information is determined either by the level of security clearance, or if the information is required in the execution of their duties.

Officials, in conjunction with the IT Manager, must ensure that classified information receives adequate protection to prevent compromise.

Officials who generate sensitive information are responsible for determining the information classification levels. This responsibility includes the labeling of classified documents.

The Minimum Information Security Standards Chapter 6, Section 1 requires that a declaration of secrecy must be made on an official form during the appointment process for any government post.

4 PROTECTION OF PUBLIC RECORDS

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

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;

Access controls must protect records against unauthorized access and tampering;

Systems must be free from viruses;

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.

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

The IT Manager must ensure that the suitability of new system for records management are assessed during its design phase. The Records Manager must be involved during the design specification.

5 PROTECTION OF RECORDS TO PRESERVE LEGALITY

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.

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
- 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

6 GENERAL CONTROL ENVIRONMENT

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.

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.

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

7 PHYSICAL SECURITY

The IT users 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 IT function must be hosted in server rooms or lockable cabinets. Server rooms must be of solid construction and locked at all times.

The IT department must retain an access control list for the server room. Access must be reviewed quarterly by the IT Manager.

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

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

Server rooms must be kept clean to avoid damage to hardware and reduce the risk of fire.
Cabling must be neat and protected from damage and interference.

No ICT equipment may be removed from the server room or offices without prior authorisation from the IT Manager.

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

All hardware owned by the Municipality must be returned by employees and service providers when no longer needed or on termination of their contract.

All data and software on hardware must be erased prior to disposal or re-use.

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.

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

8 DATABASE SECURITY

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

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

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

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

9 NETWORK SECURITY

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

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

The IT Manager must limit administrator access to the firewall and user accounts must have strong passwords as set out by the IT security controls policy

The IT 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.

The IT Manager must document the firewall rule sets and configuration settings. The rule sets 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.

The IT 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.

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

The system administrators must set the firewall to block intrusion attempts and to alert the IT Manager when additional action needs to be taken. The IT Manager must raise an incident and deal with the root causes of the event.

The IT 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.

Officials and the IT Manager must remove all modems from the internal network to avoid intruders bypassing the firewall.

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 IT.

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

10 E-MAIL AND INTERNET

The IT 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.

E-mail and Internet may not be used for any illegal or offensive activities in accordance with the Electronic Communication Policy.

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

11 WIRELESS NETWORKS

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.

Access to Wi-Fi access points is controlled by user name and password in accordance with the User Access Management Policy

12 MOBILE DEVICES AND OWN HARDWARE (BYOD)

12.1.1 The IT Manager must approve all hardware and software, owned by Officials and service providers, which is to be used for official purposes.

12.1.2 The IT team must ensure that all mobile devices must be protected with a PIN.

13 MONITORING

13.1.1 The Municipal Manager authorises the monitoring of Municipal systems by the IT Manager.

13.1.2 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.

13.1.3 Monitoring of e-mail, Internet and other network service are monitored in accordance with the Electronic Communication Policy.

14 SECURITY INCIDENT MANAGEMENT

All Municipal users must report actual or suspected security breaches or security weaknesses to the IT Manager or the delegated authority.

The IT Manager must record all information regarding security incidents. The IT Manager must review all the information security incidents to ensure that the root cause of the problems is addressed.

Investigations into security incidents may only be carried out by the IT Manager or a nominated person.

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.

15 CHANGE CONTROL

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.

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

An emergency change must follow a structured change control process, but with the understanding that documentation must be completed afterwards. Emergency changes are only reserved for fixing errors in the production environment that cannot wait for more than 48 hours.

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.

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

The IT Manager must establish the formal change control process.

All other aspects of change control is done in accordance with councils policy of Change Management Policy

16 SOFTWARE AUTHORISATION AND LICENSING

The IT Manager must retain a record of all licenses owned by the Municipality.

The IT Manager must scan all ICT resources on an annual basis to verify that only authorised software is installed.

The IT Steering Committee must approve all software being used in the Municipality. An approved software list must be maintained by the IT Manager and approved by the IT Steering Committee.

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

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

ROLES

Municipal Manager.
Directors.
Heads of Sub-directorates.
All Municipal Officials.
IT Steering Committee.

RELATED POLICIES

Access to Information,2000 [Act 2 of 2000].
Administrative Justice, 2000 [Act 3of 2000];
Films and Publications, 1996 [Act 65of 1996]; and
Electronic Communications and Transactions, 2002 [Act 25 of 2002].
Electronic Communications Policy.
Dawid Kruiper municipality Filing system.
User access to internet and Email Policy.
IT Change Management Policy

REPEALS

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