POLICY 044/2016 RAADSBELEID

MUNICIPALITY DAWID KRUIPER MUNISIPALITEIT

SUBJECT/ONDERWERP: **IT USER ACCOUNT MANAGEMENT POLICY**

REFERENCE/VERWYSING: **6.1.3.B**

RESOLUTION NR/BESLUIT NO: **17.12/11/2016 (CM)** DATE/DATUM: **25 November 2016**

PURPOSE: The purpose is to establish the rules for the creation, monitoring, control and removal of user accounts used by employees to access information, systems and facilities.

PHILOSOPHY AND PRINCIPLES

Effective security controls in relation to the access to data is an essential component of effective risk management of the Council's data resources. By managing access control data and information is protected at all entry and exit points, both logical and physical. These measures ensure that only authorised users, as determined by the Council, have access to specific information, systems and facilities.

User accounts offer a way of managing access, providing user accountability and tracking their use of information, information systems and resources. User accounts can take various forms from a system login to an ID swipe card.

Therefore the application of access controls, the management of user accounts and the monitoring of their use plays an extremely important part in the overall security of information resources.

GUIDELINES

Definitions

Contract worker - is a person appointed for a fixed period to a post on the staff establishment or to perform specific tasks;

IT - the abbreviation for Information Technology;

Permanent employee - is a person employed with an open-ended contract to an approved post of the staff establishment;

System Administrator - is the person employed as a member of information technology (IT) to maintain computer systems in use at Dawid Kruiper Municipality;

1. This policy applies to all accounts (or any form of access that supports or requires User/Network ID) on any system that resides at any Council facility, has access to the Council network, or stores any Council information whether for corporate or departmental purposes.

2. All authorized users will be provided a unique User account for their sole use. All accounts must be uniquely identifiable by:

2.1 Assigned user name. These accounts grant a user access by entering the username and a password. The password must comply with the Password Policy;

2.2 Pin code. These accounts grant a user access by entering a pin code only. A pin code may only be assigned once for the lifetime of the system.

3. Accounts will be administered by a Designated Account Administrator

4. Permissible Account types

4.1 Individual Accounts.
This is the primary and preferred method of providing access to the Council's IT resources. Only permanent employees, contract workers or Councilors will be granted such an account and users are accountable for their actions and can be audited by the systems to which they have access rights.

4.2 Administration (Privileged) Accounts
IT Administrative / Operational full-time employees can be granted privileged accounts that permit elevated access rights for specific system or application for support and maintenance. Administration accounts (e.g., Windows domain and local administrator, etc.) shall not be used for daily administration.

4.3 Application-Specific Accounts
An application-specific account controls access to individual applications available on the network. Access rights and privileges are programmed/configured within the application. These accounts must never be used for individual access to the network itself and only granted to full-time System Administrators.

4.4 Guest Account
This account type is only for physical access to facilities by non-full-time employees. These accounts are for a limited period only and expire after 24 hours. For extended access a new account must be created.

5. Access rights and privileges;

5.1 Access to information systems and facilities will be governed by a formally defined authorisation process covering the creation, modification/maintenance, re-enabling and deletion of accounts;

5.2 Users will only be granted access to information and information systems and facilities on a "need-to-know" basis;

5.3 Accounts will only be authorized, created and maintained for users that need access to information, systems and facilities and will only be granted the minimum access and privileges required to perform their duties;

5.4 It is the Departmental Heads responsibility to request for access rights change when a user's roles, responsibilities and duties change

5.5 Departmental Heads must ensure that access to data or information must not be dependent on any one individual. The same privileges should be granted to more than one user in order to facilitate this function;

5.6 Access to information systems and facilities will be revoked for users who do not need access to perform their duties in order to ensure the confidentiality, integrity and availability of information to other users.

5.7 User accounts access rights will be reviewed once per year to ensure access and account privileges remain applicable to the user's job function/role or employment status. A record of the review must be maintained.

6. User account naming standard

6.1 Only one naming standard must apply within any system;

6.2 Each assigned account must uniquely identify the user;

6.3 User account names must not give any indication of the user's access rights;

6.4 Where systems allow for long user names the name consist of the users first name followed by his/her surname separated with a dot (firstname.surname).

6.5 Where systems cannot accommodate long usernames the name consists of either the users name followed by the first letter of his/her surname (firstnameS) or surname followed by the first letter of his/her name (surnameF).

6.6 If duplicates would be created the number 1or 2 or 3, etc is added at the end of the username to eliminate any duplicate.

6.7 System administration accounts:

6.7.1 These user accounts and passwords will be the responsibility of the technical owner of that system and;

6.7.2 Must adhere to the Council policies with the exception of where this is not technically possible;

6.8 Email addresses

This policy does not apply to email addresses. For this purpose refer to the Email address naming policy.

7. Account management

7.1 All accounts created or modified must have a documented request and the appropriate authorisation. Such request must be recommended by the Departmental Heads and authorized by the Director.

7.2 A record must be maintained of all authorisations including the access rights and privileges granted;

7.3 User accounts will not be created or activated until the authorisation process has been correctly completed. Users must not have access to information systems until all documentation is handed in to the System Administrator.

7.4 Generic or shared accounts will not be permitted.

7.5 Upon notification of termination, transfer, resignation, suspension or retirement from employment received from the relevant department the user account will be disabled / deactivated. Disabled accounts will be deleted after 120 days.

7.6 Each user account must be unique, only connected with the user to whom it was originally assigned. Reuse of user accounts is not permitted.

7.7 The designated account administrator or assistant will ensure that disabled User/Network IDs are not re-issued to another user.

7.8 All user accounts will, as a minimum, force the use of a password. All default passwords for accounts must be constructed in accordance with the Council's Password Policy.

8. Event logging monitoring and reporting
Auditing will be implemented on all information systems to track access and record events.

PROCEDURES

1. When a new employee is appointed, the Departmental Head must ensure that a system/facility access form (Annexure 1) granting the employee access rights and privileges to information, systems or facilities is completed and authorized by the Director to whom he/she reports;

2. When a contract worker is appointed, the Departmental Head must ensure that a system/facility access form (Annexure 1) granting the employee access rights and privileges to information, systems or facilities is completed and authorized by the Municipal Manager;

3. When an employee's duties change the Departmental Head must revise the employees user access rights and privileges and ensure that a change request is completed and duly authorized;

4. When an employee is transferred/promoted to a new position the Departmental Head must revise the employees user access rights and privileges and ensure that a change request is completed and duly authorized;

5. The system or facility administrator must create or modify a user account for the employee in accordance with approved access rights;

6. Persons for whom a user account is created signs for the account and thereby also accepts the terms and conditions set out in this policy;

ROLES
Staff in IT Department, Directors, Departmental Heads, users.

RELATED POLICIES
Electronic communications policy, Email Address Naming Policy, Password Policy.

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

DAWID KRUIPER MUNICIPALITY

System / Facility access form

This form authorizes the person mentioned below to access systems or facilities of Dawid Kruiper Municipality with the appropriate access rights and privileges to perform his/her duties.

Purpose of authority : [ ] new access [ ] modify/change existing access *(mark appropriate block with X)*

Existing access rights remain unchanged [yes] [no] (*If no, complete a removal of access rights form)*

_____ _____ _____

(Identity No) (Names) (Surname)

The person mentioned above is *(mark appropriate block with X)*

[ ] Full-time employee Employee no: _____

[ ] Councillor

[ ] Contract worker Employee no: _____

[ ] Guest

The abovementioned individual is hereby granted physical access to the following facility that requires an access account:

The abovementioned individual is hereby granted access to the following systems with corresponding user rights and privileges: (*Note: system access is NOT granted to GUEST accounts, if the space provided is insufficient additional pages may be added but must be signed by assignees)*

System name	Rights and privileges

Recommended : Departmental Head : Name : _____

Signature : _____ Date : _____

Approved : Director : Name : _____

Signature : _____ Date : _____

IT Use : Completed by : _____ Date : _____

DAWID KRUIPER MUNICIPALITY

Form for the removal of System / Facility access

The System Administrator of Dawid Kruiper Municipality is hereby requested to remove system or facility access of the following employee as indicated below

Employee name	
Employee number	

The abovementioned individual is hereby no longer granted access to the following systems with corresponding user rights and privileges: (*Note : if the space provided is insufficient additional pages may be added but must be signed by assignees)*

System name	Rights and privileges

Recommended : Departmental Head : Name : _____
Signature : _____ Date : _____

Approved : Director : Name : _____
Signature : _____ Date : _____

IT Use : Completed by : _____ Date : _____