

DR NDZ LOCAL MUNICIPALITY



IT USER ACCESS Policy

Core Business Areas	Corporate Services Department
Operational Area	IT Unit

Version	
Date	
File Name	IT User Access Policy
Business Owner	Manager
Date Approved	

Document Classification:

Confidential
KZN 436 Local Municipality 2015

1. INTRODUCTION

The main goal of an access control policy is to protect data by defining procedures, guidelines and practices for configuring and managing information security in the corporate environment. It is imperative that the policy defines the organisation's requirements for securing information assets.

2. POLICY AND BUSINESS REQUIREMENTS

Business requirements for access control must be defined and documented. Access control rules and rights for each user or group of users must be clearly stated in an access policy statement. Users and service providers must be given a clear statement of the business requirements to be met by access controls.

The policy will take account of the following:

- (i) User security requirements of individual business applications;
- (ii) Identification of all information related to the business applications;
- (iii) Policies for information dissemination and authorisation, e.g. the need to know principle and security levels and classification of information;
- (iv) Consistency between the access control and information classification policies of different systems and networks;
- (v) User access profiles for common categories of job; *and*
- (vi) Management of access rights in a distributed and networked environment which recognises all types of connections available.

3. USER ACCESS MANAGEMENT

Objective: To prevent unauthorised access to information systems.

Formal procedures must be in place to control the allocation of access rights to information systems and services. The procedures must cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention must be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

1.3.1.1 User registration

The formal user registration and de-registration procedure is the *System Request*, supplemented by user profile information on the prescribed form. The registration process includes:

- (a) Assignment of a unique *username* identifying the user and by which the user can be held accountable;
- (b) Assignment of a temporary, one-shot password for the specific purpose of allowing the user to create his/her own password;
- (c) Granting of appropriate access rights as specified by the User Access Request Form, either directly or by associating the user with the relevant user group(s); *and*
- (d) Maintaining formal records of all persons registered to use the facilities.

Where necessary, users are de-registered in similar fashion.

1.3.1.2 Privilege management

Multi-user systems that require protection against unauthorised access must have the allocation of privileges controlled through a formal authorisation process. The following must be taken into consideration:

- (a) the privilege associated with each system object, e.g. operating system, database management system and each application, and the categories of staff to which they need to be allocated must be identified;

- (b) privileges must be allocated to individuals on a need-to-use basis and on an event-by-event basis, *i.e.* the minimum requirement for their functional role and only when needed;
- (c) an authorisation process and a record of all privileges allocated must be maintained, and privileges must not be granted until the authorisation process is complete;
- (d) the development and use of system routines should be promoted to avoid the need to grant privileges to users.
- (e) Privileges such as *approvals* and *authorisations* should be subject to a password different from the normal sign on password.

1.3.1.3 User Password Management

Passwords are the means by which a user's identity is authenticated in order to allow access to an information system or service. The allocation of passwords must be controlled through a formal management process, encompassing the following:

- (a) Users must be required to sign (either on paper or electronically) an undertaking to keep personal passwords confidential and work group passwords (where these exist) solely within the members of the group;
- (b) Users must preferably be required to maintain their own passwords, *i.e.* they are initially provided with a temporary, "one-shot" password that only allows the user to create his/her own password and confers no application access rights; *and*
- (c) Temporary, "one-shot" passwords provided when users forget their passwords must only be supplied following positive identification of the user.
- (d) Passwords must be changed every month.

1.3.1.4 Review of user access rights

To maintain effective control over access to data and information services, business management must conduct regular formal reviews of users' access rights. The following are recommended:

- (a) users' access rights should be reviewed at regular intervals (a period of six months is recommended) and after any changes in the organisational structure;
- (b) authorisations for special privileged access rights (*e.g. approvals and authorisations*) should be reviewed more frequently (a period of three months is recommended); *and*
- (c) privilege allocations should be checked at random intervals to ensure that unauthorised privileges have not been obtained.

1.3.2 User Responsibilities

The co-operation of users is essential for effective security. Users must be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

1.3.2.1 Password Use

Users must be educated to follow good security practices in the selection and use of passwords.

Passwords provide a means of validating a user's identity and thus to establish access rights to information processing facilities or services. Users must be advised to:

- (a) keep passwords confidential;
- (b) avoid keeping a paper record of passwords, unless this can be stored securely;
- (c) change passwords whenever there is any indication of possible system or password compromise;
- (d) select quality passwords with a minimum length of six characters which are:
 - (i) easy to remember;
 - (ii) not based on anything somebody else could easily guess or obtain using person-related information, *e.g. names, telephone numbers, birth dates, etc.; and*

- (iii) free of consecutive identical characters or all-numeric or all-alphabetical groups.

Where ever possible, password criteria should be enforced by program code.

- (e) change passwords at regular intervals or based on the number of accesses (passwords conferring higher privileges should be changed more frequently than normal passwords) and avoid re-using or recycling old passwords. Where possible, this should be enforced by program code;
- (f) change temporary passwords at the first log-on. This should also be enforced by program code;
- (g) not include passwords in any automated log-on process, e.g. stored in a macro or function key; *and*
- (h) never share passwords.

1.3.2.2 Unattended user equipment

Users must ensure that unattended equipment has appropriate protection. Equipment stored in user areas, e.g. workstations or file servers, may require specific protection from unauthorised access when left unattended for an extended period. All users must be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

- (a) terminate active sessions when finished, unless they can be protected by an appropriate locking mechanism, e.g. a password protected screen saver; *and*
- (b) secure PCs or terminals from unauthorised use by a key lock or an equivalent control, e.g. password access, when not in use.

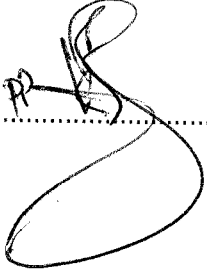
10. COUNCIL APPROVAL AND EFFECTIVE DATE

KZN 436 Local Municipality: IT User Access Policy

Approval of Policy by Council and Effective date: 06/06/2017

MUNICIPAL MANAGER

DATE


.....

19/06/2017
.....