WDRC-SWP-ICT001 Username & Password Conventions

Amendment Record

Please note that amendments have been made to the ICT Standard Work Practice (SWP) document/ form detailed below. This page will be re-issued every time amendments are made to controlled documents. Amended documents will have their revision status and issue date updated accordingly.

Revision Number	Clause/ Page/s	Description	Approved By	Issue Date
1.0		Issue	DFICT	13/03/2009
1.1	2 & 3	Amendment	DFICT	18/05/2009
1.2	3	Amendment	DFICT	06/08/2009
1.3	All	Western Downs Regional Council	DFICT	15/10/2009

PURPOSE

The purpose of this procedure is to provide instruction on the conventions used to provide usernames and the selection of appropriate passwords to enable access to Council computer systems and most computer applications.

SCOPE

The user account and password standard work practice covers the creation, use and ongoing maintenance of user accounts and passwords used for any computer system associated with the Western Downs Regional Council.

REFERENCES

FICT 2.2.1 Electronic Information & Communication Systems Policy.

RESPONSIBILITY

Director of Finance & Information and Communication Technology	– Authorise changes made to the Username and Password procedure.
ICT Manager	– Manage implementation of policy. – Ensure that system level passwords are managed appropriately.
IT Support Co-ordinator	– Apply the principles of the policy.

METHOD

Username

Each employee and elected representative of the Western Downs Regional Council will be issued with a Western Downs Regional Council network account username. All usernames will be in lower case text and will take the following form:

firstname.lastname

(with the effect that user *Jane Citizen* will have the username: "*jane.citizen"*)

Where staff share the same name, a single digit (base 10, 0-9) will be appended to the users "lastname" in order to differentiate the users. For example, should two users called *John Citizen* exist, their usernames would be issued as follows:

john.citizen

john.citizen1

The username and the associated password will be used for signing in to the network and to gain access to the majority of Western Downs Regional Council managed applications and resources.

Short term users (less than three weeks) may be issued with temporary network accounts with relevant functionality. This will be completed upon request from the relevant Director to the ICT (Information & Communication Technology) section.

Password

Western Downs Regional Council passwords are to be treated as sensitive, confidential information. The account owner must not disclose their password to any person including administrative assistants, secretaries, family, friends or support personnel. The account owner is solely responsible for all information access and all changes which are carried out while accessing a system through his/her account/password combination. Any attempt to encourage you to disclose your password should be reported to the ICT Section.

Passwords must not be inserted into email messages or other forms of electronic communication.

All system-level passwords must be stored in a secure place designated by the Information & Communication Technology Manager (ICTM) and changed every time a staff member who knows the password leaves the organisation or yearly whichever is the shortest.

All user-level passwords must be changed every 3 months (90 days).

Password history will be enabled so each user cannot re-use any of their last three (3) passwords.

All passwords must:

a. be a minimum of eight (8) characters in length;

b. contain at least two (2) letters with at least one case variance (english upper or lower case character (A-Z, a-z));

c. contain at least one (1) number (base 10 digit, 0-9), and;

d. must not contain all or any part of your name or username, e.g. if your username is "*jane.citizen*" your password cannot be, or should not contain, any of the words "*jane*" or "*citizen*". Similarly, do not use your initials in your password. Choose a password that cannot be readily associated with you e.g. do not use the name of your cat.

Computers will have system automatic lock-outs set to 10 minutes in alignment with audit recommendations. If there is no activity on your computer for more than 10 minutes your workstation will be locked and you will be required to "*ctrl-alt-del*" to log back on using your password.

Where an ICT facility, system or service is unable to support the minimum password complexity requirements detailed above, the strongest password that can be used within the restrictions of that particular facility, system or service shall be used.

The minimum password standards as detailed above must be automatically enforced by systems and applications, where possible.

The Western Downs Regional Council requires that critical software systems and/or data is protected by either passwords or encryption keys. Such encryption keys/passwords must be deposited in a secure place designated by the ICT Manager to ensure no loss of access occurs in the event of personnel that normally control the access codes being unavailable.

New User Password

When a new user is created the default password for the first logon will be:

Password01

When logging onto their profile for the first time the user will be required by the system to change their password to something that complies with this standard work practice prior to proceeding.

Emergency Password Reset

ICT staff may on occasion have the need to reset your password either to make changes to your user profile in the active directory, or to assist you when you have forgotten your password.

In all cases where a password has been set or reset by ICT staff, the default password will be:

Password01

When logging back onto their profile the user will be required by the system to change their password back to something that complies with this standard work practice prior to proceeding.

Emergency Access to Files/Systems

Where emergency access is required to specific files or resources on a users system, ICT staff will only obtain the information, or gain access to the system, on the written authorisation of the users Manager or Director. The information will be supplied directly to the users Manager or Director who shall then be responsible for the further distribution of the information.

ICT staff will notify the user of any emergency access granted to the users files/systems.

System Use

The possession of an account and a password that enables you to access, read or update information in Councils' computer systems does not imply or constitute the authority for you to do so. Such authority must be explicitly granted by your supervisor through the respective systems custodian.

It should be noted that the Western Downs Regional Council reserves the right to inspect all user accounts issued to staff and elected members by the Western Downs Regional Council or its agents, to investigate suspected security breaches, inappropriate or illegal activity, or unauthorised access.

The Western Downs Regional Council reserves the right to suspend access to a user account in cases of suspected security breaches, inappropriate or illegal activity, or unauthorised access.

In cases of suspected password compromise, the ICT section reserves the right to lock the users account or to change user account passwords without prior notice to the user in order to protect the integrity of the Councils' network.