

PASSWORD MANAGEMENT POLICY



<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-12, Rev1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 1 of 7	<u>Authorized by:</u> Managing Director


PASSWORD MANAGEMENT POLICY

APPLICABILITY

THIS MANUAL IS A COPY OF PASSWORD MANAGEMENT POLICY AS UTILISED BY THE SWAZILAND ELECTRICITY COMPANY. IT IS INTENDED FOR THE PURPOSE OF UTILISATION AND APPLICATION BY CURRENT ACTIVE SWAZILAND ELECTRICITY COMPANY PERSONNEL.

THIS DOCUMENT IS THE PROPERTY OF SWAZILAND ELECTRICITY COMPANY AND IS ISSUED TO THOSE EMPLOYEES REQUIRING IT IN THE EXECUTION OF THEIR DUTIES. ANY OTHER PERSON WHO FINDS THIS DOCUMENT MUST PLEASE SUBMIT IT TO THE SWAZILAND ELECTRICITY COMPANY FOR TRANSMISSION TO:

THE GENERAL MANAGER - FINANCE
SWAZILAND ELECTRICITY COMPANY
PO BOX 258,
MBABANE,
SWAZILAND

PASSWORD MANAGEMENT POLICY		
<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-12, Rev1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 2 of 7	<u>Authorized by:</u> Managing Director

1. Introduction

Swaziland Electricity Company (SEC) balances the need for employees to access systems and information with the need to control access for the purposes protecting information confidentiality, integrity, and availability. Account passwords are a mainstay of information security controls. This policy establishes management controls for granting, changing, and terminating access to automated information systems, controls that are essential to the security of Swaziland Electricity Company (SEC) information systems.

2. Coverage

All employees who use Swaziland Electricity Company (SEC) Information Resources must possess unique user account information, including passwords for access to various information systems. These procedures apply to accounts on all organizational systems: both in operation and in development.


3. Roles and Responsibilities

IT Manager

- 3.1 Provides management oversight of the process for administering passwords for Swaziland Electricity Company (SEC) systems
- 3.2 Publishes and maintains policy guidelines for the creation, safeguarding, and control of the passwords.

4. Systems Administrators and Network Technicians

- 4.1 Grants access and reviews access every year to determine continued need for access; and, if the need continues, re-approves through submission of System Access Request Form(s)
- 4.2 Prepares policy guidelines for the creation, safeguarding, and control of passwords

PASSWORD MANAGEMENT POLICY		
<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-12, Rev1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 3 of 7	<u>Authorized by:</u> Managing Director

- 5 Approves access of supervisor passwords and passwords for similar privileged accounts used on Swaziland Electricity Company (SEC)'s network

6 Head of Departments


- 6.1 Communicates to the users the system access and password requirements outlined in this policy.
- 6.2 Informs Swaziland Electricity Company (SEC)'s Security Officer when access is to be removed.
- 6.3 Immediately informs Swaziland Electricity Company (SEC)'s IT department if it is suspected that password has been compromised.

7. Network Administrator

- 7.1 Issues and manage passwords for systems and applications under their control in accordance with Swaziland Electricity Company (SEC)'s policy described below.
- 7.2 Issues passwords for privileged accounts to the primary system administrator and no more than one designated alternate system administrator; these passwords shall be changed at least every 30 days or when necessary due to employment termination, actual or suspected password compromise.

8. Users

- 8.1 Understand their responsibilities for safeguarding passwords.
- 8.2 Use Swaziland Electricity Company (SEC) data in accordance with job function and company policy.
- 8.3 Understand the consequences of their failure to adhere to statutes and policy governing information resources.


PASSWORD MANAGEMENT POLICY		
<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-12, Rev1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 4 of 7	<u>Authorized by:</u> Managing Director

- 8.4 Immediately notify supervisor if it is suspected that password has been compromised and then the IT department

9. Policy

9.1 Access Authorization Requirements

- 9.1.1 Access to Swaziland Electricity Company (SEC) shall be controlled and shall be based on an approved System Access Request Form for each of the systems.
- 9.1.2 Individuals shall be granted access only to those information systems necessary for the performance of their official duties; users must receive supervisor's and the IT Manager's approval prior to being granted access to Swaziland Electricity Company (SEC)'s information resources. This requirement includes contracted employees and all other non- Swaziland Electricity Company (SEC) personnel who have been granted access.
- 9.1.3 Passwords shall be used on all Swaziland Electricity Company (SEC) automated information systems to uniquely identify individual users.
- 9.1.4 Passwords shall not be shared with, used by, or disclosed to others; generic or group passwords shall not be used.
- 9.1.5 To preclude password guessing, an intruder lock-out feature shall suspend accounts after three invalid attempts to log on; manual action by a security system administrator is required to reactivate the ID.

PASSWORD MANAGEMENT POLICY		 Swaziland Electricity Company
<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-12, Rev1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 5 of 7	<u>Authorized by:</u> Managing Director


10. Password Parameters

10.1 All user and system passwords, even temporary passwords set for new user accounts, should meet the following characteristics:

- 10.1.1 Be at least six characters in length;
- 10.1.2 Consist of a mix of alpha, and at least one numeric, and special characters;
- 10.1.3 Not be dictionary words;
- 10.1.4 Not be portions of associated account names (e.g., user ID, log-in name);
- 10.1.5 Not be character strings (e.g., abc or 123);
- 10.1.6 Not be simple keyboard patterns;
- 10.1.7 In addition, users are required to select a new password immediately after their initial login. * Passwords must be changed at least every month* Previously used passwords may not be re-used.

11. Password and Account Security

- 11.1 Password accounts not used for six (6) months will be disabled and reviewed for possible deletion. Accounts disabled for 60 days will be deleted. Accounts for Swaziland Electricity Company (SEC) contractors shall terminate on the expiration date of their contract.
- 11.2 Lockout policy must be implemented for unsuccessful login attempts. As a good practice a maximum of three (3) login attempts should be allowed. The auto-lock policy for locked accounts must be released after three (3) login attempts.
- 11.3 Passwords for all users including administrator's accounts may be changed every three months.

PASSWORD MANAGEMENT POLICY		 Swaziland Electricity Company
<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-12, Rev1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 6 of 7	<u>Authorized by:</u> Managing Director

11.4 Administrative account passwords must be changed promptly upon departure of personnel (mandatory or voluntary) or suspected compromise of the password. User accounts will be disabled promptly upon departure of personnel (mandatory or voluntary). Users should immediately change their password if they suspect it has been compromised.

11.5 Vendor or service accounts will be removed from computer systems prior to deployment and new passwords are to be implemented on all systems immediately upon installation at Swaziland Electricity Company (SEC) facilities.

11.6 Passwords may not be embedded in automated programs, utilities, or applications, such as: autoexec.bat files, batch job files, terminal hot keys.


11.7 Passwords may be not visible on a screen, hardcopy printouts, or any other output device.

12. Enforcement

Unauthorized personnel are not allowed to see or obtain sensitive data. Gross negligence or willful disclosure of Swaziland Electricity Company (SEC) information can result in prosecution for misdemeanor or felony, resulting in fines, imprisonment, civil liability, and/or dismissal.

13. Supporting Documents

This Security Policy is supported by the following policy and laws:

PASSWORD MANAGEMENT POLICY		
<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-12, Rev1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 7 of 7	<u>Authorized by:</u> Managing Director

- Q-C-ER-A-02 Recognition Agreement SESMAWU
- Q-C-ER-A-01 Recognition Agreement NESMASA

14. Policy Support Contact

- IT Manager
- General Manager Finance

15. Amendment

This policy may be amended from time to time at the company's sole discretion, as and when it becomes necessary.