

COMPUTER VIRUS PROTECTION POLICY



<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-02, Rev1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 1 of 4	<u>Authorized by:</u> Managing Director


COMPUTER VIRUS PREVENTION POLICY

APPLICABILITY

THIS MANUAL IS A COPY OF COMPUTER VIRUS PREVENTION 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

COMPUTER VIRUS PROTECTION POLICY		
<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-02, Rev1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 2 of 4	<u>Authorized by:</u> Managing Director

1. Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

2. Purpose

The purpose of the Computer Virus Detection Policy is to describe the requirements for dealing with computer virus, worm and Trojan Horse prevention, detection and cleanup.


3. Coverage

The Swaziland Electricity Company (SEC) Computer Virus Detection Policy applies equally to all individuals that use any Swaziland Electricity Company (SEC) Information Resources.

4. Definitions

General Terms

- Email (or E-mail)
- Incident
- Server | Server
- Trojan Horse
- Virus
- Worm


COMPUTER VIRUS PROTECTION POLICY		
<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-02, Rev 1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 3 of 4	<u>Authorized by:</u> Managing Director

5. Roles and Functions

- IT Manager
- Network Administrator
- Information Services

6. Virus Detection Policy

- 6.1 All workstations whether connected to the Swaziland Electricity Company (SEC) network, or standalone, must use the Swaziland Electricity Company (SEC) IS approved virus protection software and configuration.
- 6.2 The virus protection software must not be disabled or bypassed.
- 6.3 Users are not allowed to install their own or non SEC IT approved antivirus software.
- 6.4 The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- 6.5 The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- 6.6 Each file server attached to the Swaziland Electricity Company (SEC) network must utilize Swaziland Electricity Company (SEC) IS approved virus protection software and setup to detect and clean viruses that may infect file shares.
- 6.7 Each Email gateway must utilize Swaziland Electricity Company (SEC) IS approved email virus protection software and must adhere to the IS rules for the setup and use of this software.
- 6.8 Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the IT Department Help Desk.

COMPUTER VIRUS PROTECTION POLICY		 Swaziland Electricity Company
<u>System:</u> Quality Management System	<u>Reference No, Revision No:</u> Q-F-IT-PO-02, Rev1	<u>Originated by:</u> IT Manager
<u>Revision Date:</u> 11.06. 2013	<u>Page No:</u> Page 4 of 4	<u>Authorized by:</u> Managing Director

6.9 Every desktop, laptop, server must have its USB port disabled at all times. In the event there is an evident need to open the USB port, such a request must be made in writing to the IT Manager.

7. Enforcement

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Swaziland Electricity Company (SEC) Information Resources access privileges, civil, and criminal prosecution.

8. Supporting Documents

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

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

9. Policy Support Contact

- IT Manager
- General Manager Finance

10. Amendment

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