I.T. BUSINESS RESUMPTION POLICY

APPLICABILITY

THIS MANUAL IS A COPY OF I.T. BUSINESS RESUMPTION 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

1.   Introduction

The Company has invested heavily on Information Technology assets encompassing physical (hardware), logical (software / data) and skills (personnel). The Operations of the Company have become reliant on the availability and integrity of these assets. Disruptions to the functionality of these assets will have a negative impact on the operations of the Company.

This policy defines the strategies and procedures in place to resume the business of the Company in case of disruptions to the operations of these assets. Disruptions will vary in scale of damage and, therefore, larger scale failures will require more resources and time to restore business continuity.

2.   Mission-Critical Operations – Impact Analysis

These operations are the core of the Information Technology services of the Company and their continued disruption will highly impact on the overall Company Operations as listed below in their impact order. The impact is based on the effects on revenue and reputation of the Company which must be minimized. The following impact ranges are used and it must be understood that this is under a disaster situation:

- **High impact** – These are operations which will be resuscitated within 7 days and data losses minimized to 1 day.

- **Moderate impact** – These operations will be resuscitated within 21 days.

- **Low impact** – These operations will be resuscitated as part of the return to normal operations. Their period will vary depending on the availability of resources (finances, staff, accommodation, etc.) which will be determined by the type of disaster.

The following are the I.T. operations and their Impact ratings:

2.1 High Impact

- **ELLIPSE** (MIS) – Materials, Suppliers, Finance, Assets / Equipment

- **Main Billing** – Electricity Statements Generation, Debtors Maintenance

- **Revenue Collection** – Receipting sub-systems (stand alones)

- **Eclipse/EVG** – Pre-paid electricity revenue collection, Customer maintenance

2.2 Moderate Impact

- ACCSYS – Staff Payroll maintenance

- NOVELL – Network Services

- Central Networking and UPS support (LAN equipment)

- Remote Site Networking and UPS support (WAN equipment)

- High Speed Printer(s) – at least one

2.3 Low Impact

- Anti-Viral and Firewall Protection

- GIS – Survey and drawing office data maintenance

- SYSPRO – Bank Reconciliation module

- COGNOS – Billing Reporting subsystem

- Business Objects – ELLIPSE Reporting subsystem

- MAIL - Internet / E-mailing

- RADICAL – IT help desk maintenance

- Decollation, Statements Mailing, etc.

3. Data backups

The following table shows the data backup strategies in place to secure critical information off the active systems. The frequency varies according to the volatility of the system data.

System	Daily/Type	Weekly/Type	Monthly/ Type	Configuration
ELLIPSE H/W– HP9000/800 O/S- B.11.45 U Oracle11i 9.2.0.7.0 Ellipse v5.2.3.7	H/O IT Area / Full	H/O Revenue / Full	Swazi Plaza / Full	Ignite Tape(IT)
BILLING – Credit H/W- HP9000/871 O/S- B.11.11 U Adabas- 3.3.3.01 Natural- 6.1.1 P1	H/O IT Area / Full	H/O Revenue / Full	Swazi Plaza / Full	Ignite Tape(IT)
GIS O/S-Windows2003	H/O IT Area / Full	N/A	N/A	N/A
ACCSYS O/S-Windows2003	N/A	H/O IT Area / Full	Personnel(PM) / Full	
SYSPRO/COGNOS O/S- Windows2003	N/A	H/O IT Area / Full	N/A	
NOVELL O/S – Netware 5.1	H/O IT Area / Full	N/A	N/A	Tape (IT)
MAIL/INTERNET O/S–Linux Redhat4	N/A	N/A	N/A	Tape (IT)

RADICAL O/S- Windows2003	N/A	H/O IT Area / Full	N/A	
/ACTARIS O/S- Windows XP	H/O IT Area / Full	H/O Revenue / Full	N/A	Install CD (IT)
ECLIPSE/EVG O/S –Linux and Win 2003	Every 5 min Replication between Servers	Every 5 min Replication between Servers	Every 5 min Replication between Servers	Failover to the Failover Servers or DR Server in case of a Disaster.

The Revenue Collection (Receipting) System is a stand-alone system and hence very low risk. Backups are not performed on it, but a configuration system copy exists within the I.T. Department. Alternatively, this may be copied from other stations and setup for new installations.

4.   **Remote Hot Site Security Backup**

Currently there is a Disaster Recovery Site in Matsapha Training Center with a new one being constructed at Manzini Regional Office. In the meantime, it is being used as remote data backup facility mainly for the High Impact systems i.e. Prepaid System and the Billing System. The hot site will be developed with time until all the critical systems can be accessed from all sites should the need arise.

5.   **Maintenance Contracts**

Agreements are in place for the maintenance of the core systems equipment and software. These, however, cover the replacements of parts that have broken down and updates of software. They do not include complete replacements. These may be called upon for assistance for re-configurations in case of a disaster at an additional cost.

5.1 HP Contracts

These are agreements for the maintenance of the hardware and operating system for the ELLIPSE and BILLING production systems. In accordance with HP policy, some components are removed from agreements as their support periods expire. These are maintained on a materials and labour basis.

5.2 Ventyx Contracts

These are agreements for the installation and maintenance of the Application Systems for the Management Information Systems (Ellipse). They include the Database Management System (ORACLE) which were taken with Oracle through MINCOM but this may change and an arrangement made with ORACLE SA or their partners.

5.3 SOFTWARE AG Contracts

These are for maintenance of the Database Management System (ADABAS/NATURAL) which runs the Application for the MAIN BILLING System. The application itself is fully in-house maintained.

5.4 Other Contracts

There are agreements for auxiliary systems like Payroll, Novell, Impact, etc.

6. INSURANCES

An inventory of the critical assets is compiled/revised every year and submitted to Finance for insurance purposes. This includes the critical operations equipment.

7. PROTECTION / SECURITY

As a means of mitigation against daily risks, the following are in place for additional protection/security of the I.T. assets:

- Fire Detection / Protection Devices inside the computer room
- Temperature control inside the computer room
- False flooring inside the computer room
- Security-controlled entrance into the computer room

8. BUSINESS RESUMPTION

Recovery procedures for disruptions will also vary depending on the extent and the affected areas of operation. I.T. Manager is responsible for the co-ordination and execution of the procedures in all categories. The following identified categories are in their scale/extent order (Lowest to Highest):

Disruption Category	Possible Cause	Resumption Procedure	Responsibility
1 - Loss of Data	-Component breakdown -Transient malfunctions	- Trouble Shooting - Equipment Replacements - Data Restores from backups	System. Administrators Network Administrator IT . Manager
2 - Loss of Network Equipment	-Component Breakdowns -Power Surges -Lightning Strikes	-Equipment Replacements -Configurations where necessary	Net. Administrator

System: Quality Management System	Reference No, Revision No; Q-F-IT-PO-08, Rev1	Originated by: IT Manager
Revision Date: 07.06. 2013	Page No: Page 8 of 11	Authorized by: Managing Director

3 - Loss of Server(s)	-Component Breakdowns -Vandalism	-Equipment Replacements -Configurations -Data Restores	GM Finance I.T. Manager I.T. Staff
4 – Loss of any combination of the above 3 items	- Flooding - Fire - Natural Causes (like earthquakes)	- Equipment Replacements - Configurations - Data Restores	GM Finance I.T. Manager I.T. Staff
5 - Loss of Computer Room	-Fire or Flooding -Natural Disasters -Terrorist Acts	** See Disaster Recoveries	
6 – Loss of I.T. Department	-Fire or Flooding -Natural Disasters -Terrorist Activities	** See Disaster Recoveries	

Those situations where the normal Business Resumption above cannot restore the normal service within the acceptable time. These are in the following categories:

9. DISASTER RECOVERIES

9.1 Category A

Under this category, the critical Server(s) would be damaged in a manner that it requires a complete replacement, which would take weeks to process. This assumes the computer room and network infrastructure are usable and operational.

The recovery method to be performed is:

- Move the corresponding Server from the Disaster Recovery site to computer room (I.T. Manager)

- Reconfigure its network connectivity similar to the production Server(Ops/Net Administrator)

- Systems Testing for Data recoveries as required(Bus Systems Manager)

- Connect to network and normal access continues(Ops/Net Administrator)

- Replacement Server will be configured as backup and moved to Hot site(I.T. Manager)

9.2 Category B

This category would render the Network infrastructure unusable but the computer room undamaged and usable. If Server(s) were also affected to the same extent, hot site Server(s) would be re-located as in Category A above. The following recovery steps would be followed:

- At least one Hub/Switch is acquired, configured and connected (Net Administrator)

- Close proximity cabling to available space laid (Ops/Net Administrator)

- Workstations(PCs) relocated from Head Office users and connected (Ops/Net Administrator)

- System(s) testing for data recoveries as required (Bus Systems Manager)

- Selection of users limited users to access the system(s) (GMs Finance/Customer Services)

- Transport/Accommodation arrangements put in place for selected users (GMs Finance/Customer Service/Human Resources)

- The number of users would depend on the available of space and Hub capacity but not less than 16 per system.

9.3 Category C

This category would render the network infrastructure, Server(s) and Computer room unusable. The first step would be to re-configure the backup Server(s) as the production servers at the hot site. The rest of the steps are the same as Category B, except the location is at the hot site instead of Head Office.

10. CONTACTS INFORMATION

The following contact information may be used to assist in the business resumption / disaster recovery processes:

Dealer	Assistance	Contact	Telephone	Add. Info.
Hewlett Packard S.A.	HP Hardware and Operating System (UNIX)	Help Desk Heather Pollock – Contracts Dept.	0711 785-1000 0711 785-1611	Our Account Id: 100850
P S Venter	HP Hardware	Paul Venter	0782 453-8104	
Ventyx S.A.	Ellipse Application and Database	Help Desk Solly Lindeque – Account Manager Fiona Baker	+27102026176 +27832805895 +27112604600 +2782516293	
Software AG	ADABAS / Natural (Billing System)	Help Desk Mpho Matsega – Account Exec.	0711 575-0970 0782 902-9131	
Computronics Systems	Other Hardware / Software	Reception	2404-5504	
PC Systems	Other Hardware / Software	Reception	2404-1083	
ITRON	Software/Hardware Other	Account Manager Eugeneo Novell	**Mobile**: +27 83 2929 436	Itron Helpdesk

			Phone: +258 21 31 77 38 / +258 21 31 75 74	
Netcomm	Other Hardware / Software	Reception		
Posix	Email Hardware / Software	Zanele Miranda Ralph Nkambule	76175578 76020068	

11.   Supporting Documentation

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

12.   Policy Support Contact

- IT Manager

- General Manager Finance

13.   Amendment

This policy may be amended from time to time at the company's sole discretion, as and

when it becomes necessary.