1 PURPOSE

The purpose of this document is to ensure that a consistent process is adopted for the backup of data, libraries and critical devices. This is to achieve: –

a) Backup are in place to facilitate system recovery to cater for eventuality of major disaster or hardware failure,

b) Backup are in place to facilitate application recovery to cater for eventuality of application investigation and ability to re-generate documents for meeting local statutory requirement and business requirement.

c) Backup are in place for critical devices in the event of a hardware failure.

2 SCOPE

This document is applicable to SMS Technology and covers Operating Systems (OS), applications, databases, logs and critical devices.

3 BACKUP POLICY

3.1 Backup should be made on a regular basis that will ensure the continuity of processing in the event of a processing interruption.

3.2 All backup media must be recorded , uniquely identified, stored securely and subject to secure disposal procedures.

3.3 Copies of backup files and documentation must be kept off-site in a secure location at all times. Backup's copies must be transferred to the off-site location regularly, preferably at least once daily.

3.4 Security of backup's storage media must be maintained in compliance with the Physical Security/Environmental Controls Standards.

3.5 There should be a periodic testing of backup media at both on-site and off-site locations (at least once a year) to ensure that backup are in useable condition for recovery and that their contents are as documented. Backup's media found to be unreadable must be reported to the Head of Computer Operations.

AD

3.6 All movements of backup media must be monitored and logged. Only authorized staff may carry out the deposit and withdrawal of backup media from storage locations only

3.7 Copies of backup files moved to or from off-site storage locations must be provided with defined and agreed levels of security during transportation.

3.8 The retention period of backup must be in accordance with relevant regulatory requirements. This must be documented in operations procedures. Business Owner should define regulatory requirements.

3.9 When a computer equipment is changed, consideration should be given to the backup media and data formats to ensure that they can still be restored.

3.10 Access to backup media must be capable of being retrieved within a time scale documented in the computer disaster recovery plan.

3.11 Where a third party has been authorized to store backup media, a service level agreement (SLA) should be defined and documented, and in compliance with the IS Security Standards.

3.12 Automated backup functions within software packages should be used where applicable.

3.13 Systems backup must also be carried out immediately after any upgrade, changes done to a system or and application.

3.14 All on-site and off-site tape must be properly labelled.

3.15 Backup Register for On-Site and Off-Site tapes must be maintained. Any tape movement must be recorded properly

3.16 Backup tape must be sent to off-site location within 24 hours.

3.17 On-site and off-site tape inventory checking should be carried out by independent party e.g. Audit or Branch Compliance Officer at least once a year

3.18 The insurance policy should be purchased to cover the additional cost of the use of backup equipment such as cost of accommodation, additional travel expenses, overtime, etc. all of which are likely to be incurred should a disaster occur.

3.19 The backup strategy for each system must be formally documented and approved by the system and data owners.

4 RESTORATION

4.1 Authorization to restore data from backup media that would overwrite existing production data must be obtained from Data Owners.

4.2 In the event of system failure, escalation procedure must be in place and made aware to system administrator.

4.3 Recovery and restart procedures must be established and brief to relevant parties. The document must be easily accessible to the authorized parties.

4.4 Source documents, reports and backup media for reconstruction of a system must be identified and documented.

4.5 Restoration of a previous configuration to any points in time within either statutory requirements or company requirements whichever is the greater should be established and documented.

4.6 Restoration of the current configuration must be within agreed recovery timescales.

5 BACKUP OF NETWORK AND CRITICAL DEVICES

5.1 Availability of critical devices with sufficient capacity and speed for backup should be established and documented i.e.

a) Maintaining spare equipment on-site for critical devices e.g. UPS, LAN interface cards, cabling, connectors, terminators and bridge devices.

b) Adequate provision for the re-routing of network messages in the event of a component failure.

c) Uninterruptible power supplies (UPS) systems to protect critical network servers and LAN components.

6 ENFORCEMENT

6.1 All staffs are required to comply with this security policy and its appendices. Disciplinary actions including termination may be taken against any SMS Technology staffs who fail to comply with SMS Technology's security policies, or circumvent/ violate any security systems and/or protection mechanisms.

6.2 Staff having knowledge of personal misuse or malpractice of IT Systems must report immediately to management and IT Security.

6.3 SMS Technology's staff must ensure that SMS Technology's contractors and others parties authorized by SMS Technology using its internal computer systems, comply with this policy.

6.4 Where the role of the service provider is outsourced to a vendor, the outsourced vendor should ensure compliance with this policy.