SBS IT Backup Policy

The purpose of this backup policy is to protect SBS Networks information systems and ensure the timely recovery of any data loss.

Scope

This policy provides a framework for the backing-up of systems and data throughout SBS Networks. It applies to:

- All those with responsibility for SBS Networks information systems
- All electronic information processed by SBS Networks
- Any system managed by SBS Networks IT Personnel

Each backup provides a point in time snapshot of information as it existed during the time the backup took place.

System backups are not meant for archiving of data or maintaining a versioned history of data.

SBS Networks have an EMC SAN located in their Manchester North office (which stores the company data) and a second recovery SAN in their Manchester South office. Using EMC's recover point software, all data is instantly replicated from North to South.

In the event of a disaster recovery invocation, this technology would be the primary way of restoring SBS Networks systems by bringing online the IT systems stored on the South Manchester SAN. Backups stored at the North Manchester office would not be used for this purpose.

Aims & Commitments

All computer systems and information belonging to SBS Networks will be backed up.

Backups will be managed, and comply with relevant legislative and regulatory requirements.

Confidentiality of information will not be breached, with information only accessed by those authorised to do so.

Backups

Backups are monitored daily by the IT Team to ensure any failures are actioned and remedied.

All backups are stored on a 50TB Network attached storage (NAS) device that is in a secure computer room, with controlled access.

Backup Schedule

All servers that have a high, medium or low data change rate are backed up each night (7 days a week) and a total of 14 days' worth of backups are kept for each server.

All servers that have limited or no data change are backed up once a week.
14 Backup copies are kept for each server.
At each month end, backups of critical servers are taken and kept for 1 year.
At each year end, backups are taken or critical servers and are kept for 7 years
Backups are run overnight and are completed before 8am each day.

Restoration of Data

Data is available to restore as soon as the backup job has been completed
Random test restores are carried out to ensure backups have been successful and data can be successfully recovered. This includes email systems; SQL databases and file restores.

Users can request restores of data by logging a support call with the IT team.
Users requesting a restore are required to provide as much information about the data as necessary.

Backup Security

All backups are encrypted, including transmission to the backup storage.
Only the appropriately authorised IT staff have access to the backup software and data.

System upgrades

Prior to any system changes or upgrades, SBS Networks IT personnel will ensure that either a VMware snapshot or backup is taken. In the event of any issues with the system upgrade, changes can be rolled back or restored to its pre-upgrade state.