MBARARA UNIVERSITY OF SCIENCE AND TECHNOLOGY
DRAFT SYSTEM AND DATA BACK UP PROCEDURES

Introduction

This document aims at providing a backup recommendation for all university data. This is to ensure that university system/application software as well as related data are adequately preserved and protected from destruction.

Coverage

The procedures and guidelines in this document shall apply to all software and data owned, used, managed and administered by Mbarara University of Science and Technology.

The responsibility of backing up data held on workstations/ computers of individuals regardless of whether they are owned privately or by the university falls entirely to the user. This shall be done using adequate infrastructure and support provided by the Computing Services Unit.

The responsibility of backing up **critical university systems and data** shall lie with the Computing Services Unit. This applies to systems that are officially handed over to the Computing Services Unit with all the necessary requirements as per policy.

Procedures and Guidelines

Data Backup procedures for all Users

1. Users should take time to identify the important data that they hold on their computer e.g. important office documents, Microsoft word and excel files, any databases held locally on machines as well as emails that may have been downloaded onto the computer.
2. Users shall use appropriate back up media/ infrastructure provided or recommended by the Computing Services Unit.
3. Any removal backup media like CDs, Disks should be labelled as precisely as possible with date, and some information to indicate what data has been backed up.
4. Users should hold multiple copies of important data from different time intervals.
5. Copies of back-up media, together with any notes on what has been backed up, should be stored safely e.g. in a locked drawer. Ideally the copy of the data should be kept in another location, at a sufficient distance away to escape any damage from a disaster e.g fire or flood.
6. Users through guidance from the Computing Services Unit should test the process of restoring data from the backup copy. This should ensure that that all the necessary data is backed up correctly and to also familiarise with the process, should there ever be the need to restore data in the case of a real emergency.

Data Backup procedures for Critical University Systems and Data

The following comprise criteria for consideration in doing backups of critical university systems and data.
The eventual process will depend on the system under consideration

1. Backups may comprise a combination of;
    a. Full backup ; where all data files and/or all application files are backed up to a secure back up media
    b. Incremental; where only files which have changes since the last FULL back up are copied
2. A full backup set should be created at least once per month for on-site storage.
3. A full backup set should be moved offsite at least once each calendar month.
4. A planned schedule of backup cycle is recommended for each system. For instance, a suitable schedule may comprise the following:
    a. An end of month full backup followed by,
    b. Daily incremental backups for the remainder of the month,
    c. Monthly full backups retained for one year on site,
    d. A copy of the monthly full backup forwarded to an offsite secure location
    e. The final full backup at the end of the year retained for 5 years both onsite and offsite depending on the nature of the system,
5. Back ups must be performed when the system is not in use to ensure the quality of the process, for example, overnight or at weekends.
6. Back up processes (logs) must be checked for successful completion.
7. Back ups must be verified to the source data to ensure integrity.
8. Backups must be tested at least quarterly to ensure that backup data can be recovered in usable form.
9. All university systems under development should be verified for backup provision and compliance before handover to the university.

Backup Media

The backup media chosen will depend on factors such as;

- Frequency of backups
- Size of backup files
- Longevity and reliability
- Cost