Finance and Accounting Manual

Satellite Centres – System Backup Procedures

Approved by the Chief Financial Officer on 10 December 2010
Date of effect: 10 December 2010. Updated: 25 September 2012.

1. Overview

1.1 Purpose

The purpose of this policy is to provide a backup recommendation for all systems which provide a repository for critical University financial data.

The objective is to ensure that applications software and university financial data are adequately preserved and protected from destruction.

1.2 Coverage

This policy applies to all departments/units operating satellite financial systems as defined below and is strongly recommended for all computer users.

1.3 Background

Data is a corporate asset and can have significant value to the University. Such data can be easily lost or destroyed by system malfunction or accidental or intentional means. Thus it is important for the University to have an effective backup strategy to ensure that this corporate resource is safeguarded at all times.

An adequate backup strategy will enable the recovery of electronic data whenever necessary. This document attempts to set out a generic backup strategy which can be adapted to different financial systems as appropriate. The effective design and implementation of a coherent backup process is the responsibility of line management with accountability for each system regardless of the scope of the system.

1.4 Policy

Each department/unit which operates administrative applications must perform a system backup on a periodic basis. The frequency of these backups, retention location and the retention timeframes for each will be dependent on the criticality and volatility of the data residing on each system.

2. Procedures and Guildelines

2.1 Guidelines

Computer systems that create or update University data on a daily basis should be backed up on a daily basis to minimise the exposure to loss of critical data.

Computer systems which do not themselves create or update University data have a lesser degree of criticality and backups may be performed on a less frequent cycle depending on each systems operating parameters. Such systems may operate on data extracts from a primary system for reporting and analysis purposes and may have data elements which would be difficult to replicate if lost.

2.2 Processes

It is a requirement to ensure that where feasible, backup strategy takes into account any centralised network data backup facility operated by ICT, in addition to the recommendations that follow.

The following comprise criteria for consideration in planning a backup strategy and the eventual process will depend on the system under consideration.

(i) Backups may comprise a combination of
- Full backup
- Incremental backup (see definitions section 2.4)

(ii) A full backup set should be created at least once per month for on-site storage.

(iii) A full backup set should be moved offsite at least once each calendar month.

(iv) Where full backups are taken less frequently than daily, incremental backups must be used to ensure data can be restored to the state as at the close of the previous session.

(v) Full backup sets should be retained for an extended period depending on the degree of criticality of the data, for example, retention of 1 year would be appropriate for critical financial data which is likely to be subject to audit and reporting.

(vi) A planned schedule of backup cycle is recommended. 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 end of year retained for 5 years both onsite and offsite depending on the nature of the system.

(vii) Backups must be performed when the system is not in use to ensure the quality of the process, for example, overnight or at weekends.

(viii) Backup processes (logs) must be checked for successful completion.

(ix) Backups must be verified (compared) to the soruce data to ensure integrity.

(x) Backups must be tested at least quarterly to ensure that backup data can be recovered in usable form i.e. that a restore will work.

2.3 Backup Media

The backup media chosen will depend on factors such as:
- Frequency of backups
- Size of backup files
- Longevity and reliability
- Cost

The selection should be made after consideration of all relevant factors. System owners should take into consideration the ICT operated backup system Legato Networker and Avamar, which provide a network based backup process.

2.4 Definitions

Satellite Financial System	A system providing facilities similar to but separate from the central administration system.
University Data	The collection of data elements which are relevant to the operations, plans or management of more than one University department or unit which forms part of the University.
Systems Backup	A documented procedure for copying applications software and data files that reside on computer disks to a backup media.
Full Backup	All data files and/or all application files are backed up to a secure backup media.
Incremental Backup	Only files which have changed since the last FULL backup are copied.
Offsite Storage	Backup media is physically stored in a remote location. This may be merely as far as the next building.
Backup Media	The storage medium for backup files, for example, CDR, DVD-R, Zip Disk, External hard disk, Tape, etc.
Networker	The ICT operated system for taking nightly backups of data on computers on the University network. Note that this facility requires configuration with ICT involvement.

2.5 Consequence of Non-Compliance

Non-compliance with this policy could severely impact the operation of the organisation by exposing the University to permanent loss of University data. Loss of funding where the data was a critical component may also follow. It may also expose the individual or the University to legal action.

3. Related Information

3.1 Resources and weblinks.

(i) Training Materials

(ii) References

(iii) Additional Resources

3.2 University procedures superseded or replaced by this procedure:

- Finance and Accounting Manual: Satellite Centres – System Backup Procedures: 1 September 2002

4. Contact and Review

4.1 Contact

Unit: Strategic Financial Solutions
Phone: 02 9351- 4633
Fax: 02 9351-4202
Email: lean.lee@sydney.edu.au

4.2 Review

The Chief Financial Officer will approve changes to financial procedures and guidelines and will co-ordinate changes to financial policy, with the Vice-Chancellor delegated to approve University financial and infrastructure policy.

Amendments to forms, schedules and weblinks will be processed by Financial Services.

Amendments to the Finance and Accounting Manual procedures and forms are listed on the Financial Services website under:-

- FAM Amendments
- Amendments to Forms

Please forward suggestions and comments on the Finance and Accounting Manual via the Feedback Form.