

(Standard) ICT Standard for Data Backup

Document Purpose

Document Purpose	<p>This standard provides directions and guidance on the data backup management (including restoration) performed by the Division of ICT Services of the University of Southern Queensland.</p> <p>This standard does not include provision for hand-held devices.</p>			
Document Information	Version	1.0		
	Release Date	November 2009		
	Release Status	Draft		
	Review Date	November 2010		
	Author(s)	Principal Manager – Infrastructure and Systems		
	Owner	Principal Manager – Infrastructure and Systems		
	Print Date	Last Printed: 21/06/2010 12:24:00 PM		
	Approved By	Principal Manager – Infrastructure and Systems		
	Policy	USQ ICT Policy for Information Management and Security		
	Type of Document	Standard		
	Electronic Location and Filename			
Version Control	Version	Date	Author(s)	Summary of Changes
Error Advisory	<p>To the Reader:</p> <p>If you encounter any inaccuracies or printing faults in this document please contact the Owner (see Document Information section, above) as soon as possible. The Owner will then initiate the required modifications</p> <p>If you are unable to contact the Owner, contact that person's Manager Supervisor.</p> <p>Thank you for helping the Division of ICT Services maintain quality documentation.</p>			

Table of Contents

Document Purpose	1
Document Information	1
Error Advisory	1
1 Definitions.....	3
2 Introduction	3
3 Exemptions	3
4 Data Backup Schedule	3
5 Backup Components	4
5.1 Backup Types and Frequency.....	4
5.2 Media, Equipment, and Utilities	5
5.3 Storage.....	5
5.4 Backup Media Disposal	5
5.5 Backup and Recovery Documentation	6
6 Data Restoration.....	6
7 Quality Assurance and Exceptions	7
7.1 Exceptions	7
7.2 Backup and Recovery Verification.....	7
8 Responsibilities.....	8
8.1 DICTS Responsibilities.....	8
8.2 Client Responsibilities	8
8.3 Exceptions	9
9 Related Documents.....	10

1 Definitions

The *ICT Glossary and Definitions* contains a description of any common ICT terminology referred to in the policy and standard documentation.

2 Introduction

The Division of ICT Services (DICTS) manages, operates, and supports a large number of computer systems throughout the University of Southern Queensland. In the event of any of these systems encountering data loss, each system is covered by a data backup regimen.

The data backup regimen is a system of recording identified data onto portable media. This media is then stored both on-site and off-site to limit total loss in case of a declared disaster. The media contains a copy of specific data as at a specified time. The backup regimen is developed in conjunction with the client to meet both business and legislative requirements.

If that data is required for recovery, a data restore may be performed from the backup media.

3 Exemptions

This standard does not apply to client devices including desktops, laptops, PDAs and USB storage devices such as USB hard drives and USB sticks. The backup and recovery of data on these devices is the responsibility of the individual user.

4 Data Backup Schedule

All computer systems operated, managed and/or supported by DICTS are covered under a Service Level Agreement (SLA) between DICTS and the client. The SLA contains a proviso for the client's computer system - ensuring continuity of data access and protecting the client from data loss due to systems failure, virus, vandalism, operator error, or accidental erasure.

Where a SLA covers a computer system, and a backup regimen has been requested for that system, then the system is included in the data backup schedule. Prior to including the computer system in this schedule, the client will have determined which components and data they require to be backed up as per business and legislative requirements, which could include conducting a business risk assessment, which is dependent on:

- Importance of the data and information to the organisation;
- Acceptable transaction loss (business areas must determine what level of potential transaction loss would not be acceptable or would be too difficult to recover. This can be determined in terms of a timeframe, the number of transactions, or the amount of time and effort required re-entering data);
- The maximum acceptable outage of the system while performing backups;
- The maximum acceptable outage of system while recovering data.

5 Backup Components

The following are the components of a backup regimen for a computer system. Component selection is agreed between DICTS and the client, and documented in a SLA, prior to the first scheduled backup for that system being initiated.

Data to be backed up may include:

Data Type	Description
Business Data	Memos, documents, customer information, financial records, databases, accounting information, project data, schedules and appointments, email, and other critical files.
Systems Data	Software and hardware configuration data, software applications, user ids, access rights, directory structures, passwords, email configurations, and any other specialised systems information.

5.1 Backup Types and Frequency

All backups occur in line with a planned Data Backup Schedule created by DICTS to meet client requirements. There are three types of backups used by DICTS:

Backup Type	Description
Full backup	A complete copy of a computer system.
Incremental backup	A copy of only the data updated since the last full or incremental backup.
Image copy	Where a computer system is virtualised, a copy of the virtual server is backed up.

Each of these backup types may be performed at different frequencies or in combination:

- Daily
- Weekly
- Monthly
- Quarterly
- Yearly

Typically, data backups are performed:

- **Daily:** for data that changes on a daily basis.
- **Per an established schedule:** for data that changes at scheduled intervals, or to respond to major system events.
- **At month, quarter and year end:** for systems with closing dates.

5.2 Media, Equipment, and Utilities

All media, equipment and backup utilities (backup management software and in-house programs) used to perform backups are tested prior to live use. This testing determines compatibility with computer systems, storage environment, and backup frequencies.

- Where media is found to be faulty after specific testing, media is replaced.
- Vendor contact details for support and maintenance of backup hardware is on hand to ensure service contingency.
- Backup utilities are supported either by DICTS or vendor staff to ensure correct operation and backup success.

5.3 Storage

Backup media is stored both on-site and off-site. On-site storage is located within a physically secure and fire-proof area of USQ.

Off-site storage is in a secure and monitored location away from USQ premises. Authorised DICTS employees have 24x7x365 access to this location.

All media is securely stored whether in the on-site or off-site location, or in transit. Media is not stored in any location other than those authorised by DICTS.

5.4 Backup Media Disposal

Obsolete backup media will be disposed of in a safe and secure manner in accordance with State Archive General Retention and Disposal Schedule.

Backup media to be disposed of must be rendered unreadable through an appropriate means.

An audit trail of disposal of backup media will be maintained.

5.5 Backup and Recovery Documentation

If not included in the DRP for a computer system, backup documentation should include the following items necessary to perform essential tasks during a recovery period:

- Identification of all critical data, programs, documentation, and support items;
- Specified period of maximum acceptable outage (MAO) for all systems;
- Backup media storage locations;
- Required backup frequency, e.g. daily, weekly;
- Required backup cycles;
- Backup retention period (as per business and legislative requirements);
- Testing regime and process;
- Recovery schedule and plan; and
- Locations of relevant software and licenses.

Backup and recovery documentation will be reviewed and updated regularly to account for new technology, business changes, and migration of application to alternative platforms.

Documentation of the restoration process will include procedures for the recovery from single-system or application failures as well as for a total data centre disaster scenario.

6 Data Restoration

All backup data is accessible through data restoration. Data restores are performed within a physically secure area of DICTS by authorised DICTS employees. Restores are performed using tested utilities.

Before a restore is initiated, the client will have specified which files are to be recovered, and where those files are to be placed.

Client requests for data restores are only undertaken where the request is authorised by client management.

7 Quality Assurance and Exceptions

On the completion of a backup, success is verified using a backup log that monitors the files being backed up. Designated DICTS employees check backup logs on a regular basis as part of their standard duties.

Backup successes and failures are noted in a Backup Status Log. All failures are investigated, and any problems corrected in accordance with the terms of the SLA.

By default, every backup should complete with a data capture of 100% success rate. This standard is vital to the principle of quality data access continuity in the event of the need for a data restore.

7.1 Exceptions

Although the backup success rate should be 100%, there are allowable exceptions to the rule. A backup may fail either partially or fully in the event of a major power failure, a major power surge, because the files are in use or hardware and software failure.

Major Power Failure

A major power failure may lead to systems being powered by the Uninterruptible Power Supply (UPS). However, the UPS is not designed to provide maximum and indefinite use. The source computer system containing files scheduled for backup may have to be shutdown during an outage, and/or the outage could affect the computer system driving the backup device. Both cases would make it impossible to perform a data backup at that time.

Major Power Surge

Although greatly reduced due to the presence of the UPS, a major power surge could damage either the source computer system or the system driving the backup device.

Files in Use

Some computer systems require that no file is accessed or open during a backup. Where a client is using a file, rendering it unable to be backed up, and the result is the client's responsibility. This includes access by authorised representatives and unauthorised persons through the fault of the client.

Backup Hardware or Software Failure

A major backup hardware or software failure may lead to backups not being completed or performed. In this situation, if appropriate, the backups will be rescheduled.

7.2 Backup and Recovery Verification

Backup and Recovery procedures will be tested and verified on regular basis or as required.

8 Responsibilities

Both DICTS and the client have responsibilities in respect of data backups.

8.1 DICTS Responsibilities

The Division of ICT Services is responsible for:

- Configuring a fully tested backup system (including media, equipment, and utilities) and data restoration capabilities.
- Securing a comprehensive vendor support and maintenance contract (including replacement).
- Ensuring all data that the client has requested to be backed up is backed up in accordance with the client's SLA.
- Initiating, managing, and monitoring all data backups.
- Reporting backup successes and failures to the client on the basis and frequency agreed to in the SLA.
- Ensuring all backup failures are investigated and examined to ensure process integrity.
- Ensuring all faults affecting backup integrity are addressed within the agreed support timeframe documented in the SLA.
- Formulating and documenting support, guidance, and operational policies, processes, and procedures in support of all backup activities.
- Secure storage of media within USQ and at the off-site storage facility.
- Ensuring all client data is inaccessible to unauthorised persons.
- Modifying backup characteristics/requirements when formally requested by the client.
- Notifying the client as far in advance as possible of any changes affecting the client's backup (e.g. time, quality, frequency etc.)
- Ensuring that backup media is rendered unreadable prior to disposal and media is disposed of in an appropriate manner.

8.2 Client Responsibilities

The client, and any authorised representative of the client, is responsible for:

- Accurately identifying and documenting all data to be stored in their backups in accordance with business and legislative requirements.
- Notifying DICTS (via the procedure documented in the SLA) of the required backup regimen, and of any changes to that frequency. Ensuring the backup regimen meets all business and legislative archival requirements.
- Requesting DICTS to perform a data restore via the channels documented in the SLA.
- Ensuring all files are free and available for backing up at the scheduled time

8.3 Exceptions

The details in this standard may be amended under the following exceptional circumstances:

- By specific agreement as formalised in the client's SLA.
- By special request of DICTS and client management.

9 Related Documents

Document (Electronic)	DICTS Maintenance Schedule http://www.usq.edu.au/ict/staff/mainsch.htm
Document (Electronic)	ICT Standard for Operational Security Management http://www.usq.edu.au/resources/ict_standard_for_operational_security_management.pdf
Document (Electronic)	Queensland State Archive Disposal Schedule for Administrative Records http://www.archives.qld.gov.au/downloads/GeneralDisposalSchedule.pdf
Document (Electronic)	Queensland State Archive Retention and Disposal Schedule for Queensland Universities http://www.governance.qut.edu.au/rms/retention_disposal/QDAN601v2.pdf
Document (Electronic)	