



POLICY DOCUMENT – No. 6

Data Backup and Restoration Policy

Relevant UTas Ordinance and/or Rule Reference No.	Ordinance 9. – Student Discipline. General Staff Agreement. Academic Staff Agreement.
Relevant State/Federal Govt. Legislation	Telecommunications Act. Copyright Act. Archives Act 1983 Evidence Act 1910 Electronic Transactions Act 2000 Financial Management and Audit Act 1990 Freedom of Information Act State Privacy Act
Commencement Date	01 April 2006
Review Date	01 April 2008

Policy Statement

1. Intent

The intent of this policy is to define the back and restoration policy for all data and information associated with the University's ICT Infrastructure.

2. Scope

This policy applies to all Staff, Students and Associates of the University of Tasmania who create, process or store data and information using the University's ICT Infrastructure.

3. Objective(s)

- To define the back and restoration policy for all data and information associated with the University's ICT Infrastructure.
- To ensure copies of data are retained and available in case of disaster, software failure or, hardware failure makes data inaccessible.

4. Definitions and Acronyms

Archive	Move data to another medium (the backup media) for long term storage. Archive is intended for the storage of data that do not need to be kept immediately accessible, but which may possibly be needed at some point in the future.
Backup	Copy data to another medium so that, if the active

	data are lost, they can be recovered in a recent if not completely current version. Backup is primarily intended for disaster recovery.
Data	Numerical represented in a form suitable for processing by computer.
Information	Processed, stored, or transmitted data such that the data holds a meaning or can be interpreted.
Restore	The recovery of point-in-time copies of active data.

5. Policy Maker

Director, Information Technology Resources.

6. Policy Provisions

- 6.1. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- 6.2. The backup and recovery process for each system must be documented and periodically reviewed.
- 6.3. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source location.
- 6.4. Backup media must be protected in accordance with the highest sensitivity level of information stored.
- 6.5. All backup operations must include verification processes to ensure the integrity of the operation.
- 6.6. Backups must be periodically tested to ensure that they are recoverable.
- 6.7. Procedures between IT Resources and any offsite backup storage vendor must be reviewed at least annually.
- 6.8. Tape drives, cleaning tapes and other backup media must be maintained according to manufacturer's recommendations.
- 6.9. Backup tapes and other backup media must have at a minimum the following identifying criteria:
 - 6.8.1. System name;
 - 6.8.2. Creation date;
 - 6.8.3. Backup set name, and;
 - 6.8.4. Data owner contact information.

7. Breaches

Breach of this policy will result in disciplinary action that may include sanctions, suspension, expulsion, termination of employment, legal action, or other disciplinary action.

Staff, Students and Associates learning of any violation of this policy must bring this matter to the attention of an appropriate staff member within the University without delay.

8. Supporting/Related Documents

- Secure Password Standard
- System Level (Privileged) Password Management Standard
- Desktop Computing Standard (Usage) Section 3 Desktop Computing Data and Information Management.

9. Key Words

- Security
- Data
- Backup

10. Supporting Procedures/ Guidelines

- Information Technology Facilities Use Agreement
- Standards for the Use of University ICT Facilities

Responsibilities

Implementation	Director, ITR
Compliance	University Staff, Students and Associates
Monitoring and Evaluation	ICT Security Officer University ICT Staff
Development and/or Review	Director, ITR
Interpretation and Advice	Director, ICT Resources ICT Security Officer

Who Needs to Know this Policy?

All Authorised Users of University ICT Facilities.

Effectiveness of this Policy

- Increased confidentiality, integrity, and availability of University of Tasmania ICT Facilities.
- Lower frequency of complaints concerning inappropriate use of the University's ICT Facilities.

Policy History

Policy No.	6, version 5
Approved / Rescinded	Approved by John Parry, Director, ITR
Date	17/03/2006
Endorsement	Pending
Vice-Chancellor	
Signature	