



Data Backup and Restoration Procedure

UNDER REVIEW

Related Policy	ICT Security Policy
Responsible Officer	Chief Information Officer
Approved by	Chief Information Officer
Approved and commenced	August, 2014
Review by	August, 2017
Responsible Organisational Unit	Information Technology Services

CONTENTS

1	Objective	2
2	Scope	2
3	Procedure	2
4	Definitions and Acronyms	3
5	Supporting Documentation	4
6	Versioning	4

1 Objective

To minimise ICT Security and Business Continuity risks associated with data loss by defining a sound backup regime for all centralised ICT data services.

2 Scope

All Authorised Users of University of Tasmania ICT Services, Facilities and Infrastructure and all ICT Services, Facilities and Infrastructure.

3 Procedure

Step	Details	Responsibility
1.	The frequency and extent of backups must be in accordance with the importance of the information. The Data Custodian will determine the importance of the data via risk assessment and notify IT Services of the required backup frequency.	Data Custodian
2.	The backup and recovery process for each system must be documented, and reviewed at least annually.	ICT Officer Data Custodian
3.	Physical access controls must be implemented to protect physical backup media. When backup media is stored onsite (within IT Services locations) physical access controls must meet those defined in the ICT Physical Security Procedure. Offsite backup storage locations must meet or exceed the physical access controls of the source location. Backup media must be protected in accordance with the highest sensitivity level of information stored.	ICT Officer ICT Security Manager
4.	Backup operations must include verification processes to ensure the integrity of the operation.	ICT Officer
5.	Backups must be periodically tested, at least annually, to ensure that they are recoverable.	ICT Officer
6.	Procedures between IT Services and any offsite backup storage vendor must be reviewed at least annually.	ICT Security Manager Chief Information Officer
7.	Tape drives, cleaning tapes and other backup media must be maintained according to manufacturer's recommendations.	ICT Officer

8. Backup tapes and other backup media must have at least one of the following identifying criteria:

- System name;
- Creation date;
- Backup set name, and;
- Data Custodian contact information.

4 Definitions and Acronyms

Academic Unit	Means the secondary organisational unit in the academic structure of the University, reporting directly to the College Executive Deans, as per Ordinance 14 – Academic Structure.
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.
Authorised User	<p>An individual who has been granted access to University ICT Services under one or more of the following categories:</p> <ul style="list-style-type: none">• a current member of the governing body of the University;• a currently employed officer or employee of the University;• a currently-enrolled student of the University;• any person granted access to use University of Tasmania ICT Services including, but not limited to:<ul style="list-style-type: none">▪ A contractor undertaking work for the University under the provisions of a legal contract;▪ A member of a collaborative venture in which the University is a partner; or <p>A visiting lecturer, student or other associate who is undertaking similar activities in a recognised University, as a registered associate.</p>
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.
College	Means (a) the primary organisational unit in the academic structure of the University, as per Ordinance 14 – Academic Structure (b) the University College
Data	Numerical represented in a form suitable for processing by computer.
Data Custodian	A nominated trustee of University of Tasmania data. A data custodian holds responsibility for protecting the data as defined by University of Tasmania Policies and Procedures.

Data Custodians may be nominated by their role with the University of Tasmania, or by their role in relation to an ICT Service. A Data Custodian will typically have responsibility for the management of a location of shared information, a database, or an application referencing a database distinct from the role of a systems administrator.

Data Custodians may include but are not restricted to:

- Application Managers
- Data Managers
- Business Systems Owners

ICT Officer	The University of Tasmania staff authorised by the College, Academic Unit and/or Chief Information Officer to maintain and/or administer ICT Services, Facilities Infrastructure, user level accounts and passwords.
ICT Security Manager	The ITS appointed representative responsible for ICT security.
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 Supporting Documentation

- ICT Security Policy

6 Versioning

Former Version	Version 1 - Data Backup and Restoration Procedure; approved May, 2010; reviewed May, 2014. Version 2 - <i>Data Backup and Restoration Procedure</i> , minor amendments to update terms and definitions, approved by Responsible Officer, Chief Information Officer, August, 2014, amended in December 2016 to incorporate Colleges.
Current Version	Version 3 – <i>Data Backup and Restoration Procedure</i> (current version); approved August 2014, amended in December 2017 to incorporate final academic structure.