

Policy and Procedure



SWINBURNE
UNIVERSITY OF
TECHNOLOGY
SARAWAK CAMPUS

Name: **Computing Equipment Backup**

Approved by: Executive Committee

Last reviewed: 21 May 2009

SECTION 1 - INTRODUCTION	2
PURPOSE	2
SCOPE	2
DEFINITIONS	2
LEGISLATIVE CONTEXT	2
SECTION 2 - POLICY	3
PRINCIPLES	3
POLICY	3
SECTION 3 - PROCEDURE	4
PROCEDURE	4
SUPPORTING DOCUMENTATION	4
SECTION 4 - GOVERNANCE	5
RESPONSIBILITY	5
VERSION CONTROL AND CHANGE HISTORY	5
POLICY & PROCEDURE DIRECTORY REQUIREMENTS	5

SECTION 1 - INTRODUCTION

PURPOSE

The purpose of this policy is to set out the responsibilities of staff and students in relation to backup and restoration of files on desktops, notebooks, handheld computing equipment and USB storage devices.

SCOPE

This policy and procedure applies to all University staff and students.

DEFINITIONS

Word/Term	Definition
Backup	The process of copying all modified data from a user's computer system onto another medium, such as floppy disk, optical disk, CD or USB storage device.
Network drives	G: Staff group share drive H: Home drive P: Applications drive T: Student and Staff group share drive

LEGISLATIVE CONTEXT

Name	Location
None	

SECTION 2 - POLICY

PRINCIPLES

The University backs-up its data on a regular basis to ensure that data can be recovered to the most recent version in the event of a breach of security, deletion of data, or corruption of data.

POLICY

1.	<p>The University will automatically take a nightly back-up of all student and staff data stored on network drives G:, H:, P: and T.</p> <p>All users must log out at night to allow network drives to be backed up. Files left open on network drives will not be backed up.</p>
2.	<p>Data stored on desktops, notebooks, hand held computers and USB storage devices will not be backed up by the University.</p> <p>Staff and students must back-up their own data stored on these mediums.</p> <p>In the event that the security of a system is breached, and data is deleted or corrupted, users will need to have a plan that enables them to restore their information to a useable form.</p>

SECTION 3 - PROCEDURE

PROCEDURE

	Procedure steps	Responsibility
1.	Data backup	
1.1	Regularly back-up data stored on desktops, notebooks, hand held computers and USB storage devices	Staff and Students
2.	Data download to network drives	
2.1	Download any required information to the network home directory (H:/drive)	Student
2.2	Download any required information to the network home directory (H:/drive), or to the (G:/drive).	Staff
2.3	Close files on network drives prior to logging out.	Staff and Students
2.4	Back-up all student and staff data stored on network drives G:, H:, P: and T, nightly:	ITS

SUPPORTING DOCUMENTATION

Forms and Records Management

Form	Retention Time	Retention Location
None		

Related Material

Name	Location	Document Type
Server and Core Database Backup Restoration Policy	Policies & Procedures Directory	Policy

SECTION 4 - GOVERNANCE

RESPONSIBILITY

Policy Owner	Manager, Information Technology Services
---------------------	--

VERSION CONTROL AND CHANGE HISTORY

Version Number	Approval Date	Approved by	Amendment
1	21 May 2009	Executive Committee	New policy; Previously used SUT Australia policy

POLICY & PROCEDURE DIRECTORY REQUIREMENTS

CATEGORY
Information Support Services

KEYWORDS
Information technology, computer equipment, backup