

Policy and Procedure



Name: **Information Technology Security**

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	7
PROCEDURE	7
SUPPORTING DOCUMENTATION	11
SECTION 4 - GOVERNANCE	12
RESPONSIBILITY	12
VERSION CONTROL AND CHANGE HISTORY	12
POLICY & PROCEDURE DIRECTORY REQUIREMENTS	12

SECTION 1 - INTRODUCTION

PURPOSE

The purpose of this policy and procedure is to provide direction and guidance on the establishment of minimum information technology security standards for use within the University.

SCOPE

The policy and procedure applies to all staff and students of the University.

Information Technology security applies to all University employees, academic/general staff, contractors, temporary staff, associated bodies and students who use the Internet with University computing or networking resources. This includes visitors and any other users utilising the Swinburne network.

DEFINITIONS

Word/Term	Definition
Appropriate Use	Means that the University IT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others.
Business Owner	An appropriate representative of the University user community responsible for the processes and access policies relating to the use of, and integrity of data within, an application. The Business Owner is responsible for ensuring that application changes are justified and will not compromise any business processes dependent on that application.
Designated Controlled Environment	Any area that is restricted to general use because of special contamination, power, security, temperature and humidity or fire protection requirements. Designated Controlled Environments are nominated by the University's Manager, Information Technology Services.
Due Diligence	Performance of an act with a certain standard of care.
Head of Management Unit	Head of Office, Division, School or Department in Swinburne University of Technology (Sarawak Campus)
Patch	A software update.
Remote Access	The ability to log onto a network from a remote location.
Standard Network Architecture (SNA)	A structure defining how computer equipment connects and communicates.
Secure Shell (SSH)	A program to log into another computer over a network to execute commands in a remote machine and to move files from one machine to another.
Secure Sockets Layer (SSL)	A protocol for transmitting private documents via the Internet.
User	An individual who uses a computer.

LEGISLATIVE CONTEXT

Name	Location
Copyright (Amendment) Act 1997	
The Computer Crimes Act 1997	

SECTION 2 - POLICY

PRINCIPLES

The University's approach to information technology security is based on national and international standards such as AS/NZS 7799.2:2000 and provides an integrated holistic approach to security. Each section is dependent upon the maintenance of a minimum standard to ensure the integrity of the whole system.

POLICY

1.	Physical computer room environment and access
1.1	Server Rooms
	All computer rooms and other information processing areas must adhere to a minimum standard of physical protection and environmental control as approved by the Manager, Information Technology Services (ITS).
1.2	Designated Controlled Environments
	1.2 .1 All designated controlled environments used by the University information processing and communications areas must be maintained to a minimum standard that provides for physical protection and environmental control.
	1.2.2 These physical controls will be appropriate for the size and complexity of the equipment and the criticality and sensitivity of the systems operated at those locations.
2.	Data Storage
2.1	Data collected and stored on University computer systems must only be used for the purpose for which it was originally collected.
2.2	Confidentiality must be maintained and appropriate back up and restoration procedures implemented for all stored data.
2.3	The Business Owner must determine how data is to be used and to whom access is to be granted, in keeping with University policies on the confidentiality and storage of data.
2.4	Data stored on the University's core computer systems must not be copied or downloaded to any computer systems without prior written approval of the Business Owner. Permission to transfer raw data to personal computers will only be given in exceptional circumstances and with written authority.
2.5	Data must not be stored external to the University without prior approval of the Manager, Information Technology Services (ITS).
2.6	Swinburne material must not be hosted on external web sites without prior approval of the Manager, Information Technology Services (ITS).
3.	User account and password management
3.1	Access to Swinburne computer systems must be controlled by usernames and passwords.
3.2	The Information Technology Services Department will generate a username and initial password for all users who require access to the University's computer systems.
3.3	Usernames and passwords must be used appropriately. i.e. They must remain confidential, not be written down in obvious locations, must not contain slang and are not to be shared.
3.4	Misuse of computer systems which is attributable to the user's login may be regarded officially as misuse and may lead to disciplinary action.
3.5	Swinburne Employees (Payroll Staff)

	3.5.1 Will be provided with access to the University's computer systems once they have completed and submitted a H1S-Network Account Form to Information Technology Services.
	3.5.2 Access to core system applications will be uniquely identified through the use of a user account.
	3.5.3 Access to functional procedures within a core application will be provided on the basis of grouped functions determined by the Business Owner to ensure appropriate segregation of duties.
	3.5.4 Access to the University's computer systems will be automatically removed at midnight on the last day of employment as documented on the H1S-Network Account Form.
	3.5.5 Access to the University's computer systems may be revoked at anytime as the result of a breach in University policy.
3.6	Students
	3.6.1 Are provided with access to the University's computer systems once their enrolment has been confirmed and they have been acknowledged within the Student Management System.
	3.6.2 Access to the University's computer systems will be removed three months after the final semester of enrolment. Student Operations will provide the list of student names to the ITS Department.
	3.6.3 Access to the University's computer systems may be revoked at anytime as the result of a breach in University policy.
3.7	A copy of all administrator server passwords must be retained by Information Technology Services.
4.	Wireless Access
4.1	Wireless access to University systems will be provided to all staff and students from certain locations on University's campuses, provided users have appropriate hardware and software.
4.2	Wireless access must only be used for activities that are directly related to the University.
4.3	Wireless service must be accessed via authorised access points that are installed and managed by the University
4.4	Use of unauthorised wireless equipment on campus premises is strictly forbidden.
4.5	All University policies relating to the use of computing facilities, including regulations on ethical and legal use of software, apply to the use of Swinburne wireless access.
5.	Internet / Intranet access
5.1	Access to the Internet and the University's intranet will be provided to all users who have a valid user account. Provision of access is subject to teaching and learning, research and administrative use and on-line monitors and filters will be used to identify inappropriate, excessive or unauthorised usage.
5.2	Under no circumstances may a user establish wireless access points, modems, Internet or other external network connections to University systems, networks and University information
5.3	Users are prohibited from using new or existing Internet connections to provide new communication channels outside of the designated services provided by the University without approval of the Manager, Information Technology Services (ITS). These channels include electronic data interchange (EDI) arrangements, electronic banking, electronic malls with on-line shopping and on-line database services
5.4	De Militarized Zone (DMZ) All systems, devices or network subnets that are accessible from the Internet must reside in the DMZ

	5.4.1 Firewall
	5.4.1.1 No traffic from the Internet to the DMZ, and vice versa, is permitted unless prior arrangements have been made with ITS to allow for such specific services.
	5.4.1.2 No traffic from the DMZ to the University private network, and vice versa, is permitted unless prior arrangements have been made with ITS to allow for the specific services
	5.4.2 User Workstation Subnets
	5.4.2.1 No direct connections from the Internet to user's workstations are permitted
	5.4.2.2 Connections from the user's workstation to the Internet is through a proxy server only
	5.4.2.3 Servers are not to be connected to user networks.
	5.4.3 Perimeter Firewall – Incoming Connections To protect University network users from attacks launched from the Internet, all external Internet traffic to the University's network may be denied, unless explicitly permitted.
	5.4.4 Perimeter Firewall – Outgoing Connections All internal traffic outbound to the Internet is denied unless explicitly permitted.
	5.4.5 Changes to Firewall
	5.4.5.1 ITS will not make changes to the firewall rules that pose an unreasonable risk to the University. Where the risk is acceptable, granting of requests will depend on network infrastructure limitations.
	5.4.5.2 By requesting additional services to be made available through the firewall, staff and the School accept the responsibility of maintaining the integrity of the host machines.
6.	Information Security
	6.0.1 University, proprietary, or private information must not be sent over the Internet unless it has first been encrypted through SSL or SSH.
	6.0.2 Credit card numbers, log-in passwords, and other parameters that can be used to gain access to University systems, networks and services, must not be sent over the Internet in readable form.
6.1	Right to Examine
	6.1.1 The Pro Vice-Chancellor or nominee retains the authority to grant the right to intercept, inspect, copy, store and disclose electronic data via written authorisation to: <ul style="list-style-type: none"> • prevent or correct improper use; or • satisfy legal obligation; or • ensure the proper operation of the network
	6.1.2 At any time and without prior notice, University management reserves the right to examine e-mail, personal file directories, and other information stored on University computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of University information systems
6.2	Reasonable Usage
	Limited use of University computing resources for personal or non-University activities is permitted as long as this does not interfere with other work activities within the University
7	Wide area network
7.1	Unless permission is granted by the Manager, Information Technology Services (ITS) staff / students will be in breach of this policy and will be subject to disciplinary or legal proceeding if they: <ol style="list-style-type: none"> a) intercept private electronic data; or

	<ul style="list-style-type: none"> b) add or alter equipment; or c) redirect electronic data; or d) add new points of presence on the public domain; or e) read private electronic data; or f) copy private electronic data; or g) modify private electronic data either in transit across a network or stored within a computer system.
7.2	Access to the University's data and voice communications network will be secured at all times and limited to nominated staff.
7.3	No other groups are to connect network devices to the Swinburne network unless explicitly permitted.
7.4	Equipment to be added to the University's network must be Standard Network Architecture (SNA) compliant.
8.	Local area network
8.1	Users must lodge an application with Information Technology Services to establish a new server.
8.2	A new server will not be connected to the University network until approval is gained from Information Technology Services and:
	8.2.1 Users or categories of users of the server are identified;
	8.2.2 System privileges for each category of user have been determined;
	8.2.3 User authentication process is implemented;
	8.2.4 Intrusion detection strategies have been implemented;
	8.2.5 The server is fully patched and secured and;
	8.2.6 Procedures for backup and recovery of information resources are documented.
8.3	The University may disconnect servers without warning if the server is not patched or secured.
9.	Anti virus
9.1	Licensed virus checking and cleansing software will be installed automatically on all desktop machines.
9.2	Anti virus programs will be updated daily and form part of the Standard Operating Environment.
10.	Software
10.1	University computer software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-university party for any purposes other than those expressly authorised by the Manager, Information Technology Services.
10.2	Software or data must not be exchanged between the University and any third party unless a written agreement has first been signed, specifying the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected. Regular business practices, such as shipment of software in response to a customer purchase order, need not involve such a specific agreement since the terms are implied.
10.3	When using University computing or networking resources
	10.3.1 Students and staff must adhere to the software vendors' licence agreements
	10.3.2 Copying of software in a manner that is not consistent with the vendor's licence is strictly forbidden.

SECTION 3 - PROCEDURE

PROCEDURE

	Procedure steps	Responsibility
1.	Physical computer room environment and access	
1.1	Minimum Standard of Access Maintain minimum standard of access to designated controlled environments, as follows:	ITS
	1.1.1 Ensure physical access to controlled environment central computer rooms is only granted to authorised staff.	Manager, ITS, and Manager, Facilities Services
	1.1.2 Restrict issuing of passwords, lock combinations and keys to staff who have a clear need to access the designated controlled environment.	Manager, ITS, and Manager, Facilities Services
	1.1.3 Maintain a register of staff who have keys.	Manager, ITS, and Manager, Facilities Services
	1.1.4 Change passwords and lock combinations when: <ul style="list-style-type: none"> • an authorised staff member leaves; • passwords or lock combinations are compromised; • a lock is serviced; • at other times as required. 	Manager, ITS, and Manager, Facilities Services
	1.1.5 Retain duplicate passwords, lock combinations and keys.	Manager, ITS
	1.1.6 Lodge duplicate keys with Facilities Department for emergency access only.	Manager, ITS
1.2	Environment Requirements Maintain minimum standard of environmental control of designated controlled environments, as follows: <ul style="list-style-type: none"> • CCTV; • dry pipe, fire suppression system. • dual power supplies to each rack; • environmental monitoring software; • fire door; • generator; • independent air conditioning; • raised floor and cable management trays installed; • secured access; • uninterruptible power supply (UPS) to all processing units. 	Manager, ITS, and Manager, Facilities Services
2.	Data Storage	
2.1	All Heads of Management Units who store data on University computer systems must identify information they have created and assign ownership and sensitivity to the data.	Heads of Management Units
2.2	Backup and restoration procedures for all stored data are to be carried out in accordance with the Server and Core Database Backup Restore policy and procedure.	ITS

2.3	Under no circumstances may data be extracted from University computer systems and stored and manipulated on personal computers without the approval of the Business Owner.	Staff Member
3.	User accounts and password management	
3.1	Staff User Accounts	
	3.1.1 Swinburne Employee	
	3.1.1.1 Issue a H1S-Network Account Form from the Human Resource Department.	Human Resource Department
	3.1.1.2 Complete the H1S-Network Account Form, have it authorised by the Head of Management Unit and submit to ITS Service Desk for processing.	Staff Member
	3.1.1.3 Review the H1S-Network Account Form submitted and validate the information provided.	ITS
	3.1.1.4 Assign a Username and create the user account for staffs.	ITS
	3.1.1.5 Communicate user login credential to the user and let them key in their own email password.	ITS
	3.1.1.6 HR Department is to ensure the ITS Department removes user access to the University's computer systems on the last day of employment.	ITS
	3.1.1.7 Remove access to the University's computer systems due to a breach in University policy.	ITS
3.2	Student User Accounts	
	3.2.1 Student Operations will provide the ITS Department with appropriate information to create student's user account and initial password once enrolment has been confirmed and acknowledged.	ITS, and Student Operations Department
	3.2.2 Student Operations Department is to provide the ITS Department a list of student accounts for removal after the last /final semester of enrolment.	ITS Student Operations Department
	3.2.3 Access to the University's computer systems to be removed - due to a breach in University policy.	ITS
3.3	Changes to Staff Accounts	
	3.3.1 Swinburne Employees	
	3.3.2 Account change requests require the Change Control Form to be completed and authorised. The form is to be submitted to the ITS help desk for review.	Staff member
	3.3.2.2 Process the request. The account profile is modified, where appropriate, following documented processes.	ITS
	3.3.2.3 The user is advised of the changes made.	ITS

3.4	Changes to Student Accounts	
	3.4.1 To change personal, the appropriate paperwork to be submitted to Student Operations following their established processes.	Student
3.5	Password Management To provide for system security that will prevent unwarranted access to any IT system, the following rules must be followed.	
	3.5.1 All passwords created by a user:	Users
	<ul style="list-style-type: none"> • Must be at least six (6) alphanumeric characters in length. • Must contain at least one (1) number. • Must contain at least one (1) character. • Must be different from the last password used. • Must be updated at least every 90 days (staff only). • Are case-sensitive. 	
	3.5.2 Passwords Creation – User accounts	Users
	<ul style="list-style-type: none"> • Passwords must remain confidential. • Passwords should not be written down on the front of the machine or other obvious locations. • Passwords must not be shared. • Users should choose a password that cannot be easily guessed or predicted. • Users should change their password if it becomes known by another person. • A good password must be chosen to prevent unauthorised use and access to other accounts and systems. • If access to another user's data is required then the network administrator must provide this access. (Please refer to the University's guidelines on passwords)	
	3.5.3 Unacceptable passwords	Users
	<ul style="list-style-type: none"> • a dictionary word (even if written backwards) • The user's name or nickname, address, phone number, date of birth, etc. • someone else's name or character name • two words joined together • place names • acronyms • slang 	
	3.5.4 Systems passwords	
	Adequacy of the systems administrator and support personnel passwords for designated servers	ITS
4	Wireless Access	
4.1	Wireless access to University systems is provided at all campuses. Access will:	ITS
	4.1.1 require appropriate 802.11abg hardware	
	4.1.2 be provided via WPA2 infrastructure	
	4.1.3 only be provided to approved user accounts and:	

	4.1.4 must only be used for activities that are directly related to the University	User
5.	Internet/Intranet Access	
5.1	Outgoing Connections	
	5.1.1 Prior arrangements must be made with ITS before access from the Internet to any systems within the Swinburne network become available.	User
	5.1.2 Prior arrangements must be made with ITS before access from any systems within Swinburne network to the Internet become available.	User
5.2	Changes to Firewall Policy	
	5.2.1 Requests for changes to the firewall policy must be put forward to ITS in writing, outlining the reason for the request. The risk of opening the Firewall to accommodate the request will be evaluated.	User
	5.2.2 By requesting additional services to be made available through the firewall, staff and the faculty accept responsibility to maintain the integrity of the host machines.	Staff/School
	5.2.3 Re-assess the access policy on an annual basis.	ITS
5.3	Suspect Information	
	All information taken off the Internet should be considered suspect until confirmed by separate information from another source.	
5.4	Contacts Contacts made over the Internet should not be trusted with University information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal University information.	User
5.5	Privacy	
	Staff using University information systems and/or the Internet should realise that their communications are not automatically protected from viewing by third parties. Unless encryption is used staff should not send information over the Internet if they consider it to be private.	User
6.	Operating system and database access	
6.1	Secure access to operating systems and databases on the servers at enterprise level.	Manager, Information Technical Services
6.2	Access to the database management system will be limited to the database administrator.	Database Administrator
6.3	Maintenance and backup of Desktop databases are the direct responsibility of the owner of the database.	Database Owner

SUPPORTING DOCUMENTATION

Forms and Records Management

Form	Retention Time	Retention Location
Change Control Form		IT Service Desk
H1S-Network Account Form		Human Resource Department

Related Material

Name	Location	Document Type
Computing Equipment Backup	http://ppd.swinburne.edu.my	Policy
Information Technology Systems Acceptable Use Policy	http://ppd.swinburne.edu.my	Policy
Password Guidelines	http://www.its.swinburne.edu.au/qas/passwords.htm	
Standards Australia - AS/NZS 7799.2:2000 (Previously known as 4444.2) : Information security management - Specification for information security management systems	http://www.standards.org.au/	

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
University Management, Information Support Services

KEYWORDS
Information technology, Security