



COMPUTER ROOM ACCESS POLICY

Date approved:	21 July 2003	Date Policy will take effect:	On Approval	Date of Next Review:	
Approved by:	Pro Vice-Chancellor (Information Technology)				
Custodian title & e-mail address:	Communications Technical Officer peter_hill@uow.edu.au				
Author:	Peter Hill				
Responsible Faculty/ Division & Unit:	Networks and Facilities Unit, Information Technology Services				
Supporting documents, procedures & forms of this policy:	Application for Temporary Access to ITS Communication and Computer Rooms				
References & Legislation:	IT Acceptable Use Policy (including Requirements Governing the Use of IT Facilities) Crimes Act, 1914 (Commonwealth) Occupational Health and Safety Act, 2000 (NSW) Occupational Health and Safety Regulation, 2001 (NSW) Student Conduct Rules				
Audience:	Public – accessible to anyone				
Expiry Date of Policy:	Not applicable				



Contents

1 Purpose of Policy.....	2
2 Definitions.....	3
3 Application & Scope.....	3
4 Revision	3
5 Executive Summary.....	3
6 Objectives.....	4
7 Providing Access.....	4
8 Administration and Implementation.....	7
9 Roles & Responsibilities.....	7
10 Version Control and Change History.....	7
Appendix 1 - Computer Room Access Requirements.....	9

1 Purpose of Policy

1. This is policy sets the controls and requirements that govern access to computer rooms operated by Information Technology Services.
2. There are several intended audiences for this document.
 - 2.1. University directors, managers and auditors who are concerned with the directions and strategies being employed to protect the security of the University's information technology assets.
 - 2.2. The wider University community who may have a general interest in information technology security operations.
 - 2.3. Staff and contractors of the University of Wollongong who need to enter a computer room to carry out their authorised duties.
3. This policy is required because of the increased need to provide both access and high levels of security to The University of Wollongong's core business computer systems and the data that is held in those systems.
4. The policy outlines the requirements needed for both permanent and temporary access to the University of Wollongong key data centres, how access is given and the requirements of both the personnel giving access and those with access.
5. It all so covers record keeping, advance notification, requirements, hours of access and visitors.
6. Requirements for people entering computer rooms have been developed in conjunction with this policy. These are included in Appendix 1. Individuals granted access to a computer room must comply with these requirements.
7. The University of Wollongong is committed to the appropriate use of Information Technology and Services in support of its teaching, research, administrative and service functions. This policy is an adjunct to the University's IT Acceptable Use Policy which defines the acceptable behaviour expected of users and intending users of the facilities. The University requires users to accept the IT policies and associated Requirements Governing the Use of IT Facilities as a condition of their use. These are accessible on the University Policy Directory.



2 Definitions

Word/Term	Definition (with examples if required)
University	University of Wollongong
User	Any person using any of the University's Information Technology Facilities
IT facilities	Information Technology facilities operated by the University, whether owned or leased
Chief Technology Officer	The Chief Technology Officer, Information Technology Services
ITS	Information Technology Services at the University of Wollongong
The room	For the remainder of this document refers to the following areas: Building 17 computer room. Building 15 DR room. Building 15 Voice server room. Building 36 computer room.

3 Application & Scope

1. This policy applies to computer rooms operated by Information Technology Services. Computer rooms are installations used to house computer and network hardware that are used to provide information technology services. Currently this applies to the following rooms:
 - Building 17 computer room.
 - Building 15 DR room.
 - Building 15 Voice server room.
 - Building 36 computer room.
2. For the remainder of this document the term "the room" refers to the above rooms

4 Revision

1. This document is maintained by the ITS Facilities Officer. Suggested changes may be submitted in writing detailing suggested emissions or additions and referencing section names or numbers where appropriate.
2. This document shall be reviewed by the Senior Manager Network & Facilities periodically.

5 Executive Summary

1. This is the policy governing requirements and access to computer rooms operated by Information Technology Services. It establishes the process to authorise people to access computer rooms in the following situations:
 - a. permanent access;
 - b. temporary access; and
 - c. emergency access.
2. It establishes the following requirements:
 - a. that details requirements of people entering computer rooms;
 - b. ITS staff responsibility; and



- c. record keeping requirements.

6 Objectives

1. To enable people to enter “the room” where necessary to carry out their authorised duties.
 - a. to identify the person;
 - b. to verify their authority;
 - c. to record the access; and
 - d. to ensure continuity of data services.
2. To ensure people who enter the rooms only carry out their authorised duties and are supervised.
3. To establish requirements for conduct that must be observed by all people entering a computer room.
4. To ensure the safety and welfare of people entering the computer rooms.

7 Providing Access

Permanent

1. Permanent access to ITS computer rooms can only be authorized by the following Information Technology Services management:
 - a. The Associate Director of Information Technology Services.
 - b. The Senior Manager Network & Facilities, Information Technology Services.
2. The proximity card access system is maintained by The University Security office (in Buildings and Grounds). They shall only provide access to the room with written authorisation from the Director of Information Technology Services or the Senior Manager Network & Facilities, Information Technology Services. The ITS Facilities Officer will maintain the access register and coordinate the process.
3. This register includes the following.
 - a. the person’s name;
 - b. the unit or organizations the person is employed with;
 - c. the person who authorised the access;
 - d. the reason they have been provided this access;
 - e. the date which the access was authorised; and
 - f. the date to authorise access.
4. This register is reviewed six monthly by the Senior Manager Network & Facilities.

Temporary

5. People who require access to a computer room infrequently or frequently but do not satisfy the condition of being a staff member of the University may be permitted to enter a computer room. This includes visitors that may be being shown around the room.

Qualification

6. To qualify for this access each person must satisfy the following before each and every occasion they enter a computer room.
 - 6.1. They must be employed by the University or contracted to perform work by the University.
 - 6.2. They must give adequate time to allow Senior Manager Network & Facilities to arrange for any internal (ITS) staffing requirement to be met.



- 6.3. They must be authorised by either:
 - a. a professional systems or network administrator who has permanent access to the computer room. (refer to permanent access register), or
 - b. an ITS Senior Manager.
- 6.4. They must provide an acceptable form of identification. Such forms include University staff card, drivers licence, credit or bank card.
- 6.5. They must require access to the room to carry out their authorised duties.
- 6.6. Their reason for accessing the room must be verified to be valid and authentic. For example, if an air conditioning mechanic asks to gain access to the room it shall be verified with the staff member of Buildings and Grounds who organised their attendance.
- 6.7. All persons must complete a local induction session.
7. In addition to the above, visitors shall satisfy the following requirements.
 - 7.1. They must be accompanied at all times by a person who has a permanent authority to enter the computer rooms.
 - 7.2. They must not perform any work in the computer room.
 - 7.3. Their visit must not be of extended duration.
 - 7.4. They must wear the lanyard and carry the access card issued, for the duration of their visit.

Temporary Emergency Access

8. In the event of an emergency Security is authorized to provide temporary access.
9. Security is to remain on site until an authorized ITS staff member is on site.
10. In the event that the situation is resolved before an authorized ITS staff member is on site. The attending security should forward a report to ITS.
11. The authorized representative member called will need to complete a down time report on the emergency.

Record Keeping

12. A log shall be maintained that records each permitted temporary entry into the computer room. This log will be stored at Information Technology Services reception. It shall record the following for each entry:
 - a. the time and date that the entry into the room was permitted;
 - b. the name or location of the room;
 - c. the name of the sections of the computer room they are permitted to access;
 - d. the number of the lanyard and identity card they are provided with;
 - e. the time that the authority to enter the room will expire;
 - f. the time and date of return of the issued identity and proximity cards;
 - g. the name of the person entering the computer room;
 - h. the name of the company or the University unit that the person works for;
 - i. their reason for entering the computer room;
 - j. the name of the person who has authorised their work. Note that this may be different to the person who is authorising their entry into the room;
 - k. the form of identification that was used to verify their identity;
 - l. an indication that the person authorising their entry into the room has verified that the reason for entry is valid and authentic;



- m. the signature of the person authorising the entry into the room;
- n. the signature of the person entering the room indicating that they are aware of their requirements; and
- o. the name of the person authorising the entry into the room.

Authorising Entry

- 13. The person authorising a person to enter a computer room shall be responsible for the following:
 - a. to ensure that all of the conditions for qualification are satisfied;
 - b. to ensure that the permitted access has been properly logged as detailed in the section "Record Keeping";
 - c. to monitor activities of this person while they are within the computer room;
 - d. it should be noted that Senior ITS Management can authorise temporary access personnel to be exempt for the need to be monitored;
 - e. to ensure that the person permitted to enter the room has returned the lanyard and proximity card provided to them by the time their authority to be in the room expires.

Lanyard and Proximity Card

- 14. People who have been given a temporary authority to enter a computer room shall be provided with a numbered proximity access card attached to a coloured lanyard. The colour shall signify the individual computer room and sections of the computer room that the holder is authorised to access. This lanyard must be worn around the persons neck at all times whilst in a computer room and it must be clearly visible.
- 15. These lanyards and proximity cards shall be accessible only to people who are permitted by this policy to authorise temporary access to a computer room.

Hours of Access

- 16. Normally access is only permitted to a computer room during a weekday between the hours of 8:30am and 5pm. Access outside of these times shall require additional approval of the Senior Manager Network & Facilities.

Advance Notification

- 17. The temporary authorisation process described above involves demonstrating qualification of the conditions and recording information about the access. This policy is not intended to prohibit or significantly interfere with the timely delivery of services by University staff or contractors. This section provides for notifying Information Technology Services of required access to a computer room so that approval can be given in advance of the visit. This will avoid any delay for the person requiring access by ensuring that most of the necessary process has been completed before their arrival.
- 18. An application form for temporary access to ITS communication and computer rooms is available at <https://intranet.uow.edu.au/myit/forms/index.html>. The application form should be received by Information Technology Services no less than three working days before the access is required. The form will be reviewed by a person authorised to approve access. If the form is correctly completed and the access justified provisional approval will be given for this access. If the information is unacceptable the person who made the application will be advised that provisional approval has not been given.



8 Administration and Implementation

Compliance

1. The University treats misuse of its IT facilities seriously. Violations of the conditions of use of IT facilities may result in temporary or indefinite withdrawal of access, disciplinary action under the University's, or relevant entities, discipline procedures, and/or reimbursement to the University.
2. IT misconduct by students will be dealt with under the Student Conduct Rules. The Chief Technology Officer or their nominee will be the Primary Investigation Officer of allegations of IT misconduct by students. Detailed investigation procedures and the penalties that may be awarded to students engaging in IT misconduct can be found in the Student Conduct Rules.
3. A user's access will be withdrawn given a written request from an appropriate staff member of the sponsoring organisation. Access may also be withdrawn by ITS in response to a suspected policy violation.
4. A student whose IT access has been withdrawn as a result of an investigation under the Student Conduct Rules can appeal the decision or the penalty to the Student Conduct Committee. Otherwise, a user whose access has been withdrawn may request reconsideration of the decision by the Chief Technology Officer who shall consider the withdrawal with the relevant Senior Executive, Dean or Director or the University Librarian. Following this the Chief Technology Officer shall confirm the withdrawal or reinstate access.
5. Misuse or unauthorised use of University IT facilities may constitute an offence under the Crimes Act, 1914 (Commonwealth), and/or other pieces of State or Commonwealth legislation. Nothing in this policy or the Requirements Governing the Use of IT Facilities may be taken as in any way diminishing or removing a person's obligations to comply with the law, or their liability to prosecution and punishment under law.
6. Users are encouraged to report any misuse and any reports will be treated as confidential.

9 Roles & Responsibilities

1. This policy governs access to computer rooms operated by Information Technology Services. It is congruent with and authorised by the University's Information Technology Security Policy. It is not to contradict any other University policy. It is approved by the Director of Information Technology Services.
2. The Senior Manager Network & Facilities is responsible for the ensuring application and correct operation of this policy.

10 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	21 July 2003	Pro Vice-Chancellor (Information Technology)	First Version
2	5 September 2003	Pro Vice-Chancellor (Information Technology)	Included exchange of identifying document for lanyard & proximity card. Added sections "Hours of Access", and "Advance Notification".
3	25 July 2006	Chris Edmondson	Changes to 1,2.1.1.2, 2.1.1.3, 3, 4, 4.1, 5,6,7.1, and 7.2, 7.3 removed
4	21 August 2006	Chris Edmondson	Minor grammatical changes plus inclusion of rules
5	6 May 2009	Vice Principal	Migrated to UOW Policy Template as per Policy



		(Administration)	Directory Refresh
--	--	------------------	-------------------



Appendix 1 - Computer Room Access Requirements

1. The following requirements apply to all people granted permanent or temporary authority to enter a computer room.
 - 1.1. All persons are required to sign a statement indicating that they are aware of and understand these requirements.
 - 1.2. All persons must undertake a local induction before entering communication & computer rooms.
 - 1.3. All persons must, in the event of a fire alarm, follow directions of Building Wardens and Security staff.
 - 1.4. All persons must, in the event of injury or illness, contact University Security on 4900 or call Emergency Services on 0 000.
 - 1.5. Only authorised persons can enter communication & computer rooms.
 - 1.6. Before lanyard proximity cards can be issued for temporary access all appropriate paper work must be completed.
 - 1.7. Authorised temporary persons must clearly display lanyard & proximity card.
 - 1.8. Lanyard & proximity card are not to be taken of site.
 - 1.9. Lanyard & proximity card are to be returned to ITS by end of business (17:30hrs) on the day of issue unless authorised by ITS Senior Management.
 - 1.10. The lanyard & proximity card has been issued to allow access for one authorised person. The authorised person is not permitted to grant access into ITS Communication & Computer Room areas to unauthorised person(s).
 - 1.11. All persons are expected to work safely at all times, in line with their obligations under the Occupational Health and Safety Act, 2000 (NSW) and the Occupational Health and Safety Regulation 2001 (NSW) as well as relevant Codes of Practice and Australian Standards.
 - 1.12. Services must not be isolated unless senior ITS management, has given permission in writing.
 - 1.13. In the event that an emergency arises from work being undertaken, you must notify ITS Systems staff and University Security staff immediately.
 - 1.14. No food, drink or smoking allowed in communication & computer rooms.
 - 1.15. All changes must be updated in log books.