



# IT SERVER SECURITY POLICY

<b>Date approved:</b>	17 March 2005	<b>Date Policy will take effect:</b>	17 March 2005	<b>Date of Next Review:</b>	
<b>Approved by:</b>	Vice Chancellor				
<b>Custodian title &amp; e-mail address:</b>	Deputy Vice Principal (Finance and IT)				
<b>Author:</b>	Rodd Jefferson				
<b>Responsible Faculty/ Division &amp; Unit:</b>	Information Technology Services				
<b>Supporting documents, procedures &amp; forms of this policy:</b>					
<b>References &amp; Legislation:</b>	<a href="#">IT Acceptable Use Policy (including the Requirements Governing the Use of IT Facilities)</a> <a href="#">Student Conduct Rules</a> <a href="#">Crimes Act, 1914 (Commonwealth)</a>				
<b>Audience:</b>	Public – accessible to anyone				
<b>Expiry Date of Policy:</b>	Not applicable				

## Contents

<a href="#">1 Purpose of Policy.....</a>	<a href="#">2</a>
<a href="#">2 Definitions.....</a>	<a href="#">2</a>
<a href="#">3 Application &amp; Scope.....</a>	<a href="#">2</a>
<a href="#">4 Policy Principles.....</a>	<a href="#">2</a>
<a href="#">5 Minimum Server Security Standards .....</a>	<a href="#">3</a>
<a href="#">6 Administration and implementation.....</a>	<a href="#">4</a>
<a href="#">7 Roles &amp; Responsibilities.....</a>	<a href="#">4</a>
<a href="#">8 Version Control and Change History.....</a>	<a href="#">4</a>



## 1 Purpose of Policy

1. This policy governs server security and minimum server standards. It should be reviewed in conjunction with the other IT infrastructure policies that are accessible on the University Policy Directory.
2. 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. The University's IT Acceptable Use Policy defines the acceptable behaviour expected of users and intending users of the facilities. The University requires users to accept the IT policies and the 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
University Network	The network infrastructure used by the University of Wollongong including all network services on main campus, satellite campuses, and wholly owned subsidiaries with trusted access to UOW services.
Servers	<p>Any and all servers providing services to one or more users, and hosted on a Microsoft Windows NT, 2000, or 2003 platform, and variations of Linux, Unix and Apple platforms.</p> <p>Servers have been defined, in terms of risk assessment, into three categories, as follows:</p> <ul style="list-style-type: none"> <li>• Critical servers, including servers hosting data of corporate sensitivity, including web services, financial, student or staff information.</li> <li>• User account services or servers hosting user accounts and passwords.</li> <li>• Non-Core Research and Teaching Servers used for research and teaching activities.</li> </ul>

## 3 Application & Scope

1. The server security policy applies to all users of the University of Wollongong IT facilities. This policy represents the University Institutional position and takes precedence over other relevant policies which may be developed at a local level.
2. All users should be aware of the policy, their responsibilities and legal obligations. All users are required to comply with the policy and are bound by law to observe applicable statutory legislation.

## 4 Policy Principles

1. The following general principles apply to usage of IT facilities:



- 1.1. All Critical servers, as defined above, will be centrally supported by ITS, and hosted in the ITS machine room. Where compliance to minimum server security standards can be achieved, some critical servers may continue to reside and be supported by local IT department and faculty staff, but these will be reviewed on a case-by-case basis.
- 1.2. All servers, including but not limited to critical servers, will comply with the minimum server security standards as outlined under Minimum Server Security Standards below.
- 1.3. All new servers planned for deployment onto the University of Wollongong network must first be registered with ITS, and must also comply with the minimum server security standards as outlined under Minimum Server Security Standards below.
- 1.4. Inability to comply with these minimum server standards will result in either:
  - a. Migration of server into central management model;
  - b. Increase and restrict access using available firewalling and networking technology; or
  - c. Decommissioning of server or isolation from the network in extreme circumstances.
- 1.5. ITS will, from time to time, conduct routine vulnerability scanning of Servers connected to the University of Wollongong network. Servers that are found to be vulnerable as part of this scan will be reported to local IT staff for immediate action.
- 1.6. All servers identified as compromised by any vulnerability scan will be subject to the practices of the University's IT Intrusion Response Plan.

## 5 Minimum Server Security Standards

1. For all servers connected to the University network, the following minimum server standards and procedures apply.

### Prior to installation / deployment to production:

2. Access requirements and function of server are reported to ITS (to ensure firewall rules and IP address allocation can be used to best protect device).
3. The physical location of server is confirmed to be sufficient (power, air-conditioning, physical security of device, OH&S requirements).
4. Specific technical staff are nominated with sufficient technical skills in server management to ensure that the server can be supported post-production. This may or may not include third party support arrangements.
5. The appointed technical staff member must subscribe to the server mailing list as a means for ongoing communication with ITS.
6. The appointed technical staff member must have an appropriate level of server training and experience in supporting the server platform.

### Upon installation

7. The server must be locked down or hardened, i.e., services not required are disabled on the server as per procedures which can be obtained from the ITS Security Officer.
8. User accounts must be managed in terms of password and username controls (password strings, password ageing, password expiry dates) as well as level of access as per procedures which can be obtained from the ITS Security Officer.
9. The number of administrator accounts is to be kept to a minimum.
10. Backup requirements are documented and coordinated with ITS as appropriate.

### Ongoing

11. Points covered under clauses 5.2 – 5.10 inclusive continue to apply.
12. All patches, especially security updates are applied as soon as possible.



13. Daily review of log areas (web logs, event logs, access logs) is conducted by the local technical staff member.
14. The server hardware is kept up to date such that the operating system installed is always current according to the server platform release schedule.
15. Servers must be managed in accordance with the Music, Video and Software Piracy Policy accessible on the University Policy Directory.

## 6 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.

## 7 Roles & Responsibilities

1. Roles and responsibilities are as detailed in this policy.

## 8 Version Control and Change History

Version Control	Date Effective	Approved By	Amendment
1	17 March 2005	Vice Chancellor	First Version
2	6 May 2009	Vice Principal (Administration)	Migrated to UOW Policy Template as per Policy Directory Refresh