UNIVERSITY
OF WOLLONGONG
AUSTRALIA

IT SERVER SECURITY POLICY

Date first approved: 17 March 2005	**Date of effect:** 17 March 2005	**Date last amended:** (refer Version Control Table)	**Date of Next Review:** August 2024
First Approved by:	University Council		
Custodian title & e-mail address:	Cyber Security Manager it-security@uow.edu.au steve@uow.edu.au		
Author:	Cyber Security Manager, Infrastructure, IMTS		
Responsible Division & Unit:	Information Management & Technology Services (IMTS)		
Supporting documents, procedures & forms of this policy:	Cyber Security Policy		
Relevant Legislation & **External Documents:**			
Audience:	Public		

Submit your feedback on this policy document using the Policy Feedback Facility.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Contents

1 Purpose of Policy 3

2 Definitions 3

3 Application & Scope 4

4 Policy Principles 4

5 Exemptions 6

6 Compliant and Non-compliant Servers ..... **Error! Bookmark not defined.**

7 Responsibilities 7

8 Version Control and Change History 9

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

1 Purpose of Policy

1. The purpose of this policy is to outline practices for administering servers that will ensure an acceptable risk posture against real-world threats. The aim is to defend servers against cyber security threats in a practical and pragmatic manner.

2 Definitions

Word/Term	Definition (with examples if required)
Cyber Security Team	Capability appointed by the Director, IMTS. Responsibilities of the Cyber Security Team are outlined in the Cyber Security Policy.
Director, IMTS	Director, Information Management & Technology Services
NTP	Network Time Protocol
Server	A computer or device which provides services over a network and is configured to allow access by multiple users. The following examples qualify as a server under this definition for the purpose of this policy: • A physical or virtual server running in a University data centre offering a web application component • A desktop computer with file sharing enabled that is accessed by a number of people • A building controller device that is accessed over the network by a management server • A virtual server instance running in a public cloud that is operated by or for the University
Service	A data storage, manipulation, presentation, communication or other capability which is implemented using a client-server or peer-to-peer architecture based on network protocols running at the application layer of a network. For example any web based application which may be supported by several Servers offering front and backend data processing and storage.
Business Owner	An individual within the University who is nominated to assume responsibility for a Service and is authorised to make business decisions with regard to the Service.
Server Administrator	An individual role or team who is nominated to administer particular servers. Must have sufficient technical skills and experience to ensure Servers are supported and administered properly. This may include third party support arrangements.
Service Owner	An individual role or team within the University who is nominated to assume responsibility of a Service and is authorised to make technical decisions with regards to the Service.
Server Registry	An information system maintained by Information Management & Technology Services in the style of a configuration management database that documents servers in scope of this policy.
University	University of Wollongong and controlled entities.

University Network	The network infrastructure used by the University including all network services on main campus, satellite campuses, and controlled entities.
User	A person assigned a User Account by the University or a person who is otherwise authorised to use University IT Facilities and Services.
User Account	An identity assigned to a User, with an associated username, for the purpose of accessing IT Facilities and Services that require authentication by the User.

3 Application & Scope

1. This Policy applies to:
    a. Servers that are connected to a University network; and
    b. Servers that are operated for or on behalf of the University regardless of which network they are connected to.
2. This policy does not apply to Services that are procured as the "software as a service" model but does apply to other cloud models of procurement such as "infrastructure as a service" and "platform as a service".

4 Policy Principles

Server Registry

1. An inventory of Servers ('Server Registry'), in the style of a configuration management database, will be maintained to assist with applying this policy. The Server Registry documents each Server's compliancy status, operating system platform, associated Services it supports, and application software in use.

Secure Operating System and Software

2. The Servers operating system and other software must be configured to prevent security weaknesses both upon initial deployment and ongoing.
3. Critical security patches must be applied within 30 days of release from the vendor.
4. The requirements of clauses 4.4 and 4.5 can be achieved with the following practices:
    a. using an industry standard check list to configure the operating system and software. This process is often referred to as hardening and involves such things as disabling unnecessary accounts, disabling unnecessary services, configuring non-executable stacks and heaps, enabling host based firewalls and so forth;
    b. implementing automated patching tools and processes that ensure security patches are installed for both applications and for operating system software; or
    c. moving to the latest software versions when old versions are no longer supported with patches.

Data Recovery Capability

5. At minimum, the data associated with the service needs to be recoverable in the event of an incident or disaster. Process and tools must be used to properly back up important data and a methodology for timely recovery must be proven.

6. This backup methodology must be tested by the Service Owner at least annually. If the same backup system is used for a number of applications at least one of these applications must be recovery tested by the Service Owner annually.

Malware Defences

7. Tools and processes are used to detect, prevent and correct installation and execution of malicious software on servers.
8. This can be achieved with the following practices:
    a. implementing relevant specialist anti-malware software that provides anti-virus, anti-spyware, and host based intrusion prevention;
    b. configuring servers to not auto-run content from removable media such as USB tokens, drives and DVDs etc; or
    c. enabling anti-exploitation features such as data execution prevention, address space layout randomisation, virtualisation / containerisation, etc.

Continuous Vulnerability Assessment and Remediation

9. The Cyber Security Team is responsible for regularly scanning to detect vulnerabilities on Servers and for communicating vulnerability assessments with the Service Owner and Server Administrator.

Limit and Control Network Ports, Protocols and Services

10. The Server only runs network services, protocols and ports that are necessary to achieve its business purpose.
11. This can be achieved with the following practices:
    a. disabling any service that is not needed; or
    b. applying host-based firewalls with a default deny rule that drops all traffic except those services and ports that are explicitly allowed. If a server is not accessed over the internet a network firewall should prevent it being visible from internet.

Controlled Use of Administrative Privileges

12. Administrative privileges must be minimised and only used when required. A high standard of security is applied to privileged accounts. These privileges must be reviewed by the Cyber Security Team at least annually.

Maintenance, Monitoring and Analysis of Audit Logs

13. Application and operating system audit and event logs are configured and maintained in a useful state. For important servers the logs are monitored either automatically or manually.
14. All authentication and account and group management events must be logged.
15. These logs must be retained for a minimum of 2 years.
16. Effective logging includes the following:
    a. Server system clock is kept accurate and synchronised;

b. log settings include date, time, source and destination addresses and other useful information;

c. storage space is sufficient to meet retention requirements; and

d. logs are rotated and retained as required.

Account Monitoring and Control

17. System and application User Accounts are tracked and controlled by the relevant faculty or division to ensure old and unnecessary accounts are removed and unable to be used for unauthorised access. When staff or contractors leave the University or change roles their accounts are restricted and removed in accordance with the IT Acceptable Use policy and IT User Account Management Procedures.

18. Where possible servers should be configured to automatically forward logs to an IMTS central log server.

19. As a condition of use, Users must agree to comply with IT Acceptable Use Policy and other IT policies.

Compliant and non-compliant Servers

20. Individual Servers are deemed to be compliant with this policy when the following are confirmed:

    a. responsibilities have been assigned for Service Owner, Business Owner and/or Server Administrator;

    b. the business purpose of the server and key risk areas are recorded; and

    c. the Server Administrator and Service owner have confirmed that the policy principles have been adequately met and a compromise or other incident involving the server is unlikely to cause the University unreasonable damage.

21. A Server is deemed non-compliant when the above has not been met or following an unsatisfactory audit or vulnerability scan. The identification of Non-compliant Servers may result in either:

    a. resolution of non-compliance

    b. migration of Server into central management model;

    c. access to Server limited with network firewall technology; or

    d. decommissioning of the Server or isolation from the network in extreme circumstances.

5 Exemptions

1. The Director, IMTS or delegated authority may approve an exemption where it is impractical to satisfactorily comply with this policy in whole or part and it is demonstrated that the risk is acceptable. These exemptions may be granted for an individual Server or a class of Server or device.

2. Individual Server exemptions will be recorded in the Server Registry. Exemptions applying to a class of device will be recorded.

3. Examples of individual exemptions include, but are not limited to:

    3.1. A device exempted from complying with principles of malware defence and maintenance, or monitoring of audit logs because there is simply no provision to achieve these.

3.2. An instrument controller may be permitted to remain on a legacy operating system if it is impractical to upgrade and sufficient firewall controls are used to minimise risk of remote compromise.

4. Examples of class exemptions include, but are not limited to:

4.1. CCTV cameras exempted from being individually identified in the Server registry and instead are treated as a single Server class as their management and configuration is uniform.

4.2. Desktops offering remote desktop service exempted because network controls minimise exposure of the service.

6 Roles & Responsibilities

Director, IMTS

1. The Director IMTS has the following responsibilities:

    a. approving exemptions for individual Servers or a class of Server or device;

    b. approving complementary operational procedures and standards to support this policy; and

    c. approving Service Owner role.

Cyber Security Team

2. The Cyber Security Team has the following responsibilities:

    a. advocating and ensuring stakeholders are aware of their responsibilities and available support;

    b. maintaining the Server Registry;

    c. conducting audits on servers from time to time involving the Service Owner and Server Administrator to ensure compliance with this policy; and

    d. undertaking routine network vulnerability scanning and reporting results to the Service Owner and Server Administrator. Every effort will be made to prevent vulnerability scans from interfering with the normal operation of Servers.

Service Owner

3. The Service Owner has the following responsibilities:

    a. communicating with the Cyber Security Team the business purpose of the Server, any key risk areas and other information required for the Server Registry;

    b. appointing a Server Administrator with sufficient technical skills and experience to ensure Servers are supported and administered properly. This can include third party support arrangements; and

    c. ensuring the provisions of this policy have been adequately met and a compromise or other incident involving Servers is unlikely to cause the University unreasonable damage.

Business Owner

4. The Business Owner has the following responsibilities:

a. communicating business decisions to the relevant individuals or teams within IMTS to ensure the provisions of this policy are adequately met.

Server Administrator

5. The Server Administrator has the following responsibilities:

    a. ensuring the provisions of this policy are adequately met for the Servers being maintained;

    b. maintaining sufficient records to indicate the application of this policy; and

    c. communicating with the Cyber Security Team to assist with the effective operation of this policy.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

7 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
3	9 March 2010	Vice-Principal (Administration)	Future review date identified in accordance with Standard on UOW Policy
4	1 March 2011	NA	Updated links to Related Documents
5	30 Nov 2012	Vice-Principal (Administration)	Updated to reflect change from OHS to WHS
6	4 November 2013	Chief Administrative Officer	Updated to reflect title change from University Librarian to Director, Library Services.
7	30 January 2014	Vice-Chancellor (VCAG)	Updated University nomenclature
8	9 December 2016	University Council	Major review of IT Policy suite
9	19 August 2020	Chief Operating Officer	Administrative amendments as an outcome of review.