# IT Server Security Policy

# Section 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.

# Section 2 - Application and Scope

(2) This Policy applies to:

a. servers that are connected to a University network;
b. servers that are operated for or on behalf of the University regardless of which network they are connected to; and
c. infrastructure as a service and platform as a service.

(3) This Policy does not apply to services that are procured as the “software as a service”.

# Section 3 - Policy Principles

### Server Registry

(4) 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. The following examples qualify as a server under this definition for the purpose of this Policy:

a. a physical or virtual server running in a University data centre offering a web application component;
b. a desktop computer with file sharing enabled that is accessed by a number of people;
c. a building controller device that is accessed over the network by a management server; and
d. a virtual server instance running in a public cloud that is operated by or for the University.

### Secure Operating System and Software

(5) The server’s operating system and other software must be configured to prevent security weaknesses both upon initial deployment and on an ongoing basis.

(6) Operating system and application security patches must be applied in line with the requirements of the ACSC's essential eight strategies to mitigate cyber security incidents.

(7) These requirements 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 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

(8) 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.

(9) 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

(10) Tools and processes are used to detect, prevent, and correct installation and execution of malicious software on servers.

(11) 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

(12) 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

(13) The server only runs network services, protocols and ports that are necessary to achieve its business purpose.

(14) 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

(15) 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.

(16) Ensure secrets relating to administrative access are changed when deemed appropriate, e.g. when administrative staff have left or if the Secrets have not been changed for more than 2 years.

## Maintenance, Monitoring and Analysis of Audit Logs

(17) 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.

(18) All authentication and account and group management events must be logged.

(19) These logs must be retained for a minimum of 2 years.

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

(21) Effective logging includes:

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

(22) 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 cannot 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.

(23) As a condition of use, users must agree to comply with the IT Acceptable Use Policy and other IT policies.

(24) Any external service or system requiring outbound email to be sent on behalf of the University, must use an appropriate subdomain with email security applied (such as DMARC).

(25) Business and technical system owners who own or manage systems and applications that send email must engage IMTS to assess and implement.

## Compliant and Non-compliant Servers

(26) Individual servers are deemed considered 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 that a compromise or other incident involving the server is unlikely to cause the University unreasonable damage.

(27) A server is deemed considered non-compliant when the above has not been met or following there has been 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.

# Section 4 - Exemptions

(28) The Chief Information Digital Officer, 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.

(29) Individual server exemptions will be recorded in the server registry. Exemptions applying to a class of device will be recorded.

(30) Examples of individual exemptions include, but are not limited to:

a. 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; or
b. 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.

(31) Examples of class exemptions include, but are not limited to:

a. 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; or
b. desktops offering remote desktop service exempted because network controls minimise exposure of the service.

# Section 5 - Roles and Responsibilities

(32) The Chief Information Digital Officer 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.

(33) 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.

(34) 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.

(35) 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.

(36) 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.

# Section 6 - Definitions

| Word/Term | Definition (with examples if required) |
|---|---|
| ACSC | Australian Cyber Security Centre |
| NTP | Network Time Protocol |
| Secrets | Key phrase or information used to form passwords for UOW Systems. |
| 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:<br>A physical or virtual server running in a University data centre offering a web application component<br>A desktop computer with file sharing enabled that is accessed by a number of people<br>A building controller device that is accessed over the network by a management server<br>A virtual server instance running in a public cloud that is operated by or for the University |
| Service | A data storage, manipulation, presentation, communicationcommunication, 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 exampleexample, 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. |

## Status and Details

| | |
|---|---|
| **Status** | Current |
| **Effective Date** | 13th December 2023 |
| **Review Date** | 13th December 2028 |
| **Approval Authority** | University Council |
| **Approval Date** | 13th December 2023 |
| **Expiry Date** | Not Applicable |
| **Responsible Executive** | Adam Malouf<br>Chief Operating Officer and Vice-President Operations |
| **Responsible Officer** | Ray Coury<br>Chief Information Digital Officer |
| **Enquiries Contact** | Information Management and Technology Services<br>+61 2 4221 3000 |