Murdoch University

ICT Security Policy

Purpose and Scope

To ensure the appropriate controls are in place to protect information owned or entrusted to the University, and its Information Technology and Communications Systems.

This policy applies to all staff and students, tenants, contractors, visitors, and the public.

Murdoch University's Information Technology (IT) systems are provided for the purposes of teaching, learning, research, engagement, and administration in support of the University's vision and are integral to the effective performance of its operations. Effective IT security is essential to ensure the University meets its obligations for security, privacy, and preservation of intellectual property.

This policy applies to **all** Murdoch University IT systems and users.

Objectives:

1. To maintain the Confidentiality, Integrity, Availability and Accountability of Murdoch University Information Technology (IT) resources and all Murdoch University assets.
2. To establish requirements for IT Security within the University, including the physical security of computer/server rooms and the authorisation and management of user access to University IT systems.
3. To establish requirements for the management of Information Security.

Roles and Responsibilities:

Different levels of University staff have different levels of responsibility in relation to this policy as outlined below:

1. The Director IT Services through the Associate Director, Planning and Governance is responsible for approving all policies related to IT Security.
2. The Manager, Information Security and Risk is responsible for providing leadership and oversight to the effective development of IT Security Strategy, and risk management.
3. All Information Technology Services Managers and their teams are responsible for the implementation of the ITS Security Strategy and associated initiatives.

4. All individuals and organisations identified in the scope of this policy are responsible for ensuring the preservation of confidentiality, integrity, and availability of the University's Information Security.

Policy

1. In this policy, the following words have the following meanings:

   1.1. "Critical ICT System" means systems that are deemed critical to the operation of Murdoch University.

2. IT Security Requirements

   2.1. IT systems must contain controls to preserve:

      2.1.1. **Confidentiality**: information is not disclosed to other parities without authorisation;

      2.1.2. **Integrity**: information cannot be altered by other parties without authorisation;

      2.1.3. **Availability**: of critical information when required; and

      2.1.4. **Accountability**: of individuals or parties breaching IT Security.

   2.2. University IT systems must be secured by appropriate access control and authentication mechanisms.

   2.3. No individual or party shall attempt to circumvent the University's authentication mechanisms without justification and prior authorisation from the Director Information Technology Services.

   2.4. University IT systems must be monitored and use effective malicious software management systems as described in the ICT Security Standard.

   2.5. Critical IT systems must have effective backup regime that is documented and tested periodically.

   2.6. All IT system's passwords must comply with the University's Password Policy.

   2.7. All authentications must have Mutli Factor Authentication enabled unless it is not possible due to technical or procedural restrictions. All exceptions must be approved and registered by the IT Security team or delegate.

   2.8. Critical IT system logs must be time stamped using the time synchronization methods described in the ICT Security Standard.

   2.9. Network devices connected to University communications systems must be secure and comply with network security provisions of the ICT Security Standard.

   2.10. Use of all IT systems must comply with the IT Conditions of Use Policy.

   2.11. All IT security incidents must be managed in accordance with the Information Security Incident Management Procedure.

2.12. Information Technology Services must undertake regular vulnerability assessments and periodic penetration testing across IT systems using appropriate tools. Where threats and vulnerabilities are identified, the risk will be evaluated and managed in accordance with the Vulnerability Management Procedure and document in the appropriate risk register.

2.13. Critical IT systems must have disaster recovery plans that are documented and regularly tested.

2.14. ITS assets must be recorded in the Configuration Management Data Base (CMDB) for the purpose of identification, classification, criticality, audit, and classified in accordance with the Data Classification Policy.

2.15. Annual, independent, IT security reviews must be undertaken to ensure risks and issues are identified, management and documented.

3. Physical Security Requirements

3.1. Computer/server rooms must be physically strong and reasonably free from risk of flooding, fire, vibration, dust and other natural threats.

3.2. Computer/server rooms must have adequate thermal, fire, and smoke detectors. Underfloor areas must have fire, smoke, and water detectors.

3.3. Computer/server rooms must employ mechanisms to control air temperature and humidly.

3.4. Combustible material such as paper, pack material etc must not be stored in computer/server rooms.

3.5. Critical ITS systems must be powered by sources able to run operations in the event of a power failure and have the ability to trigger orderly system shutdown.

3.6. Access to computer/server rooms must be restricted to authorised staff only. Computer/server rooms must be locked, secured, and protected by electronic access control systems and surveillance systems.

3.7. Server rooms that are not managed by Murdoch University but hold systems and services used by Murdoch University must meet a set of international and industry-specific compliance standards, such as ISO 27001 for assurance that the specified requirements are met.

3.8. Disposal of all ITS equipment must comply with the Digital Media Disposal Standard.

4. User Access

4.1. The level of access to IT systems must be:

4.1.1. No higher that required to perform the work applying the principle of least privileged in all cases

4.1.2. Authorised in accordance with the delegations of authority

4.1.3. Applied for and submitted through the Murdoch Support Service Management Portal;

4.1.4. Revoked immediately when access is no longer required.

4.2. Storage and retention of access requests and revocation to IT and communications systems must comply with the Recordkeeping Policy.

4.3. All user data requests must require approvals as described in the ICT Security Standard i.e. Murdoch Data Access Request Process.

4.4. IT and communications systems user accounts must comply with the Password Policy.

4.5. User accounts must be removed or disabled when a user terminates their employment or ceases to require system access.

4.6. The University reserves the right to limit, restrict, or extend access to IT and communication systems or information at the discretion of the Vice Chancellor or delegate.

4.7. The University reserves the right to monitor, inspect or search at anytime all University IT systems and information. This examination may take place with or with the consent, presence, or knowledge of the individual parties involved.

5. Change Management

5.1. All changes to Murdoch University's IT based resources including enterprise systems, operating systems, network and communications based devices and applications must follow appropriate change management processes such as the Information Security Change Management Guidelines, and be approved by the Change Advisory Board, Business Owners, and Information Technology Services.

5.2. Exceptions to the Change Management processes may apply during emergency situations such as a Critical Incident with approval.

6. External Service Providers

6.1. All outsourcing and hosting contracts between external providers and Murdoch University for services and equipment must be line with the University's Procurement Policy.

6.2. Business owners must monitor and review external provider's services at planned intervals to ensure appropriate security controls are implemented and maintained.

6.3. The responsibility for security of equipment deployed by external service providers and the data contained within such equipment must be clarified in the contract with the service provider and include all documentation of security contacts and escalation procedures.

Non-Compliance:

1. Violation of this policy may result in disciplinary action under relevant statues, policies, or other legal action. This may include removal of access to University information systems, withholding of results, expulsion or in the case of

employees, suspension or termination of employment as defined in the *Enterprise Agreement*.

2. The University retains the right to take down or disable any systems or services that are in violation of this policy at the discretion of the Vice Chancellor or delegate.

Governance

Approval Authority	Senior Leadership Team
Owner	Vice Chancellor
Legislation mandating compliance	
Category	Primarily a function of management
Related University Legislation and Policy Documents	Data Classification Policy Digital Media Disposal Standard ICT Security Standard Information Security Incident Management Procedure IT Conditions of Use Policy Password Policy Privacy Policy Procurement Policy (1001) Recordkeeping Policy Vulnerability Management Procedure Murdoch Support Service Management Portal – Access Request
Date effective	13/09/2023
Review date	13/09/2026

References:

ISO/IEC 27001 - Information Security Management Standard

The Australian Cyber Security Centre (ACSC) Information Security Manual (ISM)

Revision History

Approved/Amended	Date Approved	Resolution No. (if applicable)
Administrative Amendment	01/05/2024	
Approved	13/09/2023	
Approved	17/09/2022	
Approved	27/04/2018	
Approved by UniSec	20/09/2016	
Approved by COO	30/07/2014	
Approved	14/06/2010	

Please refer to the electronic copy in the Policy and Procedure Manager to ensure you are referring to the latest version.