ICT Security Policy

Printed copies are for reference only. Please refer to the electronic copy in the Policy and Procedure Manager (PPM), the electronic policy management system (EPMS), to ensure you are referring to the latest version.

Purpose:

To ensure the appropriate controls are in place to protect University's Information Technology and Communications Systems.

Audience:

Staff, Students, users of Murdoch University's Information and Communications Technology systems.

Preamble:

Murdoch University's Information and Communications Technology (ICT) 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 ICT 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 ICT systems and users.

Objectives:

- To maintain the Confidentiality, Integrity, Availability and Accountability of Murdoch University Information Technology (IT) resources and assets.
- To establish requirements for ICT Security within the University, including the physical security of data centres and the authorisation and management of user access to University ICT systems.
- To establish requirements for the management of Information Security.

Definitions:

Any defined terms below are specific to this document. The definition of common terms appears in the Murdoch University Dictionary of Terms.

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

Policy Statement:

1. ICT SECURITY REQUIREMENTS

1.1. ICT systems must contain controls to preserve:

1.1.1. **Confidentiality**, i.e. information is not disclosed to other parties without authorisation;

1.1.2. **Integrity**, i.e. information cannot be altered by other parties without authorisation;

1.1.3. **Availability** of critical information when required; and

1.1.4. **Accountability** of individuals or parties breaching IT security.

1.2. University ICT systems must be secured by appropriate access control and authentication mechanisms.

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

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

1.5. Critical ICT systems must have effective backup regime that is documented and tested periodically.

1.6. All ICT system's passwords must comply with the University's Password Policy.

1.7. Critical ICT system logs must be time stamped using the time synchronisation methods described in the ICT Security Standard.

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

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

1.10. All ICT security incidents are managed in accordance with the Information Security Incident Management Procedure.

1.11. Information Technology Services will undertake regular vulnerability assessments across ICT 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 documented in the appropriate risk register.

1.12. Critical ICT systems must have disaster recovery plans that is documented, and regularly tested.

1.13. IT assets must be recorded on an asset register for the purpose of identification, audit and investigation.

1.14. Annual, independent, IT security reviews will be undertaken to ensure risks and issues are identified, managed and documented.

2. PHYSICAL SECURITY REQUIREMENTS

2.1. Data Centres must be physically strong and reasonably free from risk of flooding, fire, vibration, dust and other natural threats.

2.2. Data Centres must have adequate thermal, fire and smoke detectors. Under floor areas must have fire, smoke, and water detectors.

2.3. Data Centres must employ mechanisms to control air temperature and humidity.

2.4. Combustible material (e.g. paper, packing material) must not be stored in Data Centres.

2.5. Critical ICT 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.

2.6. Access to Data Centres is restricted to authorised staff only. Data Centres must be locked, secured, and protected by electronic access control systems and surveillance systems.

2.7. Disposal of all ICT equipment must comply with the Digital Media Disposal Standard.

3. USER ACCESS

3.1. The Level of access to ICT systems:

3.1.1. is no higher than required to perform the work;

3.1.2. is authorised by an appropriate position;

3.1.3. is applied for and submitted on an official form; and

3.1.4. is revoked when access is no longer required.

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

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

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

3.5. User accounts must be removed or disabled when a user terminates his or her employment or ceases to require system access.

3.6. 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.

3.7. The University reserves the right to monitor, inspect, or search at any time all University ICT systems and information. This examination may take place with or without the consent, presence, or knowledge of the involved individuals or parties.

4. CHANGE MANAGEMENT

4.1. 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, and be approved by the appropriate governance body, business owners and Information Technology Services, except during emergency situation or Disaster.

5. EXTERNAL SERVICE PROVIDERS

5.1. All outsourcing and hosting contracts between external providers and Murdoch University for services and equipment must be in line with the University's Procurement Policy (1001).

5.2. Business owners will monitor and review external provider's services to ensure appropriate security controls are implemented and maintained.

5.3. 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 services provider and include all documentation of security contacts and escalation procedures.

Non-Compliance:

- Violation of this policy may result in disciplinary action under relevant statutes, 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.

Performance Indicators:

There are no performance indicators.

Related Documents:

Information Security Incident Management Procedure

Vulnerability Management Procedure

ICT Security Standard

Digital Media Disposal Standard

IT Conditions of Use Policy

Password Policy

Procurement Policy (1001)

Recordkeeping Policy

References:

There are no references.

Approval and Implementation:

Approval Authority:	Director Information Technology Services
Responsible Officer(s):	Director Information Technology Services
Approval Authority for supporting procedures:	Director Information Technology Services
Approval Authority for supporting standards:	Director Information Technology Services
Contact Officer:	Director Information Technology Services

Revision History:

Approved/ Amended/ Rescinded	Date Approved	Effective Date	Next Review Date	Resolution No. (if applicable)
Approved	27/04/2018		27/04/2021	
Approved by UniSec	20/09/2016		20/09/2019	
Approved by COO	30/07/2014		01/08/2017	
Approved	14/06/2010		14/06/2013	