Murdoch University

Information Security Incident Management Policy

Purpose and Scope

This policy ensures a consistent and effective approach to the management of Information Security Incidents.

This policy applies to all Staff, Students, tenants, contractors Staff, Students, tenants, contractors, visitors, public.

Objectives:

- To ensure a consistent and effective approach to the management of Information Security Incidents;
- To ensure consistent communication on security events and security weaknesses involving the University and/or the University's information technology resources;
- To enable efficient and effective management of information Security Incidents by providing a definition for an "Information Security Incident"; and
- To establish a structure for the reporting and management of such incidents.

Policy

1. Roles and Responsibilities

    1.1. All members of the University are responsible for reporting actual or suspected Information Security Incidents to the relevant internal contact as soon as possible in accordance with the Information Security Incident Management Procedure.

    1.2. Contractors using the University's information systems and services must, under the terms of their engagement, be required to note and report any significant Information Security weakness in those systems and services that they identify, in accordance with the Information Security Incident Management Procedure.

    1.3. The responsibility for responding to Information Security Incidents will be as set out in the Information Security Incident Management Procedure.

    1.4. The responsibility of reporting serious Information Security Incidents to external authorities lies with the authorised individual unless otherwise delegated in the Information Security Incident Management Procedure.

2. Policy Statement

2.1. All members of the University must be made aware of the procedure for reporting Information Security Incidents and their responsibility to report such incidents.

2.2. All Information Security Incidents must be reported promptly to the IT Service Desk and IT Security.

2.3. All Information Security Incidents must be managed in accordance with the Information Security Incident Management Procedure, including assessment of the severity of the incident and implementation of corresponding management response.

2.4. Key information about serious Information Security Incidents, including impact of the incident (financial or otherwise), must be formally recorded in writing in the matter specified in the Information Security Incident Management Procedure, and those records must be analysed in order to assess the effectiveness of the University's Information Security.

2.5. New risks identified as a result of an Information Security Incident must be assigned to the relevant risk custodian within the University, and unacceptable risks must be mitigated promptly in accordance with the University`s risk management processes.

2.6. Relevant staff must be trained in digital evidence collection, retention and presentation, in accordance with legislative or regulatory obligations.

2.7. Serious incidents must be reported to the appropriate external authorities where relevant by authorised individuals.

3. Non-Compliance

Failure to report an Information Security Incident and any other breach of this policy may be subject to disciplinary action, up to and including termination of employment.

Governance

Approval Authority	Senior Leadership Team
Owner	Chief Experience Officer
Legislation mandating compliance	
Category	Primarily a function of management
Related University Legislation and Policy Documents	*Information Security Incident Management Procedure*
Date effective	09/02/2026

Review date	09/02/2029

Revision History

Approved/Amended	Date Approved	Resolution No. (if applicable)
Approved	09/02/2026	
Approved	17/09/2022	
Reviewed no changes made	18/11/2019	
Approved	04/02/2016	

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