Australian National University

Policy: Information technology security

Purpose

To establish the framework for information technology (IT) security, systems, and operations that support the core functions of the University.

Overview

ANU is committed to ensuring appropriate security for all data, equipment, and processes within its domain of ownership and control.

Scope

The policy applies to all members of the University community who have been granted access to IT and information infrastructure, including but not limited to ANU staff, students, VaHAs, contractors and affiliated organisations.

Definitions

Authentication: the act of verifying the identity of a user, process or device as a prerequisite to allowing access to resources in an information system. Includes authentication measures such as passwords, passphrases and multifactor authentication.

Authorised user: a person who has been permitted access to all or part of the information infrastructure of the University by a responsible officer, as defined in the *Information Infrastructure and Services Rule 2020*.

Availability: the period for which information assets are available, which ensures their availability for their intended use.

Confidentiality: the process of limiting information access and disclosure to authorised users, in order to protect data and information from unauthorised access or use.

Data: includes raw data, micro data, unorganised facts or data sets in any format.

Information: data that is processed, organised, structured or presented in a given context so as to make it useful in any format.

Information infrastructure: includes buildings, permanent installations, information services, fixtures, cabling, and capital equipment that comprises the underlying system within or by which the University:

- holds, transmits, manages, uses, analyses, or accesses data and information; and

- transmits electronic communication.

Information security: preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information security risk: associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organisation.

Integrated Communication Network (ICN): the University network infrastructure including the following network sites – Acton Campus, ANU UniLodge, Hume Library Store, Gowrie Hall, Mount Stromlo Observatory, Siding Spring Observatory, North Australia Research Unit, University House Melbourne, ANU Medical School remote sites and hospitals, and ANU Exchange sites.

Multifactor Authentication: a security measure that requires two or more proofs of identity to allow a user to authenticate. Multifactor authentication typically requires a combination of something the user knows (PIN, secret question), something they have (phone, card, token) or something they are (fingerprint or other biometric).

Passphrase: a sequence of words used for authentication (e.g. pineapple Imagine 99).

Password: a sequence of characters or words used for authentication (e.g. ^Mhall.ifwwa*99btls). The use of the term password(s) also includes passphrase(s).

Personal Identification Number (PIN): a sequence of numbers used for authentication.

System owner: the senior member of staff with delegated responsibility for information assets including defined responsibilities for the security of the data, information and application component of the asset, determining appropriate classification of information, defining access rights, and ensuring that information asset risk is identified and managed. System owners are a Service Division Director or an equivalent management position.

University provided storage infrastructure: data storage systems that are provided by the University and supported by Information Technology Services (ITS).

User: a person (wherever located) who accesses the information infrastructure. This includes services intended for public use.

VaHA: Visiting and Honorary Appointments; formerly referred to as Persons of Interest (POIs).

Policy statement

1. This policy and related documents draw their authority from the *Information Infrastructure and Services Rule 2020*.

2. The University requires external network interconnectivity and the internet for its research, teaching and learning, public policy, outreach, and administration activities.

3. The University is committed to providing secure information infrastructure that protects the integrity and confidentiality of information without compromising its availability.

4. The University implements a framework for the management of information security and incident response.

5. Information security applies to all forms of information and data, be they digital, print, or other and includes the management of the software and/or communications technology systems and networks for storing, processing, and communicating information.

6. ANU is committed to ensuring the security of all information technology, data, equipment, and processes within its ownership and control.

7. The University remains the owner of University data regardless of the ownership of the device.

8. The University reserves the right to refuse, prevent or withdraw access to authorised users and/or particular devices or software.

9. The University reserves the right to modify user access to data, in line with the Infrastructure security classification standard.

10. The University has a dedicated Information Security Office (ISO) and Chief Information Security Officer (CISO). The mission of the ISO is to keep the ANU safe and credible through the delivery of coherent and sustainable capabilities aimed at building world-class information security infrastructure and culture.

University responsibilities

11. The University takes appropriate action to protect, preserve, and keep available and accessible, its IT and information infrastructure, including the managed end-to-end network.

12. The University provides and is responsible for:

a. identifying, managing and mitigating risk across the University's IT and information infrastructure;

b. coordinating all information security activities required to ensure the security of IT and information infrastructure;

c. providing network security to protect the University's information sources, electronic resources, intellectual property, and network access;

d. applying security updates to software and operating systems to minimise security vulnerabilities; and

e. ensuring periodic audits of areas to ensure compliance with relevant policies and procedures.

System owner responsibilities

13. All information technology systems have a system owner. System owners:

a. ensure systems and applications are documented, classified, and secured in accordance with the Infrastructure security classification standard;

b. identify and manage disaster recovery and business continuity requirements for their systems;

c. ensure that all changes to infrastructure are managed through the Change Advisory Board and that only authorised changes are made;

d. ensure that risk management, including risk assessment and mitigation, is undertaken with respect to the information assets within areas under their control;

e. ensure periodic reviews of information assets are conducted to maintain the required security level as specified in the Infrastructure security classification standard;

f. ensure that authorised users are aware of their obligation to operate in accordance with this policy and its related procedural documentation, and receive adequate support and training to do so; and

g. advise the Information Security Office of any exceptional circumstances that warrant non-patching of servers hosting their systems.

User responsibilities

14. Users:

a. protect information infrastructure resources from unauthorised access, modification, destruction, or disclosure;

b. maintain compliance with University policies, procedures, rules and standards governing IT and information assets;

c. report suspected or known security incidents and/or breaches to the Information Security Office by emailing it.security@anu.edu.au; and

d. keep University information and data secure.

15. Users assist and support the University in carrying out its legal and operational obligations, including co-operating with ITS and the Information Security Office should it be necessary to access or inspect University data stored on a personal device.

Defence Industry Security Program (DISP) responsibilities

16. Staff and Students who are listed on contracts with DISP membership requirements are known as DISP Personnel and will abide by the requirements listed in the DISP Handbook.

17. The DISP Handbook provides a 'working guide' for DISP Personnel and other ANU staff working to implement the security measures required for DISP membership. The DISP Handbook is available at the Information Security Office page.

Breaches

18. The University investigates unauthorised use of the University's IT and information infrastructure.

19. Identified breaches of this policy and related documents are investigated under the following:

- *Information Infrastructure and Services Rule 2020*.
- ANU Code of Conduct
- *Discipline Rule 2021*

Legislation, standards, and regulations

20. To enable better practice within its policy and procedural frameworks, the University recognises, and is consistent with, the following standards and regulations:

- *Australian National University Act 1991*
- *Australian Government Protective Security Policy Framework*
- *Public Governance, Performance and Accountability Act 2013*
- *Public Governance, Performance and Accountability Rule 2014*
- *Commonwealth Crimes Act 1914*
- *Privacy Act 1988*
- *Telecommunications Act 1997*
- *Telecommunications Regulations 2021*
- *Telecommunications (Interception and Access) Act 1979*

Document information

Title	Information technology security
Document Type	Policy
Document Number	ANUP_000421
Version	20
Purpose	This policy establishes the framework for Information Technology (IT) security, systems, and operations that support the core functions of the University, and outlines the responsibilities of the University, owners, and users of IT, infrastructure, and systems.
Audience	Staff, Students, Alumni, Affiliates
Category	Administrative
Topic	Information Security
Subtopic	
Effective Date	27 Jun 2023
Review Date	26 Jun 2028
Responsible Officer	Chief Information Security Officer (ciso@anu.edu.au)
Approved By	Vice-Chancellor (eo.vc@anu.edu.au)
Contact Area	Information security office (it.security@anu.edu.au)
Authority	AS ISO/IEC 27002:2015 Australian National University Act 1991 Australian Government Protective Security Policy Framework Public Governance, Performance and Accountability Act 2013 Public Governance, Performance and Accountability Rule 2014 Australian Government Department of Finance and Deregulation Finance Circular No. 2009/08 Crimes Act 1914 (Cth) Privacy Act 1988 Telecommunications Act 1997 1504249908 116172256 Information Infrastructure and Services Order 2020
Printed On	11 Dec 2023