Policy: Acceptable use of information technology

Purpose

To establish the standards of acceptable use of the University's information technology (IT) and information infrastructure, and end-to-end network by authorised users.

Overview

Permission for members of the University community to use the University's IT and information infrastructure is contingent on compliance with this policy.

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

Authorised user: a person who has been granted 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.*

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 the 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.

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.

Network access: access to the University's ICN.

Network connecting devices: includes servers, storage devices, desktop computers, laptop computers, printers, scanners, photocopiers, mobiles, tablet devices, other personal computing devices, and any computing devices with networking interfaces capable of connecting to the ICN.

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, the implementation and operation of enterprise systems, and ensuring that information asset risk is identified and managed. System owners are a Service Division Director or an equivalent management position.

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).

Visitors: authorised users who are part of the University community, but are not ANU staff or students, who have been approved by a delegate to have access to specific information infrastructure and services. This term preplaces the previously use term of affiliate.

Policy statement

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

2. Acceptable use is defined as activities undertaken in the course of performing the functions of the University, as specified by the *Australian National University Act 1991*.

3. Members of the University community are permitted use of the University's IT and information infrastructure, unless explicitly denied use by the University, or under specific legislation. Authorised users are required to use IT and the end-to-end network responsibly, safely, ethically, and legally.

4. University IT facilities and services, such as email, must not be used to conduct personal business or unauthorised commercial activity. Limited personal use of University IT is acceptable, however access can be revoked at any time and is subject to the same monitoring practices as employment related use.

University responsibilities

5. To support its core activities of teaching and research, the University is responsible for:

a. ensuring the security, integrity, accessibility, authority, and fitness of the University's IT and information infrastructure;

b. providing users with relevant legal information regarding the use of IT and information infrastructure;

c. ensuring software used by the University is licensed in accordance with the procurement and contracts licensing procedures, as found in the ANU Policy Library;

d. backing up University data and information in University storage infrastructure subject to any requirements under the Records and Archives Management policy;

e. providing infrastructure networks to meet the information access needs of the University, and to enable collaboration with external, local, national and international research and education institutions;

f. governance, management and assurance of all systems, including enterprise systems and applications; and

g. the design, operation, and management of the end-to-end data and voice networks.

User responsibilities

6. Authorised users of the University's information infrastructure and end-to-end network use the University's IT and information infrastructure in a manner that is consistent with the provisions of the *Code of Conduct*, *Discipline Rule* and *Information Infrastructure and Services Rule*. These provisions include but are not limited to the following statements.

7. Authorised users of the University's information infrastructure and end-to-end network:

a. use IT and information infrastructure within the directions, limits, and obligations of University Statutes and Rules, and maintain an appropriate level of awareness and compliance with University policies and procedures; and

b. use software and services within the conditions of use specified in the software licence or within any licence agreement between the University and a vendor.

8. Authorised users of the University's information infrastructure and end-to-end network do not:

a. attempt to breach security to access information or parts of the information infrastructure that are outside their authority;

b. allow access to the information infrastructure or end-to-end network to unauthorised users;

c. use another user's credentials, masquerade as, or represent, another user;

d. intentionally connect compromised or unapproved devices, or communication equipment to the University's information infrastructure or end to end network;

e. use IT, information infrastructure, or the end-to-end network to harass, threaten, defame, libel, or illegally discriminate (as defined in relevant legislation);

f. create, transmit, access, solicit, or knowingly display or store electronic material that is offensive, disrespectful, or discriminatory, as identified under the Code of Conduct and Discipline Rule;

g. contravene any provision of the *Copyright Act 1968*, including, but not limited to, unauthorised use of copyright material, and downloading or sharing pirate content using the University's information infrastructure or end-to-end network;

h. modify or remove University information without authority to do so;

i. breach the confidentiality of others, or the University, and the confidential information of others or the University. Information is considered confidential, whether protected by the computing operating system or not, unless the owner intentionally makes that information available; and

j. damage or destroy IT equipment used to access the information infrastructure and end-to-end network.

Breaches

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

- *Information Infrastructure and Services Rule*
- *Information Infrastructure and Services Order*
- *ANU Code of Conduct*
- *Discipline Rule*

Legislation, standards, and regulations

10. 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	Acceptable use of information technology
Document Type	Policy
Document Number	ANUP_001222
Version	19
Purpose	To establish the standards of acceptable use of the University's Information Technology (IT) and information infrastructure, and end-to-end network by authorised users. Acceptable use of information technology policy, policy Acceptable use of information technology
Audience	Staff, Students, Alumni, Affiliates
Category	Administrative
Topic	Information Technology
Subtopic	Usage
Effective Date	2 Apr 2019
Review Date	5 Apr 2024
Responsible Officer	Director, Information Technology Services
Approved By	Vice-Chancellor (eo.vc@anu.edu.au)
Contact Area	Information Technology Services (cio@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 Crimes Act 1914 (Cth) Privacy Act 1988 Telecommunications Act 1997 Telecommunications Regulations 2021 Telecommunications (Interception and Access) Act 1979 116172256 Information Infrastructure and Services Order 2020 Discipline Rule 2021
Printed On	25 Mar 2023