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

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 expected to use IT and the end-to-end network responsibly, efficiently, ethically, and legally.

Access to, and use of, the University's IT and information infrastructure requires users to meet the obligations of this policy.

Scope

The policy applies to all ANU staff, students, and visitors (including VaHAs and contractors) across the University.

Definitions

Authorised user: a person defined under Rule 6 of the *Information Infrastructure and Services Rule 2015* including University staff, students, and visitors (including VaHAs and contractors).

Data: Information that has been converted into binary digital form. In the context of the University, this includes all information stored electronically.

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 information, and
- carries communication.

Integrated Communication Network: the University network infrastructure including the following network sites – Acton Campus, Mount Stromlo

Observatory, Siding Spring Observatory, North Australia Research Unit, Kioloa, University House Melbourne, ANU Medical School remote sites and hospitals, Fenner Hall, ANU UniLodge, ANU Exchange sites, and Hume Library Store.

Network access: access to the University's ICN, which supports the University's data, voice and video resources, services, and applications.

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: someone with delegated responsibility for information assets including defined responsibilities for the security of the data 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 should be a Service Division Director or in an equivalent management position.

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

Visitors: authorised users who are a 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 replaces the previously used term of affiliate.

Policy statement

1. This policy and related documents draw their authority from the *Information Infrastructure and Services Rule 2015*.

2. Acceptable use is defined as behaviour consistent with the mission and authorised activities of the University.

3. 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

4. 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 in University storage infrastructure and optimising storage by deleting any unwanted data, 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. Physical infrastructure and networks within the University provide the basis for national and international connections, and educational and research excellence

f. identifying and managing overall risk across the University's IT and information infrastructure

g. supporting network security at a sufficient level to protect the University's information sources, electronic resources, intellectual property, and network access.

User responsibilities

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

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

b. not intentionally connect compromised or unapproved devices or communication equipment to the University's information infrastructure or end-to-end network

c. not intentionally attempt to breach security to access information or parts of the information infrastructure that are outside their authority

d. not allow access to the information infrastructure or end-to-end network to unauthorised users

e. not use the University's IT and information infrastructure in a manner that is inconsistent with the provisions of the ANU *Code of Conduct* and/or *Discipline Rule 2015*

f. not use another user's credentials, masquerade as, or represent, another

user

g. not use IT, information infrastructure, or the end-to-end network to harass, threaten, defame, libel, or illegally discriminate, as defined in relevant legislation

h. not create, transmit, access, solicit, or knowingly display or store electronic material that is offensive, disrespectful, or discriminatory, as identified under the ANU Code of Conduct and Discipline Rule 2015

i. not 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

j. 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

k. not modify or remove University information without authority to do so

l. not 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

m. not damage or destroy IT equipment used to access the information infrastructure and end-to-end network.

Breaches

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

- *Information Infrastructure and Services Rule 2015*
- *ANU Code of Conduct*
- *Discipline Rule 2015*.

Legislation, standards, and regulations

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

- AS/NZS ISO/IEC 27002:2006 Standards Australia Information Technology
- *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 2001*
- *Telecommunications (Interception and Access) Act 1979*

Document information

Title	Acceptable use of Information Technology
Document Type	Policy
Document Number	ANUP_001222
Version	9
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.
Audience	Staff, Students, Alumni, Affiliates
Category	Administrative
Topic	Information Technology
Subtopic	Usage
Effective Date	1 Nov 2017
Review Date	1 Nov 2018
Responsible Officer	Director, Information Technology Services (director.its@anu.edu.au)
Approved By	Vice-Chancellor (vc@anu.edu.au)
Contact Area	Information Technology Services (policies.its@anu.edu.au)
Authority	Information Infrastructure and Services Statute 2012 Information Infrastructure and Services Rule 2015 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 1998 Telecommunications Act 1997 Telecommunications Regulations 2001 Telecommunications (Interception and Access) Act 1979