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 POIs and contractors) across the University.

Definitions

Definitions provided in this document are terms that are used throughout this policy and its related documents.

AICTEC: Australian Information and Communications Technology in Education Committee manages the closed second level domain .edu.au.

APNIC: Asia Pacific Network Information Centre is responsible for the assignment of public IP addresses in the region. APNIC set policies for IP address assignment to ensure global uniqueness, address space aggregation, conservation, and fairness.

auDA: .au Domain Administration Limited. auDA is the overarching policy authority and industry self-regulating body endorsed by the Australian Government to administer and manage the .au domain space.

Authorised user: a person defined under Rule 6 of the *Information Infrastructure and Services Rules 2009* including University staff, students, and visitors

(including POIs and contractors) with a current active user account.

Authoritative DNS service: the primary name server which holds the authoritative domain database. It propagates information about the University's domain names and systems to the internet. Official secondary servers are also configured for redundancy and load balancing.

Boundary network device: a network device under the control of the University that provides suitable secure and isolating inter-network boundary between ICN and a non-ANU entity's private network.

CNAME record: a DNS record that assigns an alias to the true (canonical) name of the server.

Domain name: the unique name by which a network connecting device is known to the internet.

DNS: Domain Name System is a hierarchical grouping of hosts based on domain levels. In Australia, the first level domain is .au.

DNS server: resolves host names to IP addresses (either directly or through the hierarchy) and locally holds a database of hosts and IP addresses within its domain.

Hostmaster: manages the University's authoritative domain database and DNS server and University secondary name servers.

Hostname: the unique name of a network connecting device, which has a unique MAC address.

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 information, and
- carries communication.

Integrated Communication Network (ICN): the University network infrastructure including the following network sites – Acton Campus; MSO; SSO; NARU; 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, personal computing devices, and other computing devices with networking interfaces

capable of connecting to the ICN.

Non-ANU entity: a separate legal entity to the University that has a presence within the University boundary, and requires as a minimum, access to the ICN and an allocation of the University's IP addresses.

RF spectrum: radio frequency spectrum, which, for IEEE 802. 11 wireless LAN services and any wireless WAN services, the microwave radio frequency spectrum is split into channels and a campus area network requires spectrum planning of these channels to avoid interference.

Subnet: a contiguous group of IP addresses from the University's IP address range assigned to access the information infrastructure and services via the ICN.

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

2. University IT facilities and services (such as email) must not be used in the conduct of 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

3. 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

d. backing up University data in University data storage repositories and optimising storage by deleting any unwanted data, subject to any requirements under the Records and Archives Management Policy

e. identifying and managing overall risk across the University's IT and

information infrastructure

4. University responsibilities in this policy and its related documents are vested in Information Technology Services (ITS).

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 Rules 2014

f. not use another user's credentials, or 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 Rules 2014

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 specific 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 owners 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 IIS Statute and Rules 2015 or through the ANU Code of Conduct or Discipline Rules 2015.

Legislation, Standards, and Regulations

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 (PGPA Act)
- Public Governance, Performance and Accountability Rule 2014
- Australian Government Department of Finance and Deregulation Finance Circular No. 2009/08
- 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	7
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	8 Apr 2016
Review Date	10 Apr 2017
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