Policy: Information Technology security

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.

Overview

ANU is committed to ensuring appropriate security for all data, equipment, and processes within its domain of ownership and control. University assurance of compliance with relevant policies, associated procedures, and security standards is achieved through the use of regular audits or inspections of the IT infrastructure and environment, and information assets.

Scope

This policy applies to all University staff, students, and visitors (including VaHAs and contractors) using the University's IT, systems, and data.

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).

Availability: ensuring that information assets are available for their intended use.

Confidentiality: limiting information access and disclosure to authorised users, and preventing access by, or disclosure to, unauthorised users.

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 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.

Information security: a set of measures by which the University seeks to treat risk to the confidentiality, integrity, and availability of its information assets.

Information security risk: the potential loss of an asset's confidentiality, integrity, or availability. Risk is defined by a combination of threats, vulnerabilities and impact. A threat exploiting a vulnerability results in an impact. Risk can be accepted if the cost of treating the risk outweighs the cost of impact, is mitigated through applying appropriate controls, or transferred through insurance.

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.

Password: the primary means of authenticating user access to ANU information services and systems. Encompasses passphrases.

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, and ensuring that information asset risk is identified and managed. System owners should be a Service Division Director, College General Manager or their nominated delegate

University provided storage infrastructure: data storage systems that are provided by the Information Technology Services (ITS) Storage and Compute Team, including but not limited to solid state drive storage area networks.

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 2015*.

2. The University depends on external network interconnectivity and the internet for its research, teaching and learning, outreach, and administration activities, and is committed to providing a secure yet open information infrastructure that protects the integrity and confidentiality of information without compromising its availability.

3. The University implements an effective framework for the management of

information security and incident response. Information security is the preservation of the confidentiality, integrity and availability of information.

4. Information security applies to all forms of information 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.

5. ANU is committed to ensuring appropriate security for all information technology, data, equipment, and processes within its ownership and control.

University responsibilities

6. The University will investigate non-permitted use of the University's IT and information infrastructure within the bounds of University policies and take appropriate action to protect, preserve, and keep available and accessible, the University's IT and information infrastructure, including the managed end-to-end network.

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

a. governance and assurance of all systems, including enterprise systems and applications

b. management of enterprise systems

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

d. coordinating information security activities for members of the University community

e. coordination in tandem with the Corporate Governance and Risk Office, to identify, manage and mitigate overall risk across the University's IT and information infrastructure

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

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

9. The University reserves the right to refuse, prevent or withdraw access to authorised users and/or particular devices or software where it considers that there are unacceptable security or other risks to its staff, students, business, reputation, data, systems or infrastructure.

10. The University also reserves the right to modify access to users based on the

reviewed classification of data.

System owner responsibilities

11. All information infrastructure systems must have a system owner.

12. All system owners must:

    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 information technology within their area

    c. ensure that changes to infrastructure are carried out using ITS change management practices to ensure that the risk and impact of each change has been assessed and managed, 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

    f. ensuring authorised users are advised of all relevant ANU policies and related documents, and are provided with adequate training and support on the use of information infrastructure and security of information assets.

User responsibilities (including non-ANU entities)

13. All users must:

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

    b. maintain an appropriate level of awareness and comply with University policies, procedures, Rules and Standards governing IT and information assets

    c. report suspected or known security incidents and/or breaches to the ITS Cyber and Digital Security Team by emailing it.security@anu.edu.au.

14. Authorised users are required to keep University information and data secure.

15. Authorised users are required to assist and support the University in carrying out its legal and operational obligations, including co-operating with ITS

should it be necessary to access or inspect University data stored on a personal device.

Breaches

16. 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

17. 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	Information technology security
Document Type	Policy
Document Number	ANUP_000421
Version	11
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 Technology
Subtopic	Security
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

	1504249908
Printed On	11 Dec 2018

Please ensure you have the latest version of this document from the Policy Library website before referencing this.