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 POIs and contractors) using the University’s IT, systems, and data.

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

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

Elevated Access Users: Elevated Access users are users within a business system or application who have additional access via roles or functionality, who do not have privileged access. Elevated Access users may include supervisors or reviewers.

Information: includes data stored in print, electronically, or any other format.
Information Asset: any set of information or part of the information infrastructure critical to the functioning of the University, with a designated system owner.

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.

Integrity: ensuring the trustworthiness of information assets.

Privileged Access Users: Privileged Access users are users of a systems with one or more of the following, and may include supervisors or reviewers:

- the ability to change key system configurations
- the ability to change control parameters
- access to audit and security monitoring information
- the ability to circumvent security measures
- access to data, files, and accounts used by other users, including backups and media
- special access for troubleshooting.

System Owner: someone with delegated responsibility for information assets including defined responsibilities for 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 or in an equivalent management position.

System Support Staff: a person or persons defined for a specific information asset with some responsibility for operation of the asset as delegated by the system owner.

Threat: any technological, natural, or man-made cause of harm to an information asset including software bugs, unlocked rooms, or well-known passwords.
Vulnerability: a weakness in the security of an information asset that might be exploited by a threat.

Policy statement

1. 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.

2. 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. 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.

University Responsibilities

3. 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.

4. 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. in coordination with the ANU Corporate Governance and Risk Office (CGRO), 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.

**Owner Responsibilities**

5. All information infrastructure systems must have an owner. A system owner is defined as the nominated position that has responsibility for the security of the data and application component of an information asset, and is accountable for those aspects of an information system. System owners should be a Service Division Director or in an equivalent management position.

6. 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 change management practices that 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. ensure users are provided with adequate training and support on the use of systems and applications
   g. ensure users are made aware of, and comply with, all relevant policy documentation.

**User Responsibilities (including non–ANU entities)**

7. All users must:
   a. protect information infrastructure resources from unauthorised access, modification, destruction, or disclosure
   b. ensure network–connecting devices meet ANU standards and specifications for approved network connectivity and security
   c. maintain an appropriate level of awareness and comply with University policies, procedures, Rules and Standards governing IT and information assets
d. report suspected or known security incidents and/or breaches to University Cyber and Digital Security.

Breaches

8. 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

9. 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