ANZSOG INFORMATION SECURITY POLICY

Table of Contents

1 Overview

The Australia and New Zealand School of Government (ANZSOG) values the use of information in supporting the mission of the organisation. ANZSOG has strong engagements and partnerships with both local and global communities allowing ANZSOG to share knowledge and resources and be a leader in research outcomes.

In this context, ANZSOG information, whether managed and residing on ANZSOG resources or held in trust and managed by third parties or business partners, is an important asset that must be protected. Any person or organisation that uses or holds in trust these assets has a responsibility to maintain and safeguard them. ANZSOG is committed to preserving the confidentiality, integrity, and availability of information regardless of the form it takes - electronic or non-electronic. Improper use of information resources may result in harm to ANZSOG and its mission of teaching, research and international outreach.

2 Purpose

The purpose of this policy is to ensure that ANZSOG information can be used when required with the confidence that it is accurate and complete, and that it is adequately protected from misuse, unauthorised access, disclosure, damage or loss. The policy reinforces the value of data and information to ANZSOG. The Information Security Policy sets out management's information security direction.

3 Definitions and Terms

Term	Definition
Asset custodian	Users who perform operations within information systems to manage, operate and protect information assets on behalf of the asset owner.

Asset owner	All individuals who have been allocated responsibilities and hold accountability for an information asset. E.g. owner(s) of an image library, of the Student System The information assets that must have a nominated asset owner are: a) financial data – CFO b) human resources data – Director, Human Resources c) student data – Director, Government Relations d) research data – TBC e) Business Unit specific data – The Director of the Business Unit
Corporate Device	A Device owned or leased by ANZSOG.
Device (can also be referred to as an Endpoint)	Computing device that communicates back and forth with a network to which is it connected. Examples of endpoints include: desktops; laptops; smartphones; and tablets.
External provider	An external entity which provides computing and network facilities to ANZSOG
Computing and network facilities	Includes computers, computer systems, data network infrastructure, dial-in network access facilities, email and other communications and information facilities together with associated equipment, software, files, and data storage and retrieval facilities, all of which are owned or operated by the ANZSOG and form part of the central facilities or the local facilities, as the case may be.
Stakeholder	Employees, contractors, consultants, temporaries, and other workers at ANZSOG.
Data	Any information (including personal information) obtained, received or held by ANZSOG. Also referred to as information.

Data Confidentiality	Data confidentiality, in the context of computer systems, allows authorised users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.
Data Integrity	Data integrity refers to the fact that data must be reliable and accurate over its entire lifecycle.
Information Asset	A body of knowledge that is organised and managed as a single entity e.g. financial; human resources; student; research; system identity; division-specific data.
Trusted third party	Suppliers with whom ANZSOG has engaged, typically in the context of program delivery. Examples: hotels, logistics companies, venue hire firms, University partners. The engagement will include a contract or service agreement at the outset which addresses privacy.
Whitelisted Applications	ANZSOG approved software applications that are permitted to be present and active on a computer system. The goal of whitelisting is to protect computers and networks from potentially harmful applications.

4 Objectives, Aim and Scope

4.1 Objectives

The objective of ANZSOG's Information Security Policy is to preserve:

- **Confidentiality** - Access to data shall be confined to those with appropriate authority.
- **Integrity** – Steps must be taken to ensure that data cannot be altered by unauthorised people. All systems, assets and networks shall operate correctly, according to specification.
- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed.

4.2 Policy aim

The aim of this policy is to ensure the confidentiality, integrity, availability and accountability of ANZSOG's information assets:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for information security as an integral part of the day-to-day business.
- Protecting information assets under the control of the organisation.

4.3 Scope

This policy applies to all stakeholders. This policy also applies to all equipment that is owned or leased by ANZSOG.

5 Responsibilities for Information Security

Role	Responsibility
Chief Executive Officer and Dean	• Ultimate responsibility for information security rests with the Chief Executive of ANZSOG, but on a day-to-day basis the CIO shall be responsible as per below.
Executive Team	• Promoting a risk—and-control-aware culture. • Ensuring that their staff and contractors have appropriate access to information and that information is managed in accordance with this Policy and the associated Standards. • Identifying fraud and corruption risks. • Taking appropriate actions and making relevant decisions in light of those risks.
CIO	• Act as the policy steward. • Manage, maintain, implement, review and update the policy annually. • Day-to-day responsibility for the protection of information assets to ensure their confidentiality, integrity and availability. • Determining ANZSOG's whitelisted applications (see definitions and terms), approval of any specialised software.
Line Managers	Ensure that: • The information security policy is applied in their work areas. • Incidents are reported in a timely manner.
Asset owner	Each IT asset (hardware, software, application or data) shall have a named custodian who shall be responsible for the information security of that asset.

	Individuals are accountable for the classification, definition, quality, maintenance and end- to-end usage of the information in their area of responsibility. This includes: • Assess risk and classify the information assets they own and communicate that classification to intended Information Asset Users • Determine and monitor who has access to, and the appropriate usage of, that information asset • Approve key changes to the system housing the information asset • Report to the CIO any misuse, transmission or storage of the information asset inconsistent with its classification.
All Stakeholders	All stakeholders shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action. All users shall be individually responsible for the security of their physical environments where information is processed or stored. Each member of staff shall be responsible for the operational security of the information systems they use. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.
CFO	Contracts with external contractors that allow access to ANZSOG's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies. The management of information security risks are compliant with ANZSOG's risk management framework.
HR	Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

	Information security expectations of staff shall be included within appropriate job descriptions. All ANZSOG staff (Including casuals), consultants, contractors, third parties, agency staff, and associates may be subject to appropriate security processes before (e.g. police checks) and during their employment.
Facilities	Building facilities are responsible for physical security including maintaining appropriate environmental conditions, such as temperature, air and humidity, as well as fire safety, visitor access, perimeter security and building requirements.

6 Applicable legislation, standards, and policies

ANZSOG is obliged to abide by all relevant Australian legislation. The requirement to comply with this legislation shall be devolved to employees and agents of ANZSOG, who may be held personally accountable for any breaches of information security for which they may be responsible. ANZSOG shall comply with international legislation (such as GDPR) as appropriate.

This policy supports compliance with the:

a) Copyright Act 1968 (Cth);
b) Health Records Act 2001 (Vic);
c) Privacy and Data Protection Act 2014 (Vic);
d) Public Records Act 1973 (Vic);
e) AS ISO/IEC 27001:2015 – Information technology – Security techniques – Information security management systems – Requirements;
f) AS ISO/IEC 27002:2015 – Information technology – Security techniques – Code of practice for information security management; and
g) Payment Card Industry Data Security Standard (PCI DSS)

This policy supports compliance with related ANZSOG policies, procedures and guidelines:

a) Travelling In High Threat Countries Guideline

b) Provision and Acceptable Use of IT Policy (*under development*)
c) Flexible Work Policy (*under development*)
d) Data Breach Response Plan
e) Social Media Policy

7 Policy Requirements

7.1 Information Security Awareness

Information security awareness shall be included in the staff induction process.

An ongoing awareness programme shall be established and maintained in order to ensure that staff awareness is refreshed and updated as necessary.

Asset owners ensure that users receive information security induction and awareness training on commencement of employment/engagement at least every two years. The training includes consideration of information security policies and related processes, and the correct use of information asset processing facilities.

Information security awareness content includes consideration of:

- this policy and supporting processes.
- the types of information assets that may be encountered.
- how information assets should be handled and transmitted.
- information security concerns such as viruses, malware and social engineering.
- workplace/facility security including building access, security controls and reporting of incidents.
- the consequences of failure to comply with this policy and related processes.
- information security considerations as appropriate to the individual's role.

7.2 End User Access Controls

Only authorised personnel who have a justified and approved business need shall be given access to restricted areas, systems or stored data. Access to computer facilities, mobile devices and ANZSOG-related information assets shall be restricted to authorised users who have a bona-fide business need to access the information.

Access to all data shall be controlled and restricted to those authorised users who have a legitimate business need. Authorisation to use an application shall depend on the availability of a licence from the supplier.

Temporary staff

For auditing and security purposes, all temporary staff will logon to computing and network facilities using their own named ANZSOG account and not a shared logon. The approval of the CIO is required for exceptions.

Subcontractors and secondees

Subcontractors and secondees, which can include Faculty, may be issued with an ANZSOG logon and a mailbox, however access to any information will only be provided in strict accordance with contractual arrangements.

7.3 End User Security

Devices are the primary gateway to ANZSOG's data and business applications. Consequently, end user protection is critical to ensuring a robust, reliable and secure IT environment. Failing to do so can result in an information security incident, causing financial and/or reputational loss to ANZSOG.

7.4 Mobile Device Management and BYOD

Refer to the Provision and Acceptable Use of IT Policy, section on mobile device management.

7.5 User Removable Media

Several security measures will be used to prevent threats from removable media which include: data encryption; antivirus; blocking executable files from running; allowing only specifically approved peripherals; blocking write access to removable media. In extreme situations the use of removable media may be blocked.

Only information categorised as Internal or Public should be stored on removable media, the approval of the CIO is required for storing information that is not Internal or Public. See below Classification section.

7.6 Remote Working

ANZSOG is a networked organisation with staff working from anywhere in the world. Therefore, ANZSOG will design information security controls accordingly. Further, ANZSOG is committed to assisting staff members' flexible work arrangements.

7.7 IT Acceptable Use /Monitoring System Access and Use

An audit trail of system access and data use by staff is continuously logged and reviewed on a regular basis. ANZSOG will use the recorded monitoring to investigate a potential breach of policy.

7.8 Communications

Also refer to the Social Media Policy.

Communications between ANZSOG and related parties regarding official ANZSOG business should be carried out by approved personnel using approved computing and network facilities.

Unless approved by the CIO, these exclude the use of third-party services for work purposes such as:

- public email domains such as Hotmail;
- communications apps such as WhatsApp;
- cloud hosting platforms such as Dropbox.

Such third-party services may be blocked to support policy where required.

7.9 Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorised by the CIO.

7.10 Information Risk Assessment

The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within the ANZSOG risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular

intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of ANZSOG's risk management program. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

7.11 Project based Privacy Impact Assessments

ANZSOG employees must perform a privacy impact assessment for all high-risk projects. A project will be considered to be 'high risk' if the organisation reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals or the project deals with sensitive information.

Preferred Privacy Impact Assessment Template: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments

7.12 Incident Reporting of Information Security Events And Weaknesses

If you suspect an information security incident and/or breach has occurred, you must report it through established channels as per the awareness training, depending on the nature of the incident. ANZSOG's approved incident management processes are managed by a third party. For more information, please contact the CIO.

Related policies: Data Breach Response Plan

7.13 Accreditation of Current and New Information Systems

ANZSOG shall ensure that all new information systems, applications and networks are approved by the CIO before they commence operation.

7.14 System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the CIO.

7.15 Third Party Risk Management

Third party service providers must ensure the confidentiality, integrity and availability of ANZSOG's information systems and associated information assets are secured and protected at

all times. Security controls, service definitions and service level agreements must be consistent with ANZSOG's information security requirements.

Third party suppliers such as hotels, event managers, travel consultants and partnering educational institutions must only be provided information on a need to know basis (i.e. hotels can receive a list of names of expected guests). This information must be shared with the nature of the information in mind. For more information see section 8 Classification below.

7.16 Licensing Rights

ANZSOG shall ensure that all information products are properly licensed and approved by the CIO.

Apart from standard issued software, users can access other whitelisted applications through the following means:

- From the Windows Store or Apple App Store.
- Submitting a request for specialised software.

7.17 Business Continuity and Disaster Recovery Plans

Given outsourced Cloud Infrastructure is used for all IT applications, ANZSOG shall ensure that business continuity and disaster recovery plans are produced by third party partners for all mission critical information, applications, systems and networks.

7.18 Reporting

The CIO shall keep the CEO informed of the information security status of the organisation by means of regular reports and presentations.

8 Classification

A consistent system for the classification of information within ANZSOG enables common assurances in information partnerships, consistency in handling and retention practice when information is shared internally and with trusted third parties.

Classification	Definition	Examples
Restricted	Information that is extremely sensitive, of great value to ANZSOG and intended for use only by various named individuals, including any personally identifiable information or financial information	• Credit card data • Faculty contract/payment Agreements • All identity data of participants (including passport details) • Confidential staff details such as: home contact details; pay; leave; incident reports; performance related.
Confidential	Information assets intended strictly for distribution/use by a small selected group The classification of Confidential – shall be used for customer records and personally identifiable information passing between ANZSOG staff and staff of trusted third parties and business partners. Documents so marked shall be held securely at all times in a location which only authorised persons have access, not left unattended where unauthorised persons might gain access to them and should be transported securely in sealed packaging or locked containers.	• Details of current and former students, including marks • Supplier Lists • Operating manuals • Financial Statements • Commercially sensitive documentation and conversations • Participant travel schedules • Passwords • Security Incident information

	The classification Confidential covers information that the disclosure of which is likely to: • adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals • cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations • facilitate the commission of crime or other illegal activity • breach statutory restrictions on disclosure of information, eg OAIC • disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.	
Internal	ANZSOG information intended only for all employees and approved non-employees such as contractors, vendors or students	• Budget reports • Internal memos • Other business-related data created by ANZSOG that includes purchase orders, non-sensitive meeting minutes or details of office social events

Public	Information available to the general public and intended for distribution outside ANZSOG	Marketing promotions, press releases/media articles, anything approved for the public domain

If in doubt, treat information as internal-use only in order to protect it from third party exposure and preserve its integrity.

9 Policy Compliance

9.1 Policy Audit

This policy shall be subject to audit by internal and external auditors.

9.2 Compliance Measurement

The CIO will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback.

9.3 Exceptions

Any exception to the policy must be approved by the CIO in advance.

9.4 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

10 Further Information

Category: ICT

Review due by: 2/7/2020

Version: 1

Policy Steward: CIO

Status: Published

Further information and advice on this policy can be obtained from the CIO.

11 Revision History

Version	Authorised by	Date Approval	Effective Date	Sections modified
1	CEO and Dean	2/7/2019	2/7/2019	