ANZCA
FPM

Australian and New Zealand College of Anaesthetists (ANZCA)

INFORMATION SECURITY POLICY

1 Purpose

This policy defines guiding principles for protecting the security of data and information within ANZCA's environments and ensure the confidentiality, integrity, and availability of information throughout its lifecycle from creation to archival and disposal.

1.1 Scope

ANZCA provides a variety of Information and Communications Technology (ICT) resources to support the activities of the College. These include, but are not limited to:

- the voice & data network, including fixed, wireless & mobile network services.
- the learning management system,
- the training portfolio system (TPS),
- the continuing professional development (CPD) system,
- the exam management system (EMS),
- the ANZCA portal and online event registration system,
- iMIS, the College's core database of records,
- Informz, the College's electronic newsletter and survey tool, computer hardware and software, including personal computers, notebooks, and servers,
- Zoom for communication and video conferencing,
- Microsoft productivity suite for content development, communication, document management, and collaboration,
- internet access, including wireless internet access,
- mobile phones, smart phones, and wireless data cards, and
- other services for specific use-cases across the business.

The above ICT resources process and store sensitive or confidential information regarding the College and its stakeholders. It is therefore essential that everyone involved ensures the security of the data and information.

This policy applies to:

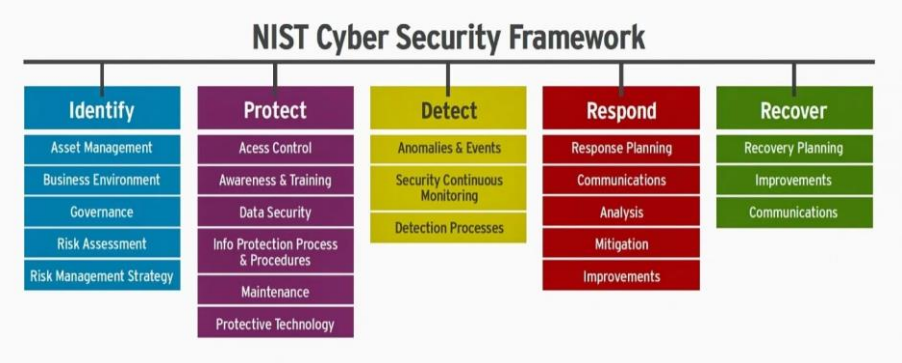
a) all technology resources used by, operated by, or provided on behalf of ANZCA.
b) all information collected, created, stored, or processed by, or for ANZCA on our information systems and infrastructure; and
c) all users (individuals) who utilise, or are involved in deploying and supporting, information systems and resources provided by ANZCA. This includes all staff (full-

time, part-time, casual), contracted and agency staff, trainees, fellows, specialist international medical graduates (SIMGs), volunteers, suppliers, partners, contractors, sub-contractors, or affiliated organisations.

2 Policy

This policy applies to digital information, hardcopy records, and unstructured content including but not limited to content in emails, notepads, conversations, chats etc. ANZCA will apply a risk-based approach to information security to maintain the confidentiality, integrity, and availability and protect against unauthorised disclosure, access, use, loss, compromise (malicious or accidental), or breach of privacy.

ANZCA will use the National Institute of Standards and Technology (NIST) Cyber Security Framework (image below) as a guide to develop a continuous improvement strategy for security capability uplift.



3 Principles

- ANZCA will ensure protection of information (and/or data) against unauthorised disclosure, access or use, loss, or compromise (malicious or accidental) or a breach of privacy that could have an adverse impact upon the organisation.
- A flexible and tailored approach to information security will align with the corporate risk framework. A consistent risk-based approach to information security will reduce the likelihood and consequence of unauthorised disclosure, access or use, loss, or compromise (malicious or accidental) or a breach of privacy.
- Information risks will be proactively managed by continual reviews and updates to procedures, processes, technical standards, and training materials as technology and threats change.
- Staff will be kept up to date with changes to information security requirements through communication channels, updates to procedures and mandatory information security training.
- It is not singularly the domain of the Management Team, the Information Technology and Security team, IT Security, or Systems Administrators to protect information but everyone's responsibility to play their part in protecting ANZCA information:
  a) All users are responsible for understanding and complying with ANZCA policies and manage college information securely.
  b) A risk-based approach to information security should be adopted by all users to help ensure that all information related risks are managed in a consistent and effective manner.

c) All users are to assist with the protection of sensitive ANZCA data and information to prevent disclosure to unauthorised individuals.

d) All users must comply with relevant legal and regulatory requirements.

e) All users are to use or apply approved security solutions and services, where possible, to avoid the creation of disparate IT Security controls.

4 Information Security Domains and Guidelines

4.1 Human Resources Security

a) 'All users' interacting with information assets have a responsibility to ensure the security of those assets as per section 2 of the Acceptable Use of IT Resources Policy.

b) ANZCA will perform compliance checks to ensure that individuals suitable to be given access to the college ICT systems and the information held on these systems.

c) Users must be trained, equipped, and periodically reminded to use information securely.

d) When employment ends with ANZCA, user access must be suspended or removed from ICT systems and all college equipment must be recovered.

e) Where a user's role changes, the user's information access privileges must be reviewed and changed accordingly on a 'least privilege' basis.

4.2 Access Control

a) It is the responsibility of all ANZCA information owners and system owners to determine appropriate access controls, access rights and restrictions for their information and information systems as per section 2 of the *Acceptable Use of IT Resources Policy*.

b) All users using ANZCA ICT resources must ensure appropriate authorisation to systems and services.

c) User registration and de-registration process should ensure

- appropriate authorisation prior to account creation
- appropriate assignment of access rights and allocation of unique user identities
- user acknowledgement of the policy regarding acceptable use

d) Access privileges must be assigned using Role-Based Access Control (RBAC).

e) All accounts must adhere to the following privilege management principles:

- Need to know – the legitimate requirement of a person to know, access, or possess sensitive information that is critical to the performance of the authorised job function.
- Least Privilege – every user and program must operate using the least set of privileges necessary to complete the authorised job function.
- Segregation of duties – the practice of dividing the steps in a system function among different individuals, to keep a single individual from subverting the process.

f) Information owners must review user access rights on a regular basis to ensure that role changes (promotion, demotion, transfer, and termination) are correctly reflected in all information systems.

g) All account passwords must meet recommended complexity criteria. Long passwords of 14 or more characters including non-alphanumeric characters, numbers and upper/lower case alphabets. Passphrases are recommended over short passwords. Once a password has been issued, full responsibility for that account and associated password is transferred to the user.

h) Passwords must not be written down or stored in clear text, although password management software may be used to securely store them.

i) Recommended user account management controls must be enforced to cover the following:

- account lockouts following multiple invalid logon attempts.
- disablement of staff accounts not accessed for an extended period.
- enforcement of password resets if notified that credential are suspected to be compromised.
- email alerts when a login is detected from a new device or new location.

j) All smart devices containing ANZCA data (including email) must be secured with a 4-digit PIN or a biometric lock with a compliant backup password/PIN.

k) All users with access to privileged accounts must maintain the confidentiality of any information they have access to, both during and after their employment with ANZCA.

l) Privileged user access to ANZCA ICT domains, services and systems must be authenticated using multi-factor authentication (MFA) unless there is a system limitation. Privileged credentials must only be used when performing tasks that specifically require those privileges. While performing normal activities, administrators must use a separate, unprivileged account.

m) Privileged account passwords should be held in ANZCA approved Privileged Account Management (PAM) platform to ensure they remain available to system administrators.

- *Shared accounts* must be the exception, approved by CIO, use secondary authentication, be monitored, and password regularly changed.
- *Service accounts* must be single use and restricted to the purpose issued for.

4.3 Asset Management

a) Information must be assessed and classified based on the level of protection required as documented in the Information Asset Register (IAR).

b) The Australian Government Protective Security Policy Framework (Policy 8 Classification System) details how to assess information security classification and adopt marking, handling, storage and disposal arrangements that guard against information compromise. Below is an overview of the classifications levels from this policy. ANZCA is not expected to use *Protected, Secret or Top-Secret* classifications.

			Security classified information			
	UNOFFICIAL	OFFICIAL	OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
	No business impact	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Compromise of information confidentiality would be expected to cause ➔	**No damage.** This information does not form part of official duty.	**No or insignificant damage.** This is the majority of routine information.	**Limited damage** to an individual, organisation or government generally if compromised.	**Damage** to the national interest, organisations or individuals.	**Serious damage** to the national interest, organisations or individuals.	**Exceptionally grave damage** to the national interest, organisations or individuals.

c) Classifications will be determined by the Information Owner and based on the value, legal requirements, sensitivity, and criticality of the information and the potential impact to ANZCA if the information is disclosed, misused, misrepresented, or lost.

4.4 Physical & Environmental Security

4.4.1 Equipment

a) ICT infrastructure must be protected from damage/disruptions caused by failures in supporting utilities.

b) Equipment must be correctly maintained to ensure availability and integrity of sensitive information and assets. When serviced, System Owners must consider the sensitivity & value of the information.

c) Data must not be disposed of any College resources without appropriate authorisation.

d) All data and software must be erased from equipment using authorised method prior to disposal or redeployment to prevent breaches of privacy or licence agreements.

e) Asset inventories must be updated to record details of the data wiping.

f) Workspaces must be secured when they cannot be monitored by authorised staff.

4.4.2 Secure Areas

Secure areas are locations restricted to authorised access only. These include server rooms, cupboards with ITS network equipment, or storerooms with ITS hardware.

a) Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

b) Third-party personnel may be granted restricted access only when required; their access must be authorised and monitored. Visitors must be escorted by authorised personnel.

c) All staff and authorised personnel must wear visible identification. Access rights must be regularly reviewed. an audit trail of all access must be maintained.

d) Where appropriate, entry points must be monitored by a Closed-Circuit Television (CCTV) system on a 24/7 basis. All video surveillance data must be protected from unauthorised disclosure, modification, and erasure, and maintained for an agreed period.

e) Physical protection against natural disasters, malicious attack or accidents must be applied.

4.5 Operations Management

Key ITS operations and applications team members responsible for maintenance of ANZCA systems will be referred to as ANZCA system owners in this section.

a) ANZCA system owners must ensure that their development code, and software libraries are adequately protected to prevent the corruption of information systems or the disruption of business operations.

b) Development and Test environments must be separated from Production to reduce risk of unauthorised access or accidental damage to integrity or content.

c) Application development security must ensure use of a code repository that is access controlled.

d) All changes to ITS services and system environments, including provisioning and de-provisioning of assets, promotion of code, configuration changes and changes to standard operating procedures (SOPs) must be authorised by the IT Change Advisory Board (CAB).

e) Detection, prevention, and recovery controls, supported by user awareness activities, must be implemented to protect against malware.

f) Backups of information systems must be done periodically and be available for recovery. Information owners and system owners must agree on, define, and document backup and recovery processes, that consider the confidentiality, integrity and availability requirements of information and information systems. However, the college recommends that work is regularly saved to avoid losing content.

g) ANZCA system owners must ensure that event logs recording user activities, exceptions, faults, and information security events are produced and retained for agreed periods. Event logs from critical business systems and endpoints must be fed to the security incident and event management (SIEM) solution configured to alert the MDR partners and operations team and if certain events or signatures are detected.

h) Activities of privileged users must be monitored, and the logs periodically reviewed.

i) Vulnerability scanning and penetration tests should be conducted before any system deployments, after a significant change to a system, and at least annually or as specified by system owners. To support vulnerability management, an inventory of ICT assets must be maintained. Penetration testing should be based on risk exposure and rotated annually between systems. E.g. newly built, internet exposed services.

j) Introduce vulnerability scanning tools for continuous scanning of network assets.

k) All IT infrastructure, systems and services must be updated with the latest stable patches released by the respective vendors.

l) Services no longer supported by vendors with patches or updates for security vulnerabilities must be updated or replaced with vendor-supported versions by ICT in consultation with relevant suppliers.

4.6 Telecommunications Security

a) Networks must be designed, implemented, and managed using security best practices. Access to internal non-public facing ICT resources will only be allowed after valid identification, authentication, and authorisation of the user.

b) Networks will be designed with multiple functional areas and network zones with physical and virtual separation where possible based on the sensitivity and criticality of information and services.

c) Before installing a device on the network, the default account settings and configurations must be changed, and devices must be hardened.

d) Firewalls must be deployed in a highly available configuration and managed using a central management console, with changes tracked for auditability.

e) Remote access if authorised shall only be provided through ANZCA-managed secure tunnel such as a Secure Sockets Layer (SSL) or Internet Protocol Security (IPSec) Virtual Private Network (VPN). Remote access must be controlled with encryption and strong passwords, and multifactor authentication (MFA).

f) Bring your own device (BYOD) access to ANZCA services will require authorisation and offer restricted access to internal network and systems.

g) Wireless access points must implement strong encryption for authentication and transmission. Wireless networks provided for the public (e.g., guest users) must be segregated from all other networks.

h) Where feasible communication devices and systems shall be enabled with encryption.

i) Annual assessment must be conducted to ensure compliance with standards.

4.7 Mobile Device Security

This section outlines guidelines for safe use of mobile devices and applies to:

a) all mobile devices, whether owned by ANZCA or owned by employees, suppliers, providers or their respective staff and agents inclusive of smartphones and tablet computers, that access ANZCA ICT resources, confidential data, and systems governed by this mobile device security policy.

b) all applications used by employees, suppliers, providers and their respective staff and agents on their own personal devices which store or access corporate data.

As an exception, ANZCA reserves the right to exempt devices from this policy on a case-by-case basis.

4.7.1 Technical Requirements

a) Devices must store all user-saved passwords in an encrypted form.

b) Devices must be configured with a secure password that complies with ANZCA's password policy. This password must not be the same as any other credentials used within the organization.

c) Only devices managed or authorised by ANZCA ICT will be allowed to connect directly to the internal corporate network and will be subject compliance monitoring.

4.7.2 Compliance guidelines

- Users must always comply with the *ANZCA Acceptable Use of ICT resources Policy*.
- Sensitive or business-critical data must not be stored on mobile devices.
- Device screens must be locked with a passcode, fingerprint, face recognition etc.
- Device auto-lock must be enabled.
- If the device supports *'Remote Wipe',* this functionality must be enabled to enable ANZCA to erase a lost or stolen device.

4.8 Application Development Security

Controls will be enforced to ensure secure application development including:

- Ensuring alignment to the overall security strategy;
- Documenting application security requirements;
- Embedding security into solution design;
- Using secure coding principles;
- Using secure software libraries and ensuring code is protected at all time;
- Building security testing into the development pipeline;
- Separating Development from Production environments;
- Ensuring Production data is not used or de-identified before use;
- Ensuring changes to the development pipeline are change-controlled;

4.9 Third Party Risk Management

ANZCA partners with a range of suppliers and third-party service providers to deliver and maintain ITS services. To mitigate third party risks related to the use of third parties including vendors, suppliers, partners, contractors, or service providers, ANZCA will leverage the following processes

- Seek SOC2 Type 2 or ASAE 3150 certifications and accreditations for critical Tier1 suppliers and partners to assess the extent to which they comply with one or more of the five trust principles of Security, Availability, Integrity, Confidentiality, and Privacy based on the systems and processes in place.
- Complete security questionnaires for Tier2 and Tier3 suppliers and partners to identify potential weaknesses that could result in a data breach, data leak, or other forms of cyber-attack.
- Explore cost effective tools to conduct third party risk assessments for suppliers and partners based on publicly available information.

4.10 Incident Management

a) ANZCA must plan for response to information security incidents involving information assets. Response will be based on nature and severity of the incident, data involved, and other factors. The approach must include four phases:
    - **Preparation** - policies, stakeholder notification and technology acquisition.
    - **Detection** - detecting and confirming an incident has occurred, categorising, and prioritising the incident.
    - **Containment, Eradication and Recovery** - minimising the loss or theft of information or service disruption; eliminating the threat and restoring services quickly and securely.
    - **Post-Incident Activity** - submitting a formal closure report including lessons learned. This report must also contain recommendations for improvement, mitigation of exploited weaknesses and additional security controls to prevent similar incidents from occurring in the future.

b) ANZCA will build resilience and capability to effectively respond to incidents causing business disruption with artefacts detailing the Incident Response Plan, Business Impact Assessment (BIA), Business Continuity Plan (BCP), Disaster Recovery (DR) plan for critical infrastructure and resources, Communications and media liaison strategies, and Crisis management, recovery, and emergency planning. This includes

planning and preparation to ensure operational continuity, or recovery to an operational state within a reasonable timeframe, in the event of a business disruption.

5 Definitions

- **Availability** – ensuring authorised persons can access information when needed.
- **Confidentiality** – ensuring only authorised persons can access information.
- **Integrity** – providing assurance that information is only being created, amended, or deleted by authorised means and is correct and valid.
- **ICT assets** - ICT hardware, software, systems and services including voice, video and unified communication such as telephony and collaboration systems that are used in the department to process, store or transmit information such as computers, telephone systems, close circuit television (CCTV) and video surveillance systems, servers, switches, wireless network equipment, cabinets, scanners multifunctional printers, mobile phones, laptops, iPads, Surface Pros, digital cameras, electronic whiteboards, projectors etc.
- **Information Security** - Information security is the preservation of confidentiality, integrity, and availability of information, in addition to other properties such as authenticity, accountability, non-repudiation and reliability.
- **Information security management system (ISMS)** - An ISMS is part of an overall management system (a type of framework), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.
- **Personally Identifiable Information (PII)** - This is information that, on its own or combined, can be used to identify, locate, or contact an individual. Some examples of PII are obviously sensitive: Social Security number, credit card number, driver's license number, and account numbers. Others are less obvious but just as important: full name, date of birth, home address, phone number, employment history, purchase history, email address, or even a photo of an individual's face.
- **Protected Health Information (PHI)** - This is a subset of PII that is protected by the HIPAA Privacy Act of 1996. PHI is information that can be used to identify an individual AND that relates to that individual's past, present, or future physical or mental health care or health care payments. Some examples of PHI are all PII gathered while providing health services, or prescription drug records, health plan number, status in a government health program, and dates of hospitalization.
- **Privileged Accounts**
    - Privileged Personal Accounts (DBA, Server Administrator, Tenant Admin, Domain Admins) assigned to individual users (IT Support Staff). Examples include the following privileged groups.
    - Generic/Shared Administrative Accounts (Windows Administrator, UNIX root, Oracle SYS, SA) - accounts used by multiple users that hold "super user" privileges and are often shared among IT Support staff.
    - Break Glass (Emergency) Accounts or Generic/Shared Administrative Account used when elevated privileges are required for business continuity, disaster recovery, or to fix urgent problems.

- Service Accounts that provide a security context to a running service, daemon, or process such as a file server, web server, e-mail server, etc., or are used by applications to access databases etc.

- **Sensitive data** - Classes of data with a high level of security that ANZCA is legally or contractually required to protect under Privacy, Legislation, or any other data that has been identified as business-critical or business-sensitive, such as financial records, intellectual property, or other confidential information of ANZCA.

6 Related Documents

- ANZCA Privacy Policy
- ANZCA Information Security Classification Framework
- ANZCA Acceptable Use of ICT resources Policy
- ANZCA Employee Code of Conduct
- ANZCA Electronic Communications Policy

7 Policy Review and Change Control

Version	Policy Owner	Approved by	Approval Date	Section Modified	Next Review Date
1.0	ED-CIO	ICTGC	Nov-2023	Created to replace the ANZCA ICT Security Policy dated Apr-2016	Nov-2026