INFORMATION SECURITY POLICY

Version No: 1.0 | Author: General Manager ICT | Next Review Date: 2026/01

1. Purpose

The MACG Information Security Policy defines the guiding principles to securely manage information throughout its lifecycle within MACG environments and ensure Confidentiality, Integrity, and Availability.

This policy is aligned to the *MACG Privacy Policy* and *MACG Acceptable Use of IT Resources Policy* and will enable MACG to align with recommendations within ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements.

The policy applies to:

a) all technology resources used by, operated by, or provided on behalf of MACG.

b) all information collected, created, stored, or processed by, or for MACG 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 MACG. This includes all staff (full-time, part-time, casual), contracted and agency staff, students, volunteers, suppliers, partners, contractors, sub-contractors, or affiliated organisations.

All persons to whom this policy applies are required to comply with the terms of this policy as well as all applicable legislation.

2. Policy

MACG will apply a consistent, risk-based approach to information security that maintains the Confidentiality, Integrity, and Availability of information by protecting against unauthorised disclosure, access or use, loss, or compromise (malicious or accidental), or a breach of privacy.

This includes identifying and managing risks to information, applications, and technologies, throughout their lifecycle by implementing an Information Security Management System (ISMS) aligned to ISO/IEC 27001 standards.

This policy does not just apply to digital information, but extends to hardcopy records, and unstructured content including but not limited to content in emails, notepads, conversations, chats etc.

3. Principles

- MACG 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 team, IT Security, or Systems Administrators to protect information but everyone's responsibility to play their part in protecting MACG information:

  a) All users are responsible for understanding and complying with MACG policies and manage MACG 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 MACG 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

In addition to the guiding principles, below is an overview of key Information Security domains providing direction on how MACG intend to manage Information securely:

4.1 HUMAN RESOURCE 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) MACG will perform checks (compliance checks) to ensure that each individual user is suitable to be given access to the MACG 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 MACG, user access must be suspended or removed from ICT systems.

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 MACG 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 MACG ICT resources must ensure appropriate authorisation to systems and services.

c) User registration and de-registration process should ensure

- appropriate authorisation prior 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) Privilege Management must adhere to the following 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 (15 characters or more) and 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 credentials are suspected to be compromised. .
- email alerts when a login is detected from a new device or new location.

j) All smart devices containing MACG 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 MACG.

l) Privileged user access to MACG 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 MACG approved Privileged Account Management (PAM) platform to ensure they remain available to system administrators.

4.3 ASSET MANAGEMENT

a) Information held must be assessed and classified based on the level of protection required. Commonwealth data classification levels include five categories - Unclassified, Protected, Confidential, Secret, and Top Secret (not used by MACG).

b) 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 MACG if the information is disclosed, misused, misrepresented, or lost.

Below is a guideline for classification:

IMPACT TYPE	SEVERITY			
Impact	**Insignificant to Minor**	**Moderate**	**Major**	**Severe**
Competitive advantage	Little or no advantage.	Might provide some advantage.	Definite advantage.	Significant Advantage.
If this asset or information is disclosed, stolen, or lost.				
Business Operation and service.	Some localised inconvenience, but no impact to MACG. Disruption to operations. No permanent or significant impact to MACG	Some impact on MACG's operational performance. Less impact on strategic goals in the medium term.	Significant effect on operational performance.	Achievement of operational and strategic goals in the medium term jeopardised. Existence of MACG under threat.
Compliance / Legal	Breach of legislation, contract, rule, or policy that does not have any	Breach of legislation, contract rule or policy leading to escalated legal enquiries.	Breach of legislation, contract, rule or policy leading to possible legal action.	Breach of legislation, contract, rule, or policy leading to significant and costly legal action with widespread

IMPACT TYPE	SEVERITY			
Impact	**Insignificant to Minor**	**Moderate**	**Major**	**Severe**
	penalty or litigation impact. Breach of legislation, contract, rule, or policy. May impact on relationship with third party or legislator. No long-lasting effect, litigation, prosecution and/or penalty. Regulatory consequence of standard inquiries.	Regulatory or legal consequence limited to additional questioning or review by legislator.	Possible litigation or criminal prosecution and/or penalty. External enquiry or regulatory review and/or possible negative sanction by a regulatory body.	potential impact for MACG. Litigation or criminal prosecution and/or substantial major negative sanction by a regulatory body.
Employees / WHS	No impact to employees / WHS	Continuity of employment concerns across MACG. WHS incident requiring significant medical attention. WHS event reported and investigated.	Significant (up to 15%) loss of staff contained to one facility. Widespread damage to staff morale. WHS event causing serious injury, or negative environmental impact, and external authority notified.	Significant loss of staff extending to entire MACG (over 15%). WHS event causing serious permanent injury, death or environmental. Impact leading to costly action and widespread impact MACG and/or senior staff.
Financial	Less than 1% of budget or up to $25K. 1 to 2% of budget or $25-50k.	2-5% budget or $250k – 1m.	5-10% budget or $1-5m.	Over 10% of budget or over $5m.
Reputation	No impact to reputation.	Customer and/or community concern. National media coverage and external criticism. Reputation impacted with some stakeholders.	Loss of customer confidence at a facility. Sustained adverse media/public coverage. Reputation impacted with multiple stakeholders.	Loss of customer confidence. Serious public outcry and/or media coverage. Reputation impacted with majority of stakeholders.

IMPACT TYPE	SEVERITY			
Impact	**Insignificant to Minor**	**Moderate**	**Major**	**Severe**
			Breakdown in strategic or business partnership.	Significant breakdown in strategic and or business partnerships.
Service Levels	Loss of less than one day's business functions. Loss of one full day of business functions.	Loss of 1-7 days of business functions.	Loss of two weeks to two months of business functions.	Loss of over two months of business functions.
Example information types	MACG staff directory information. MACG Catalogues and published MACG data.	MACG process and procedure. Unpublished IP System design information	Customer or Employee HR Data. MACG financial data.	Data subject to regulatory control. ER/Complaints information. Medical, CC information.
DATA CLASSIFICATION	Consider for **PUBLIC OR UNCLASSIFIED**	Consider for X – **In Confidence**	Consider for **Restricted**	Consider for **HIGHLY Restricted**

4.4 PHYSICAL & ENVIRONMENTAL SECURITY

4.5 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) All data and software must be erased from equipment prior to disposal or redeployment. Asset inventories must be updated to record details of the data wiping.

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

4.6 SECURE AREAS

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.

4.7 OPERATIONS MANAGEMENT

Key business stakeholders of MACG systems will be referred to as MACG System Owners in this section.

a) MACG System Owners must ensure that their 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 environments to reduce the risk of unauthorised access or accidental damage their integrity or contents.

c) All changes to MACG ICT services and system environments, including provisioning and de-provisioning of assets, promotion of code, configuration changes and changes to SOPs must be authorised by MACG IT Change Advisory Board (CAB).

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

e) 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.

f) MACG 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 may be configured to alert relevant teams if certain events or signatures are detected.

g) Activities of privileged users must be logged, and the logs must be periodically reviewed.

h) Vulnerability assessments and penetration tests should be conducted before a system is deployed, after a significant change to a system, and at least annually or as specified by the system owner. To support technical vulnerability management, an inventory of ICT assets must be maintained.

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

j) 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.

4.8 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 must be divided into multiple functional network zones according to the sensitivity and criticality of information and services. Database servers and web servers should be functionally separated, physically or virtually.

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 a MACG-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.

f) Bring your own device (BYOD) access to MACG 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 solutions.

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

4.9 INCIDENT MANAGEMENT

a) MACG must plan for responding to information security incidents involving ICT resources and 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 the nature of the incident and then 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) MACG Business Continuity Management framework will build resilience and capability to effectively respond to incidents causing business disruption. 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. Focused on the safety and resilience of people, property, processes, systems, and providers as well as the availability and integrity of information, it involves the following:

- Business Impact Assessments (BIA)
- Business Continuity Plans (BCP)
- Disaster Recovery (DR) planning for critical infrastructure and resources.
- Communications and media liaison strategies; and
- Crisis management, recovery, and emergency planning.

5. Mobile Device Security Policy

5.1 OVERVIEW

Mobile devices represent a significant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection.
MACG has a requirement to protect its information assets to safeguard its residents, confidential information, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices and applications.

5.2 SCOPE

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

b) MACG may consider and determine whether any devices are exempted from this policy on a case-by-case basis.

c) Applications used by employees, suppliers, providers and their respective staff and agents on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

5.3 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 MACG'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 MACG ICT will be allowed to connect directly to the internal corporate network and will be subject compliance monitoring.

5.4 USER REQUIREMENTS

a) Users may only load corporate data that is essential to their role onto their mobile device(s).

b) Users must report all lost or stolen devices to MACG ICT immediately.

c) If a user suspects that unauthorized access to company data has taken place via a mobile device, they must report the incident in alignment with MACG's data breach requirements.

d) Devices must not be "jailbroken" or "rooted" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

e) Users must not load pirated software or illegal content onto their devices.

f) Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source, contact MACG ICT.

g) Devices must be kept up to date with manufacturer or network provided patches. As a minimum, patches should be checked for weekly and applied at least once a month.

h) Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with MACG policy.

i) Devices must be encrypted in line with MACG's compliance standards.

j) Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that MACG data is only sent through the MACG email system. If a user suspects that MACG data has been sent from a personal email account, either in body text or as an attachment, they must notify MACG ICT immediately.

k) The above requirements will be checked regularly, and should a device be non-compliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.

l) The user is responsible for the backup of their own personal data and MACG will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.

m) Users must not use corporate workstations to backup or synchronize device content such as media files unless such content is required for legitimate business purposes.

n) The use of solutions and applications not authorised by MACG ICT will imply a compliance breach and the loss of access to the MACG ICT resources for the user.

o) In case of 3rd party personal devices not issued by MACG, users must ensure that the device(s) have adequate and up-to-date anti-malware and threat protection at all times. Users must immediately notify MACG of any potential threat to their device which may have the potential to impact MACG ICT systems and networks.

5.5 INSTANCES REQUIRING IMMEDIATE ACTION

The following instances may require a full or partial wipe of the device, or other intervention:

a) A device is jailbroken/rooted.
b) A device contains an app known to contain a security vulnerability (if not removed within a given timeframe after informing the user).
c) A device is lost or stolen.
d) A user has exceeded the maximum number of failed password attempts.

5.6 CCOMPLIANCE GUIDELINES

Users must comply at all times with the MACG *Acceptable use of IT Resources Policy*.

5.7 OTHER REQUIRED BEST PRACTICES

- Sensitive or business-critical data must not be stored on mobile devices.
- Device screen must be locked with a passcode, fingerprint, face recognition, or similar method.
- Device auto-lock must be enabled.
- If the device supports “Remote Wipe” this functionality must be enabled to permit the end-user to erase a lost or stolen device.

5.8 ADDITIONAL RECOMMENDED SAFEGUARDS

- Always verify the authenticity of an email, text, and telephone call. Mobile devices unfortunately only show the user’s name and not the actual email address from which a message was sent. These names are often spoofed to mimic someone you may typically know and trust.
- Never click links in emails or text messages from untrusted sources and verify the source of the message even with trusted sources.
- Always verify callers’ information recognizing many scams involve spoofing Banks, ATO, or Social Security Administration asking for personal banking information. Always verify by initiating a call to a known number.
- Keep a close eye on URLS, avoid ads, giveaways, “free” applications that are likely too good to be true. These could be phishing sites used to steal your information.
- Be cautious of the permissions you give installed applications to read other information on your personal phone, this includes phones, text message, contact lists, lists, etc. Many free applications use this information to mine or sell personal data.
- When discarding used technology, follow the manufacturers recommendations on how to properly wipe the technology so that your data doesn’t fall into someone else’s hands.

6. MACG Business Systems

Below is a view of MACG business systems and the types of information held on them.

- Clinical Care & Medication (PHI, PII)
- Dietary Information (PHI, PII)
- Communication Systems (Vocera, Video Conferencing, Messaging)
- Nurse Call / Facility Annunciator System
- Consumer Feedback (PII)
- Quality & Compliance (PHI, PII)
- Human Resources Information Systems (PII, Financial)
- Time & Attendance (PII)
- Payroll (PII)
- Workplace Health and Safety (Incident/Injury) (PII)
- Learning Management (PII)
- Financial, P2P, AR, AP, Billing, Procurement (PII, Financial)
- Reporting (PII, PHI, Financial)
- Website (PII)
- Content Management System, Intranet, Corporate documents (Miscellaneous)
- Email & Archive (PII, PHI, Financial, Miscellaneous)
- E-marketing (PII)
- Building Management Systems (Access control, CCTV, Fire, Solar, Electricity, Water etc.) (PII)
- ICT Infrastructure (Network, Telephony, Wifi etc)

7. Definitions

- **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.

- **ISO/IEC 27001:2013**

  An international standard that provides a model for establishing, implementing, maintaining and continually improving an information security management system within an organisation. This international standard also includes requirements for assessing and treating information security risks tailored to the needs of the organisation.

- **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. PII is legally protected by many state laws and good business practices.

- **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 any and all PII gathered in the course of providing health services, medical, dental, or prescription drug records, insurance coverage, 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 MACG is legally or contractually required to protect under Privacy, Legislation, or otherwise, 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 MACG.

8. Related Documents

- Privacy Act, 1988
- Privacy Amendment (Notifiable Data Breaches) Act 2017
- Australian Privacy Principles (APP)
- MACG Privacy Policy
- MACG Acceptable Use of IT Resources Policy