IT Security Policies and Procedures

1. Policy Title

IT Security Policies and Procedures

2. Purpose

This policy establishes the controls [Practice Name] uses to protect clinical information systems, patient data, and connected devices from unauthorised access, misuse, and cyber threats. It aligns with criterion F8 – Information security of the RACGP Standards for general practices (6th edition), which significantly strengthens digital health and cybersecurity expectations.

3. Scope

This policy applies to all staff, contractors, and third parties who use, manage, or support the practice's information technology and digital health systems.

4. Definitions

- Information system: Any system used to create, store, transmit, or process information, including the clinical information system (CIS), practice management software, email, and connected devices.
- Cybersecurity incident: An event that compromises, or threatens to compromise, the confidentiality, integrity, or availability of information or systems.
- Multi-factor authentication (MFA): Authentication using two or more independent factors.
- Endpoint: Any device that connects to the practice network (workstation, laptop, tablet, phone, medical device).

5. Principles

- Patient information is protected by layered, defence-in-depth controls.
- Access is granted on a least-privilege, role-based basis.
- Digital health records are the source of truth; paper-only clinical records are not acceptable under criterion CG1 of the 6th edition.
- Cybersecurity risks are actively managed alongside clinical and operational risk.
- Business continuity and disaster recovery are tested regularly.

6. Access Control

- Each user has a unique account with a strong passphrase; sharing of credentials is prohibited.
- Multi-factor authentication (MFA) is enabled for all systems that support it, including remote access, email, and the clinical information system.
- Role-based access ensures staff see only the information they need.
- Administrator accounts are separate from routine use accounts.
- Access is reviewed when staff change roles and revoked promptly on termination.

7. Endpoint and Network Security

- All endpoints run current, supported operating systems with automatic security updates.
- Endpoint protection (antivirus/EDR) is installed and active on all devices.
- Screen lock engages automatically after a short period of inactivity.
- Wi-Fi networks use WPA2/WPA3 encryption; a guest network separates visitor devices from clinical systems.
- Firewalls are enabled and configured to deny inbound traffic by default.

8. Data Protection

- Patient data is encrypted at rest where supported by the clinical information system.
- Backups are encrypted, automated, and stored securely offsite or in the cloud; backups are tested for restorability at least quarterly.
- Removable media is encrypted and used only where authorised.
- Mobile devices accessing clinical data are managed by an MDM solution enabling remote wipe.

9. Email, Web, and Telehealth

- Email uses a business-grade service with anti-phishing, anti-malware, and SPF/DKIM/DMARC configured.
- Staff are trained to recognise phishing and to report suspicious messages.
- Telehealth platforms used are accredited and end-to-end encrypted.

- Cloud services are assessed for compliance with the Australian Privacy Principles and the Australian Government Information Security Manual (ISM) / Essential Eight as relevant.

10. Cybersecurity Incident Response

- Suspected incidents (phishing, ransomware, unauthorised access) are reported immediately to the IT Security Officer.
- Incidents are triaged, contained, and investigated; affected systems may be isolated.
- Privacy impacts are assessed in parallel; the Privacy Officer engages the OAIC Notifiable Data Breaches process where required.
- A post-incident review identifies root causes and corrective actions.

11. Business Continuity and Disaster Recovery

- A business continuity plan covers loss of systems, premises, key personnel, and suppliers.
- A disaster recovery plan defines recovery time and recovery point objectives and is tested at least annually.
- Critical clinical workflows have documented manual fallback procedures.

12. Roles and Responsibilities

IT Security Officer (Practice Manager or IT provider):

- Maintains this policy and the IT asset register.
- Coordinates patching, backups, MDR, and incident response.

All staff:

- Follow access, email, and endpoint security requirements.
- Report suspicious activity or devices immediately.

13. Monitoring, Audit, and Review

- Quarterly review of access logs, patch status, and backup restorability tests.
- Annual review of this policy, the business continuity plan, and the disaster recovery plan.
- Annual cybersecurity awareness training for all staff.

14. Documentation and Record Keeping

The practice maintains:

- An IT asset register.
- User access lists and change records.
- Backup and recovery test reports.
- Cybersecurity incident reports and outcomes.
- Staff IT security training records.

15. References

- The Royal Australian College of General Practitioners. Standards for general practices (6th edition). East Melbourne, Vic: RACGP; published 26 August 2026. Available at: https://www.racgp.org.au/running-a-practice/practice-standards/standards-6th-edition
- Australian Cyber Security Centre. Essential Eight Maturity Model. Available at: https://www.cyber.gov.au
- Australian Government Information Security Manual (ISM). Available at: https://www.cyber.gov.au
- Office of the Australian Information Commissioner. Notifiable Data Breaches scheme. Available at: https://www.oaic.gov.au

---

Version Control

Policy title: IT Security Policies and Procedures

Version: 2.1

Effective date: 27 August 2026

Next review date: 27 August 2027

Policy owner: IT Security Officer / Practice Manager

Aligned to: RACGP Standards for general practices (6th edition, published August 2026)