Alphacrucis University College

Cybersecurity Policy

Effective Date: 2025.12.04
Last Reviewed: 2025.09.18
Version: v2 2025.09.18

1. Purpose

This Cybersecurity Policy establishes a structured framework to safeguard Alphacrucis University College's digital information, systems, and infrastructure. The primary aim is to progressively ensure the confidentiality, integrity, and availability of institutional data. This policy aligns with relevant legal, regulatory, and educational standards. It also serves to guide the implementation of robust cybersecurity controls, while fostering a culture of security awareness and shared responsibility among all users.

2. Scope

This policy applies to all individuals and digital assets that interact with the University's information systems. It includes:

- All employees, contractors, and third-party vendors who access university resources;
- All students who utilise university-owned platforms and systems;
- All computing devices, software applications, network services, and cloud-based technologies connected to Alphacrucis University College's infrastructure.

3. Policy Statement

3.1. This section outlines the foundational principles guiding Alphacrucis' approach to cybersecurity. These principles represent the philosophical and operational basis on which all other security practices are established.

3.1.1. **Risk Management:** Cyber risks are dynamic and will be continuously evaluated and managed based on their potential impact on the institution's operations, data, and reputation. Risk assessments will inform security controls, policy updates, and mitigation strategies across systems and business units.

3.1.2. **Data Protection:** The College is committed to the confidentiality, integrity, and availability of its data. This includes safeguarding sensitive information such as academic records, personnel files, and proprietary research. Protections will extend across all stages of data processing — from creation to archival — and apply to both physical and digital forms.

3.1.3. **Compliance:** Cybersecurity practices at Alphacrucis will align with applicable laws and frameworks, including the Australian Privacy Act 1988, TEQSA requirements, and ACSC guidelines. Compliance efforts will be documented and reviewed regularly to ensure sustained accountability.

3.1.4. **User Responsibility:** Security is a shared responsibility. Every user — whether staff, student, or vendor — is expected to act with diligence, adopt secure practices, and report potential threats. Awareness and compliance at the user level is key to maintaining an effective security posture.

3.2. **Governance**

3.2.1. Cybersecurity governance is essential to maintaining consistent and accountable security practices across the College. The IT Team, reporting to the Vice President — Operations, will lead the implementation of this policy. To support continuous improvement, periodic

internal reviews and third-party assessments, such as the ACSC's Essential Eight maturity model, may be employed to evaluate progress and guide enhancements.

3.3. **Security Controls**

3.3.1. To operationalise its cybersecurity principles, Alphacrucis has implemented a range of layered security controls. These controls span system access, device management, network segmentation, data encryption, secure development, and more. Each is outlined below.

3.3.2. **Access Management**

Access to digital resources will be regulated based on identity, role, and business need:

a. Every user will be assigned a unique ID to ensure traceability and accountability;
b. Role-Based Access Control (RBAC) will be enforced, restricting data access according to predefined roles and responsibilities;
c. Multi-Factor Authentication (MFA) is mandatory for staff, students, and contractors to provide an additional layer of defence;
d. Access rights will be reviewed quarterly to ensure ongoing appropriateness and to reduce exposure.

3.3.3. **Endpoint Protection**

Endpoints such as desktops, laptops, and mobile devices must be secured whether they are university-managed or personally owned:

a. Institution-owned devices must be equipped with antivirus software, host-based firewalls, and full-disk encryption;
b. Personally owned devices that connect to university systems must utilise secure access technologies such as virtual private networks (VPNs);
c. IT will monitor endpoint compliance and may restrict access for non-compliant devices.

3.3.4. **Network Security**

Network infrastructure will be fortified using modern security tools and methodologies:

a. Sensitive systems will be segmented from general-use networks to limit lateral movement in the event of compromise;
b. Firewalls, intrusion detection systems (IDS), and anomaly detection tools will be deployed to monitor and block unauthorised traffic;
c. Regular vulnerability scans and scheduled penetration testing will be used to proactively identify and address weaknesses.

3.3.5. **Data Security**

All institutional data must be protected according to its classification and sensitivity:

a. Encryption will be used for data in transit (e.g., transmitted over networks) and at rest (e.g., stored on disks) where technically feasible;
b. Cloud storage providers should preferably be based in Australia or certified by IRAP (Information Security Registered Assessors Program);
c. Backups and disaster recovery plans are to be maintained and tested regularly for critical systems.

3.3.6. **Secure Development**

Development and maintenance of software must adhere to secure engineering principles:

a. All in-house development projects will follow secure coding standards and undergo regular code reviews;

b. Third-party and open-source libraries must be vetted for vulnerabilities before integration;
c. Patching will follow a consistent schedule: operating systems and major applications will be patched automatically, while platforms like Moodle follow structured release cycles. Hardware patching will occur on an ad hoc basis based on vendor guidance.

3.3.7. **Incident Response**

Quick and effective response to security incidents is crucial to limiting damage:

a. All users must report suspected cybersecurity incidents to the IT Team within 30 minutes of discovery;
b. Incidents deemed critical will be escalated to senior leadership and, where required, reported to the Australian Cyber Security Centre (ACSC) as per national guidelines.

3.3.8. **Awareness and Training**

Building a security-aware culture is central to the success of this policy:

a. All staff will have access to the cybersecurity training software and are monitored and encouraged to complete the training every six months;
b. Phishing simulations will be conducted periodically throughout the year using a third-party cybersecurity training tool that has been evaluated and is managed by the IT team;
c. Ongoing guidance and resources will be provided to promote secure usage of common platforms such as email, Microsoft 365, and mobile applications.

3.4. **Third-Party and Vendor Risk**

External vendors and partners can introduce cybersecurity risks and must be managed accordingly:

a. All third-party vendors handling institutional data must sign a data protection agreement that outlines their responsibilities and liabilities;
b. Critical vendors will be reviewed periodically to assess their security posture and performance;
c. Cloud service providers must demonstrate compliance with ISO 27001 or comparable security certifications.

3.5. **Policy Compliance**

To enforce accountability, policy adherence is mandatory:

a. Violations of this policy may result in disciplinary action, which may include access restrictions, HR involvement, or termination;
b. Any deviations from the policy must be formally documented and approved in writing by the Director of IT.

---

4. Roles and Responsibilities

4.1. The Director of IT is responsible for the overall implementation, monitoring, and enforcement of this policy.

4.2. All staff, students, and contractors are responsible for complying with the requirements set out in this policy and for reporting any suspected cybersecurity incidents promptly.

---

5. Procedures

5.1. Procedures supporting this policy, including incident response procedures and access management processes, are maintained by the IT Team and reviewed periodically in alignment with this policy's review cycle.

6. Responsible for Implementation

Director IT

7. Related AC Policies or Documents, Standards and Legislations

7.1. AC Policies or Documents

7.1.1. Electronic Publishing and Resource Use Policy.

7.2. Relevant Standards and Legislation

7.2.1. Privacy Act 1988 (Cth);
7.2.2. TEQSA Act 2011 (Cth) and associated standards;
7.2.3. Australian Cyber Security Centre (ACSC) Essential Eight Framework;
7.2.4. ISO/IEC 27001 Information Security Management.

8. Review and Revision

This policy is a living document and will be reviewed:

- Annually, as part of the College's broader governance and compliance cycle; or;
- After any major security incident, audit recommendation, or regulatory update that materially affects its scope or implementation..

9. History of Approval and Amendments

Policy owner	Director IT
Policy category	Governance: Council
Policy status	Approved
Approval Body	Council
Endorsement Body	Executive
Approval Date	2026.03.31
Last Review Date	2026.01.31
History of Policy Amendments	
V1 2025.08.14	Creation of policy — requested by Finance & Audit Committee
V2 2025.09.18	Update to section 3.3.7 based on feedback from Council; new template

Add a new row for each version of the policy. Do not remove previous changes.

Appendices

- N/A.