POLICY		
Ref. to Legislative Frameworks in Point 13	**Cyber Security and Foreign Interference**	
Version: 1.0	Policy Owner: Board of Directors	Issued on: 10/06/2026 Review by: 10/06/2028

Revision History

Version	Description of Change	Policy Developer	Effective Date
1	AAPoly-specific Cyber Security Policy derived from Academies Australasia Group Cyber Security Policy v2 (May 2026). Adapted for HE / VET context at AQF Levels 7 and 9; comments resolved; role-title terminology standardised; foreign interference section scoped to AAPoly HE operations; data classification confirmed.	Group General Manager, Cyber Security / CEO	June 2026

1. PURPOSE

This policy sets out how Academies Australasia Polytechnic (AAPoly) protects its digital systems, information, and data from cyber threats and foreign interference. AAPoly operates across two regulated sectors:

- Higher Education (HE): regulated by TEQSA under the Higher Education Standards Framework (HESF 2021). Cyber security and foreign interference are identified as sector risks under Standards 2.3.4, 2.3.5, 5.2.2, 6, and 7.3.3(b). Standard 2.3.4 directly requires providers to manage risks to academic integrity, research integrity, and information security.
- Registered Training Organisation (RTO): regulated by ASQA under the Standards for Registered Training Organisations (NVETR Instrument 2025). RTOs must incorporate cyber security into their risk management systems, particularly to protect personal and sensitive student information.

This policy applies to all staff, contractors, students accessing AAPoly systems, and any third party operating on behalf of AAPoly. It directly addresses the cyber security risks identified across both sectors and demonstrates AAPoly's commitment to robust, transparent, and accountable cyber governance.

2. SCOPE

This policy applies to:

- All AAPoly campuses and all sectors (Higher Education and VET).
- All staff, contractors, consultants, sessional and casual staff, and volunteers engaged by AAPoly.
- IT systems, networks, applications, and data; whether hosted on-premises or in the cloud.
- Third-party service providers who access AAPoly systems or data.
- Students insofar as they use AAPoly-provided systems, accounts, or platforms.
- Learning Management Systems (LMS) and other platforms used for course delivery, including student management systems operated by third-party providers.

3. DEFINITIONS

ASD Essential Eight is a prioritised set of baseline cybersecurity mitigation strategies developed by the Australian Signals Directorate (ASD). It is designed to make it significantly harder for adversaries to compromise organizations' internet-connected networks by addressing the most common cyber-attack techniques (Australian Signals Directorate, 2026). The eight controls include:

Control	Definition
Application Control	Preventing unapproved or malicious programs from running on systems.
Patch Applications	Applying security patches and updates to applications within defined timeframes.
Configure Microsoft Office Macro Settings	Restricting macro execution to approved, digitally signed macros only.
User Application Hardening	Configuring browsers and email clients to block malicious content.
Restrict Administrative Privileges	Limiting admin access to those who require it, with separate accounts for daily use.
Patch Operating Systems	Keeping OS software up to date with security patches applied promptly.

Multi-Factor Authentication (MFA)	Requiring a second form of verification beyond a password for access to systems.
Regular Backups	Maintaining daily encrypted backups stored separately and tested regularly.

ASD Information Security Information Security Manual (ISM) is a comprehensive cybersecurity framework. It provides strategic principles and practical guidelines to help organizations protect their information and operational technology systems, applications, and data from cyber threats. Developed by the ASD, the ISM is the overarching standard for Australian Government agencies and is highly recommended for the private sector (Australian Transformations Agency, 2026)

Cyber Attack is a deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information resident on them, with the effect of seriously compromising national security, stability or economic prosperity (Australian Signals Directorate, 2026).

Foreign interference is covert, deceptive, or coercive activity carried out by, or on behalf of, a foreign principal or foreign state, intended to secretly influence an individual, institution, or government process in a way that is contrary to Australia's national interests. (Australian Government Department of Home Affairs, 2026).

Foreign principal means a foreign government, a foreign political organisation, a foreign government-related entity, or any foreign individual or organisation acting on behalf of, under the direction of, or in the interests of a foreign state or foreign political body (Australian Government Attorney-General's Department, 2025).

Foreign-state actors mean any foreign government, government-related body, or proxy acting on behalf of a foreign state to influence, interfere with, or exploit the Group's activities, people, systems, or information (Australian Federal Police, 2026).

4. POLICY STATEMENT

Academies Australasia Polytechnic (AAPoly) is committed to maintaining the confidentiality, integrity, and availability of all information it holds. In fulfilment of this commitment, and in accordance with its obligations as a registered higher education and vocational education and training provider, AAPoly embeds cyber security as a core component of its organisational risk management system. AAPoly will ensure that appropriate technical, governance, and human controls are in place across all campuses, systems, and sectors to protect student, staff, and institutional information from unauthorised access, misuse, or harm, including harm arising from covert, deceptive, or coercive activities by foreign actors.

This commitment is operationalised through four pillars:

- Risk Management. AAPoly integrates cyber security and foreign interference risk into its enterprise risk management framework, with particular attention to the protection of personal and sensitive student information in accordance with the Privacy Act 1988 and applicable sector standards.
- ASD Essential Eight. AAPoly's technical controls are aligned to the Australian Signals Directorate (ASD) Essential Eight Maturity Model, which represents best practice for protecting internet-connected networks and systems. The framework encompasses application control, patch management, multi-factor authentication, and regular backups, among other controls. Refer to Section 5 for detailed control requirements.
- ASD Information Security Manual (ISM). AAPoly draws on the ASD Information Security Manual as supplementary best-practice guidance for information security governance, particularly in the higher education and VET contexts.

- Governance and Compliance. Cyber security and foreign interference risks treated as a governance priority, addressed through compliance with the Privacy Act 1988, the ESOS Act 2000, the National Code of Practice, the Foreign Influence Transparency Scheme, TEQSA and ASQA regulatory requirements, and AAPoly's broader organisational governance framework.

5. FOREIGN INTERFERENCE RISK

AAPoly operates in an environment of significant international engagement. AAPoly's HE operations place a strong focus on research-informed practice, critical thinking, evidence-based decision-making at AQF Levels 7 and 9, and support for international student and staff pathways. TEQSA and the Australian Government recognise foreign interference as a serious issue for higher education and research integrity. These concerns are especially important in higher education because providers operate in open, globally connected, and internationally engaged learning environments. While the overwhelming majority of international student enrolments and staff appointments are positive for Australia's research, cultural, and economic interests, foreign state actors have a capacity to exploit these pathways.

This section establishes the obligations of AAPoly to identify, assess, and mitigate risks of foreign interference arising through the recruitment, enrolment, and employment of students and staff.

Recruitment-related risks may manifest in, but are not limited to, the following forms:

- Recruitment of students or staff by foreign intelligence services, state-affiliated entities, or their proxies for the purpose of gathering sensitive information or influencing institutional decisions.
- The placement of individuals in roles or study programmes at the direction or instigation of a foreign principal.
- The use of government-sponsored scholarship schemes by foreign states to create dependency or obligation in recipients, including implicit or explicit expectations of loyalty, information-sharing, or ideological alignment.
- Coercion, surveillance, harassment, or intimidation of students or staff (whether online or in person) by agents of a foreign government, including acts targeting individuals based on their ethnicity, nationality, religion, political opinion, or diaspora identity.
- Exploitation of student-led associations, clubs, or cultural organisations by foreign-state actors as platforms for monitoring, influencing, or reporting on members of the community.
- Undue influence over staff recruitment and promotion decisions through foreign-funded endowments, gifts, or third-party arrangements that create conflicts of interest or conditional obligations.

5.1 Actions AAPoly Will Take to Address Foreign Interference Risk

- Screen and assess risks associated with international partnerships, research collaborations, and third-party and vendor relationships.
- Implement proportionate due diligence measures across the student recruitment lifecycle, including documented screening processes for high-risk enrolment pathways.
- Implement proportionate risk-based measures in staff recruitment and employment processes, including appropriate declarations regarding membership of, affiliation with, or obligation to foreign government bodies, foreign political organisations, or foreign state-linked entities that may give rise to a conflict of interest or a foreign influence transparency obligation. For the purposes of this policy, a foreign government body or foreign political organisation includes any entity controlled by, operating at the direction of, or substantially funded by a foreign state, government agency, or foreign political party.

- Restrict access to sensitive student, financial, and operational data on a need-to-know basis.
- Train staff to recognise social engineering and foreign interference tactics.
- Report any suspected foreign interference incidents involving student or staff recruitment pathways to the Department of Education.
- Comply with the Foreign Influence Transparency Scheme (FITS) as applicable. AAPoly operates in a highly international environment; foreign influence risks can arise through recruitment, scholarships, research, collaborations, alumni networks, and third-party arrangements. TEQSA and the Department of Education treat foreign interference as a serious higher education and research issue, and this policy reflects that governance expectation.
- Ensure senior management and the Academic Board stay abreast of existing and emerging threats to inform and support the whole-of-organisation risk mitigation strategy, in accordance with TEQSA Domain 6 expectations (governance and accountability; risk management).

5.2 Data Classification

AAPoly classifies data into the following categories to determine appropriate handling and protection:

Classification	Examples	Protection Level
RESTRICTED	Student visa details, financial records, HR data, TEQSA / ASQA compliance documents, personal information under the Privacy Act 1988	Highest: MFA required, logged access, encrypted at rest and in transit
CONFIDENTIAL	Internal policies, staff performance records, contracts, course delivery plans, research data, intellectual property	High: role-based access, encrypted storage in Google Drive
INTERNAL	Operational guides, internal communications, meeting minutes	Moderate: staff access only
PUBLIC	Marketing materials, published course information, website content	Standard: no special controls required

6. CYBER SECURITY FRAMEWORK: ASD ESSENTIAL EIGHT

AAPoly's cyber security controls are aligned to the ASD Essential Eight Maturity Model. The target is Maturity Level 2 (ML2) across all eight controls, with a roadmap to Maturity Level 3 (ML3) for highest-risk systems. The current maturity level for each control and the date of assessment is recorded in the IT Risk Register, maintained by the Manager, Cyber Security.

This framework applies to all AAPoly campuses across all sectors and is consistent with both TEQSA's and ASQA's alignment to ASD frameworks for education provider governance. The Manager, Cyber Security is responsible for monitoring and reporting on maturity progress.

6.1 Application Control

Only approved and allowlisted applications may be installed or run on any AAPoly-managed device. IT maintains an approved software register. Unapproved software must not be

downloaded or installed. Approval for new applications is sought through the IT Manager, who escalates to the Cross-Functional Tool Approval Panel where required.

6.2 Patch Applications

All applications — particularly internet-facing software such as web browsers, Microsoft Office, and the Student Management System — must be patched within 48 hours of a critical patch being released. Non-critical patches are applied within 14 days. IT is responsible for monitoring and applying patches.

6.3 Configure Microsoft Office Macro Settings

Microsoft Office macros are disabled by default on all AAPoly devices. Macros from the internet are blocked. Where macros are required for legitimate business purposes, they must be approved by the IT Manager and digitally signed.

6.4 User Application Hardening

Web browsers and email clients are configured to block advertisements, malicious scripts, and web-based code execution. Flash Player is disabled. Java is disabled in web browsers where not required. These settings are managed centrally by IT.

6.5 Restrict Administrative Privileges

Administrator accounts are only issued where there is a clear business need. Standard staff use non-administrator accounts for day-to-day work. Administrator accounts are not to be used for email or general internet browsing.

6.6 Patch Operating Systems

Operating systems on all AAPoly-managed devices must be kept up to date. Critical OS patches are applied within 48 hours. Unsupported operating systems (e.g. Windows 7) are not permitted on any AAPoly network. IT is responsible for automated patch management.

6.7 Multi-Factor Authentication (MFA)

Multi-factor authentication adds a second layer of security beyond a password. Staff will be prompted to verify their identity using a second factor, typically the Google Authenticator app, after entering their password. IT will assist any staff member in setting up MFA.

MFA is required for all staff and administrator accounts, including access to:

- Staff email accounts (Google Mail - Gmail).
- Student Management System (Paradigm).
- Learning Management System (LMS).
- Remote access.
- Cloud storage and file sharing platforms.
- Administrator accounts without exception.

MFA requirements for specific servers, financial systems (e.g. MYOB), and other systems are to be confirmed by IT and documented in the IT Risk Register. IT will assist any staff member in setting up MFA. Staff who travel internationally should notify IT in advance to avoid account lockouts.

6.8 Regular Backups

All critical data, including student records, financial data, LMS content, and operational systems, is backed up daily. Backups are:

- Stored in a separate, secure, and geographically distinct location (cloud-based backup). Current backup arrangements are to be confirmed by IT and documented in the IT Risk Register.
- Encrypted both in transit and at rest.
- Tested quarterly to confirm they can be successfully restored.
- Retained for a minimum of 90 days.

Coverage for backups includes student records, research data, LMS content, cloud services, and data held by third-party systems.

7. ACCESS CONTROLS AND ROLE-BASED PERMISSIONS

Access to AAPoly systems and data is granted on the principle of least privilege: staff are only given access to what they need to perform their job.

7.1 How Staff Access is Managed

- System access is requested through the IT team using a formal access request process.
- Access is approved by the relevant manager and the IT Manager.
- Accounts are created with the minimum permissions required (role-based access control).
- Access requests and approvals are logged.

7.2 Student Access

Students are provided access to the LMS and relevant student-facing platforms only. Student accounts are automatically disabled at the end of their course. Students do not have access to staff or administrative systems.

7.3 Third-Party and Vendor Access

Any third-party requiring access to AAPoly systems must comply with this policy. Vendor access is time-limited and revoked immediately upon completion of the relevant engagement. Where the Student Management System or LMS is operated by a third-party provider, the vendor's data handling obligations must be documented in a data processing agreement and reviewed annually.

8. INCIDENT RESPONSE PLAN

AAPoly has a clear process for detecting, responding to, and recovering from cyber security incidents. An incident is any event that threatens the confidentiality, integrity, or availability of AAPoly information or systems. The Manager, Cyber Security leads incident response and is the primary point of escalation.

8.1 Examples of Incidents

- Phishing email that results in a staff member entering their credentials.
- Ransomware or malware detected on a device.
- Unauthorised access to student or staff records.
- Data breach or suspected data leak.

- System unavailability caused by a cyber-attack.
- Suspected foreign interference or espionage attempt.
- Compromise of an LMS or Student Management System.

8.2 Response Steps

Step	Phase	Actions
1	Identify	Any staff member who suspects an incident reports it immediately to the IT Help Desk. Do not attempt to fix it yourself.
2	Contain	IT isolates affected systems to prevent further spread. Disconnect affected devices from the network if safe to do so.
3	Assess	Manager, Cyber Security, IT Manager, AAPoly CEO and Deputy Group Managing Director are notified. Severity is assessed: Low, Medium, High, or Critical. High/Critical incidents are escalated immediately. Suspected or potential High/Critical incidents and near-misses are also notified.
4	Notify	If personal data is involved, the CEO and Deputy Group Managing Director assess whether notification to OAIC is required within 72 hours. ACSC is notified of significant incidents. TEQSA is notified where the incident materially affects HE registration obligations or student welfare. Refer to Appendix A for full notification obligations.
5	Eradicate	IT removes the threat, patches vulnerabilities, and resets compromised credentials. Student Management System and LMS breach procedures are activated if those systems are affected.
6	Recover	Systems are restored from verified clean backups. Staff and students are notified when systems are safe to use.
7	Review	A post-incident review is led by the Manager, Cyber Security within 5 business days. Findings and lessons learned are documented and presented to the AAPoly CEO and Board of Directors as required.

8.3 Reporting Contacts

Body	Contact / Purpose
AAPoly IT Help Desk	First point of contact for all suspected incidents
Australian Cyber Security Centre (ACSC)	report.cyber.gov.au — for significant cyber incidents
Office of the Australian Information Commissioner (OAIC)	oaic.gov.au — for notifiable data breaches under the Privacy Act 1988
TEQSA	teqsa.gov.au — where incidents affect Higher Education registration obligations or student welfare
ASQA	asqa.gov.au — where incidents affect RTO registration or student data obligations
Department of Home Affairs (DHA)	homeaffairs.gov.au — where incidents affect CRICOS-registered providers or international student data
Department of Education	education.gov.au — for suspected foreign interference incidents

9. CYBER RISK INSURANCE

AAPoly holds cyber risk insurance as part of its broader Academies Australasia Group risk management strategy. Coverage includes response costs following a data breach or cyber incident (including forensic investigation, legal advice, and communications), business interruption losses, third-party liability where a breach affects students, staff, or partners, ransomware and cyber extortion events, and incidents affecting student records, research data, LMS, cloud services, and third-party systems. The Finance Manager is responsible for reviewing the cyber insurance policy annually to ensure coverage remains adequate as AAPoly's digital footprint evolves. All staff must immediately notify the CEO if they become aware of any incident likely to trigger an insurance claim.

10. BOARD OVERSIGHT AND GOVERNANCE

The Board of Directors of Academies Australasia Polytechnic holds ultimate responsibility for cyber security governance across AAPoly. The Board ensures that cyber risk is managed as a strategic organisational risk and that the cyber posture is appropriate for its size, operating environment, and multi-sector regulatory obligations. This is consistent with the expectations of TEQSA and ASQA for governing bodies to exercise due diligence to identify, prevent, and manage risks within the provider's remit of operations.

This policy is approved by the Board of Directors and must be reviewed and re-approved whenever material changes are made.

10.1 Incident Reporting Protocol

The Board is to be notified promptly of any High or Critical cyber security incident. The AAPoly CEO is responsible for ensuring the Board is briefed within 24 hours of a Critical incident being declared. The Board is also to be notified of any incident that is reasonably likely to escalate to High or Critical, and near-misses are to be included in Board reporting.

For lower-severity incidents, a summary is included in the next Board report. Incident reports to the Board will include:

- Nature and scope of the incident.
- Immediate response actions taken.
- Impact on students, staff, or operations.
- Regulatory notification obligations (OAIC, ACSC, TEQSA, ASQA, DHA, Department of Education as applicable).
- Lessons learned and remediation steps.

10.2 IT Risk Register Review

The IT Risk Register includes cyber and technology risks and their likelihood, potential impact, current maturity level per control (with assessment date), and current mitigation status. The Manager, Cyber Security maintains the register and provides it to the CEO on request. The Board reviews the IT Risk Register at least once per year.

The IT Risk Register includes as a minimum:

- Risks to personal information, student records, staff records, research data, and intellectual property.
- Risks relating to foreign interference and data sovereignty.
- Risks associated with third-party and cloud service providers, including the Student Management System (Paradigm) and the LMS. Where the SMS or LMS is subject to a cyber-attack, the Incident Response Plan (Section 8) applies; vendor incident response obligations are documented in the relevant data processing agreement.
- Risks from legacy systems or unpatched infrastructure.

- Risks associated with AI and emerging technology use across AAPoly operations.
- Current ASD Essential Eight maturity level per control and assessment date.

10.3 Governance Roles and Responsibilities

Role	Responsibilities
Board of Directors	Ultimate governance oversight of cyber security as a strategic organisational risk; approve this policy; review IT Risk Register; receive incident reports for High and Critical incidents; receive reports on suspected or potential High/Critical incidents and near-misses; approve significant changes to AAPoly's cyber security posture.
CEO	Accountable for policy implementation within AAPoly; escalate Critical incidents to the Board within 24 hours; approve incident response actions; notify IT when staff depart; ensure Board is briefed on all High/Critical incidents and near-misses.
Manager, Cyber Security (Group)	Maintain this policy, lead implementation and maintenance of all cyber security controls; maintain the IT Risk Register (current maturity level recorded per control with assessment date); lead incident response; report maturity progress to the Board; coordinate campus IT on cyber matters.
IT Manager (AAPoly)	Day-to-day implementation of technical controls at campus level; report to Manager, Cyber Security on all cyber security matters; escalate incidents immediately; implement and monitor patch management, MFA, backups, and access controls.
All Staff (including sessional, casual, and contractors)	Complete mandatory annual cyber security awareness training; complete induction briefing before accessing systems; report suspected incidents immediately; comply with this policy and all related procedures; meet the same cyber security obligations relevant to their role and system access.
Students	Use AAPoly-provided systems and accounts in accordance with this policy and the Acceptable Use of IT Resources Policy.

11. PASSWORD AND CREDENTIAL MANAGEMENT

- All passwords must include a mix of letters, numbers, and symbols.
- Passwords must not be shared, written down, or sent by email.
- Staff are encouraged to use a password manager (e.g. Microsoft Authenticator).
- Default passwords on new devices and systems must be changed immediately upon commissioning.
- Passwords for privileged accounts must be changed every 90 days.
- Compromised credentials must be reported to IT immediately and changed at once.

12. ACCEPTABLE USE OF AAPOLY SYSTEMS

- AAPoly systems, including email, internet access, cloud storage, LMS, student portals, and devices, are provided for legitimate business and educational use. Staff must not:
- Use AAPoly systems to access, download, or distribute illegal or inappropriate content.
- Install unapproved software on AAPoly devices.
- Connect personal devices to the AAPoly corporate network without IT approval.
- Use personal email accounts to conduct AAPoly business.
- Share login credentials with anyone, including colleagues.
- Misuse or compromise LMS, student portals, or other AAPoly digital systems.

Reasonable personal use of work internet is permitted. AAPoly monitors network activity and system use logs for security purposes.

13. LEGISLATION AND REGULATORY COMPLIANCE

This policy supports AAPoly's compliance with the following legislation, standards, and frameworks:

Legislation / Framework	Relevance to AAPoly
Privacy Act 1988 (Cth)	Governs the handling of personal information of students and staff across all sectors. Requires incident response, containment, and preventative controls consistent with TEQSA cyber security governance expectations.
Notifiable Data Breaches Scheme	Requires notification of eligible data breaches to OAIC and affected individuals within 72 hours of assessment that a breach is notifiable.
TEQSA Higher Education Standards Framework (HESF 2021)	Cyber security and foreign interference are identified sector risks under Standards 2.3.4, 2.3.5, 5.2.2, 6, and 7.3.3(b). Standard 2.3.4 directly requires providers to manage risks to academic integrity and information security.
ASQA Standards for Registered Training Organisations (NVETR Instrument 2025)	RTO risk management, data protection, and governance obligations; cyber security must be embedded in the RTO risk management system.
ESOS Act 2000 and National Code of Practice for Providers of Education and Training to Overseas Students	Obligations for international student records, welfare, and delivery. Requires secure handling of international student data and compliance with CRICOS registration requirements.
ASD Essential Eight Maturity Model	AAPoly's technical controls framework. The ASD Essential Eight provides a practical, best-practice framework for protecting internet-connected networks and systems. Aligned with both TEQSA and ASQA expectations for education provider cyber governance.
ASD Information Security Manual (ISM)	Supplementary best-practice guidance for information security governance in higher education and VET contexts.
CRICOS Registration Requirements	Obligations for providers enrolling international students, including data protection and Department of Home Affairs reporting requirements. PRISMS records and student visa data must be protected.
Foreign Influence Transparency Scheme (FITS)	Transparency obligations for foreign-linked activities affecting AAPoly operations, research, and partnerships.
Security of Critical Infrastructure Act 2018	May apply as higher education sector obligations evolve under the Act.
Privacy Act 1988 – AI-related amendments and guidance	Emerging obligations around transparency, accountability, and governance of AI use, including restrictions on sharing sensitive data with third-party AI platforms. Cross-reference: AAPoly Acceptable Use of AI Policy.

Appendix A: Breach Notification Obligations

This appendix may be used as a standalone internal quick-reference document. It should be reviewed annually and updated whenever relevant legislation or regulatory guidance changes. Last reviewed: June 2026.

In the event of a cyber security incident or data breach, AAPoly's notification obligations vary by sector and the type of data affected. The table below summarises the key reporting bodies, channels, and timelines. This appendix supplements Section 8 (Incident Response Plan).

Regulatory Context	Reporting Body / Channel	Timeline	Notes
All sectors; Personal data breach	Office of the Australian Information Commissioner (OAIC); oaic.gov.au	72 hours from assessment that breach is notifiable	Notifiable Data Breaches Scheme. Notify affected individuals as soon as practicable.
All sectors; Significant cyber incident	Australian Cyber Security Centre (ACSC); report.cyber.gov.au	As soon as practicable	Voluntary for most; mandatory for critical infrastructure entities.
Higher Education (TEQSA)	TEQSA; teqsa.gov.au | Provider's designated contact	Notify TEQSA where incident materially affects HE registration obligations or student welfare	Consider obligations under HESF Standards 2.3.5, 6, and 7.3.3(b).
VET / RTO (ASQA)	ASQA; asqa.gov.au	Notify ASQA where incident affects RTO registration obligations or student records	ASQA may require evidence of breach response and remediation for compliance audit purposes.
CRICOS / International students	Department of Home Affairs; homeaffairs.gov.au	As soon as practicable where international student visa or enrolment data is compromised	PRISMS records may be affected. Notify DHA and consider ESOS Act obligations.

Key contacts for breach notification:

- OAIC Notifiable Data Breaches: oaic.gov.au/privacy/notifiable-data-breaches
- ACSC Report Cyber: report.cyber.gov.au
- TEQSA: teqsa.gov.au
- ASQA: asqa.gov.au
- Department of Home Affairs: homeaffairs.gov.au
- Department of Education: education.gov.au/countering-foreign-interference-australian-university-sector

Appendix B: ASD Essential Eight Definitions

The following definitions apply to the eight controls referenced in Section 5 of this policy:

Control	Definition
Application Control	Preventing unapproved or malicious programs from running on systems.
Patch Applications	Applying security patches and updates to applications within defined timeframes.
Configure Microsoft Office Macro Settings	Restricting macro execution to approved, digitally signed macros only.
User Application Hardening	Configuring browsers and email clients to block malicious content.
Restrict Administrative Privileges	Limiting admin access to those who require it, with separate accounts for daily use.
Patch Operating Systems	Keeping OS software up to date with security patches applied promptly.
Multi-Factor Authentication (MFA)	Requiring a second form of verification beyond a password for access to systems.
Regular Backups	Maintaining daily encrypted backups stored separately and tested regularly.

Appendix C: References

The following references inform this policy:

- Australian Federal Police. (2026, February 10). Espionage and foreign interference. https://www.afp.gov.au/crimes/espionage-and-foreign-interference
- Australian Government Attorney-General's Department. (2025, March 6). The Foreign Influence Transparency Scheme: Information for community organisations. https://www.ag.gov.au/integrity/publications/foreign-influence-transparency-scheme-information-community-organisations
- Australian Government Department of Home Affairs. (2026, May 24). Defining foreign interference. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/defining-foreign-interference
- Australian Signals Directorate. (2024). Essential Eight Maturity Model. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight
- Australian Signals Directorate. (2024). Information Security Manual (ISM). https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism
- Department of Education. (2024). Countering foreign interference in the Australian university sector. https://www.education.gov.au/countering-foreign-interference-australian-university-sector
- Office of the Australian Information Commissioner. (2024). Notifiable Data Breaches Scheme. https://www.oaic.gov.au/privacy/notifiable-data-breaches
- TEQSA. (2021). Higher Education Standards Framework (Threshold Standards) 2021. https://www.teqsa.gov.au/hesf
- ASQA. (2025). Standards for Registered Training Organisations (NVETR Instrument 2025). https://www.asqa.gov.au/standards