Australian Association
for Research in Education

CYBER SECURITY POLICY & PROCEDURES

Policy number	6.0	Version	1.0
Drafted by	AARE Executive Office Manager	Date approved	June 2023
Responsible person	Treasurer	Review date	June 2024

1. Introduction

The Australian Association for Research in Education (AARE) wishes to foster a culture of openness, trust, and integrity however this can only be achieved if external threats to the integrity of the organisation's systems are controlled and the Association is protected against damaging actions.

2. Purpose

This policy sets out guidelines for generating, implementing and maintaining practices that protect the Association's cyber media – its computer equipment, software, operating systems, storage media, electronic data, and network accounts – from exploitation or misuse.

This policy applies to all system users and equipment as follows:

Employees	**Service Provider & other Contractors** (including all employees of or personnel affiliated with third parties)	**AARE Executive Office Bearers and Members engaged in Association Work**	**Members**	**All equipment owned or leased by AARE, and/or authorised by AARE for the conduct of the Association's business**
✓	✓	✓	✓	✓

AARE Members are reminded that their conduct will also be subject to the policies and procedures of their employing institution.

3. Policy

While AARE wishes to provide a reasonable level of personal privacy, users should be aware that the data they create on the organisation's systems remains the property of AARE. All system users (as identified at Policy item 2) will take all necessary measures to maintain the necessary cyber security procedures, including protecting passwords, securing access to computers, and maintaining protective software.

Information in the possession of the organisation shall be classified into different grades depending on its degree of confidentiality with particularly sensitive information receiving special protection (refer ***Appendix 1***).

Because of the need to protect AARE 's network, the confidentiality of information stored on any network device belonging to AARE cannot be guaranteed, and AARE reserves the right to audit networks and systems periodically to ensure compliance with this policy.

4. Roles & Responsibilities

4.1 It is the responsibility of the Executive Management Team to ensure that:

- All system users (as identified at Policy item 2) are aware of this policy and procedures via;
  - Policy and procedures published at the AARE website
  - Communication to members annually including recent past members
  - Induction and handbooks for Executive Office Bearers and Members engaged in Association Work
  - Sign off on policy by third party service providers
- any breaches of this policy coming to the attention of management are dealt with appropriately;
- a Cyber Security Officer is appointed.
  - Unless otherwise indicated this will be the Association Manager.
  - Where the Association Manager is a contracted third-party service provider, the service provider will have their own Cyber Security Policy and will provide a copy to AARE.

4.2 It is the responsibility of the Cyber Security Officer to ensure that:

- the Executive Management Team is kept aware of any changes to the Association's cyber security requirements;
- a report on the organisation's cyber security is submitted annually to the Executive Committee and included in the Association's annual report.

4.3 It is the responsibility of all system users (as identified at Policy item 2) to ensure that:

- they familiarise themselves with cyber security policy and procedures;
- their usage of cyber media conforms to this policy.

4.4 In the event of any uncertainty or ambiguity as to the requirements of the cyber security policies or procedures, system users (as identified at Policy item 2) should consult the Executive Management Team.

4.5 The AARE Executive Committee may nominate a risk sub-committee which would include oversight of cyber security risk.

5. Breaches

Breach of this policy may result in disciplinary action, (e.g. rescindment of User access, requirement to step down from their appointment, revocation of membership, termination of contract) as determined by the AARE Complaints Policy and Procedure and/or contractual terms.

6. Related Documents

- AARE Code of Conduct
- AARE Privacy Policy
- AARE Terms & Conditions

CYBER SECURITY PROCEDURES

---

1. Cyber Risk Assessment

1.1 A cyber risk assessment is to be conducted annually by the Cyber Security Officer using the ACSC Cyber Security Assessment Tool. The assessment should seek to identify:

- Whether AARE is complying with Australian cyber security principles
- Any new cyber risks that have been identified
- Changes to any existing cyber risks
- Whether existing controls need to be changed or new ones implemented

Results from the assessment will be reported to the Executive Committee, within the Association Risk Register as part of the Treasurer's Report.

1.2 The Cyber Security Officer will subscribe to ACSC alerts to stay across emerging cyber threats.

2 Confidentiality

2.1 The Executive Management Team authorises the Cyber Security Officer and other third parties as required, (including web development service providers) to monitor the organisation's equipment, systems and network traffic for security and network maintenance purposes.

2.2 Other than a representative of the Association Management service provider, where a third party is authorised to monitor the organisation's equipment, systems and network traffic for security and network maintenance purposes, the party will be required to sign a declaration of confidentiality prior to being provided with system access.

2.3 In consultation with the Cyber Security Officer, the Executive Management Team shall issue cyber security procedures appropriate to different levels of confidentiality.

2.4 The organisation shall classify the information it controls in the organisation's computer systems, files and databases as either non-confidential (open to public access) or confidential (in one or many categories). Refer to ***Appendix A & Appendix B***.

2.5 The Cyber Security Officer shall review and approve the classification of the information and provide advice to the Executive Management Team to determine the appropriate level of security and controls that will best protect it.

3 Monitoring

3.1 The Cyber Security Officer shall undertake an annual audit of the organisation's computer systems, files, databases, security classification (Appendix A).

3.2 The Cyber Security Officer shall undertake an annual audit of the organisation's cyber security risk management controls methods for cyber risk monitoring (Appendix B).

4 Access control

4.1 Individuals shall be assigned clearance to particular levels of access to the organisation's information resources and shall access only those resources that they have clearance for. Access control shall be exercised through username and password controls, with multi-factor authentication wherever possible.

4.2 AARE Office staff will be the only users authorised as system administrators. Other users who need this level of access to production systems must request a special access account.

4.3 Special access accounts may be provided to individuals requiring temporary system administrator privileges in order to perform a job or volunteer role. These accounts will require the permission of the Executive Management Team.

4.4 Administrator and special accounts will be deactivated by the AARE Office as soon as possible after a contract, job or role has been completed.

4.5 Monitoring of special access accounts shall be undertaken via the AARE Office annually and more frequently as required, generating reports to the Cyber Security Officer showing who currently has a special access account, for what reason, and when it will expire.

5 Computer and system security

5.1 PCs, laptops and workstations should not be left unattended, or should be secured by a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off when unattended.

5.2 Databases and Cloud systems should be configured to maximise security and data back-ups, in line with recognised best practice principles.

6 Password management

6.1 System and user passwords will be managed centrally by the AARE Office using a secure password manager and will be audited and reset every six months, with inactive accounts suspended.

6.2 System users must keep passwords secure. Accounts must not be shared unless authorised. Passwords should not be readily accessible in the area of PCs, laptops or workstations. Authorised users are responsible for the security of their passwords and accounts.

6.3 Copying, reading, deleting or modifying a password file on any computer system is prohibited.

6.4 Wherever possible multi-factor authentication should be applied to all passwords and should not be recorded in any form not also protected by password and multi-factor authentication (e.g. handwritten or password file accessible to others).

6.5 System and user passwords should meet Australian best practice for password security. If not generated by a password manager, the strongest type of password is a passphrase which is easy to remember and hard for machines to crack. Passphrases are a combination of unpredictable words (a random mix of four or more), ideally at least 14 characters long, do not use popular or known phrases/words (e.g. names, song lyrics or quotes) and are not re-used across multiple accounts. Strong passwords also contain capital and lower-case letters, numbers and symbols).

6.6 Users who forget their password must contact the AARE Office (aare@aare.edu.au) to have a new password assigned to their account. The user must identify themselves by full name and Executive Portfolio role/title to the AARE Office.

6.7 User log-on IDs and passwords will be deactivated as soon as possible if an employee, sub-contractor or volunteer is terminated, fired, suspended, placed on leave, or otherwise leaves the organisation. Supervisors/managers shall immediately and directly contact the AARE Office to report change in status that require terminating or modifying log-on access privileges.

6.8 Users should change all account passwords immediately if a device is stolen.

7 System updates

7.1 Security updates of browsers and systems should be enabled automatically where possible or installed as soon as updates are available.

7.2 System updates will be audited annually.

8 Virus protection

8.1 All computers and devices should have virus-scanning software installed, operating with settings to maximise security and kept updated.

8.2 Virus-scanning should include all email attachments and all documents imported into the computer system.

9 Downloads, attachments, websites and external devices

9.1 Users should refrain from downloading suspicious, illegal or unauthorised software from the internet onto their PCs or workstations.

9.2 Users should use extreme caution when using messaging systems and opening email attachments or clicking on links embedded within emails, messaging systems or social media, especially those received from unknown senders; these may contain viruses, malware or Trojan horse code.

9.3 Users should avoid accessing suspicious websites.

9.4 Users should use extreme caution if using external USBs or hard drives; these may contain viruses, malware or Trojan horse code.

10 Data hygiene and transfer

10.1 Association Management service provider, with support from the Executive Secretary and/or Communications Coordinator, will undertake regular data cleaning/hygiene practices including removing inactive, bounced, and other unengaged email addresses from the Association member database.

10.2 Users must not transfer sensitive data (e.g. customer information, organisational financial data) to other devices, accounts or users unless absolutely necessary and only after receiving consent from the Executive Management Team.

10.3 Users must ensure that the recipients of data being transferred are properly authorised people or organisations and have adequate security policies.

10.4 Users must report scams, privacy breaches and hacking attempts resulting from data transfer to the Cyber Security Officer and Executive Management Team immediately.

11 Incident management

11.1 The Executive Management Team to ensure that a Cyber Incident Response Plan is developed and kept up to date.

11.2 Users must report perceived attacks, suspicious emails, phishing attempts or improper access or use of PC to the Cyber Security Officer and Executive Management Team as soon as possible for prompt investigation and resolution.

11.3 Users must not themselves breach security. Security breaches include accessing data of which the user is not an intended recipient or logging into a system account that the user is not expressly authorised to access, unless these duties are within the scope of regular duties. "Disruption" includes network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

12 Training

12.1 Association Management service provider will undertake regular cyber security training from reputable Australian sources and report participation to the Executive Management Team.

12.2 Service providers and contractors will commit to up-to-date cyber security training.

AUTHORISATION

Date Policy authorised by AARE Executive Committee 16 June 2023
Professor Michele Simons, Treasurer
Australian Association for Research in Education

APPENDIX A: SYSTEM & DATA CLASSIFICATION

System taxonomy

Security level	Description	Example	AARE systems	
Red	System contains confidential information – information that cannot be revealed to personnel outside the company. Even within the company, access to this information is provided on a "need to know" basis. The system provides mission-critical services vital to the operation of the business. Failure of this system may have life-threatening consequences and/or an adverse financial impact on the business of the company.	Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information	1. AARE Silverstripe Membership Administration Portal	Confidential Customer and financial information
			2. AARE Office365 SharePoint	Confidential customer information and organisational financial and strategic information/data
			3. XERO Financial System	Confidential organisational and customer financial data
			4. EWAY Payment Gateway	Confidential organisational and customer financial data
			5. CBA Banking portal	Confidential Customer and financial information
			6. EventsAir	Confidential Customer and financial information
			7. Survey Monkey	Confidential customer and organisational financial and strategic information/data
			8. SA Government OCBA Portal	Confidential organisational financial data
			9. Copyright Agency	Confidential organisational financial data
			10. IP Australia	Confidential organisational strategic information/data
Green	This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network.	User department PCs used to access server and application(s). Management workstations used by systems and network administrators.	1. Association Management Service Provider Sub Contractor PCs	Access to all RED systems
			2. Last Pass password manager	Access to all RED systems
			3. Domain management Service provider Administration Portals (Digital Pacific, Vodien, Domainname.edu.au)	Access to RED system 1
			4. Telstra Marketplace (O365 Set up)	Access to RED system 2
			5. Web Central Email Console	Access to all email accounts, and password reset for RED systems 1, 2, 4 & 5

White	This system is not externally accessible. It is unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services.	A test system used by system designers and programmers to develop new computer systems.	1. MailChimp	Customer email addresses
			2. AARE Silverstripe Conference Website Administration Portal	Customer email addresses
			3. AARE Blog Website Administration Portal	Subscriber email addresses
			4. eOrganiser Abstract Submission Portal	Customer email addresses; 2021 conference abstracts
			5. Loomly Social Media Manager	AARE & SIG Social Media Account administrator access
			6. Zoom	Some customer names; meeting attendance
			7. Google Account	Gmail, Google Files, Google Analytics
			8. DropBox	Capacity for shared files; inactive
Black	This system is externally accessible. It is isolated from RED and GREEN systems. While it performs important services, it does not contain confidential information.	A public web server with non-sensitive information.	**1. AARE website**	Externally accessible, non-sensitive information
			2. AARE conference website	
			3. AARE Blog website	
			4. AARE & SIG Social Media Accounts	
			5. AARE YouTube Channel	

Data taxonomy

Security level	Description	Example	
Red	Client or Organisation data allowing banking or financial exploitation or identity theft.	Client credit card and banking data Organisational credit card and banking data Client details that would facilitate phishing	Customer credit card and banking data Organisational credit card and banking data Customer email, address, mobile number, date of birth, professional details
Green	Client data allowing address or email exploitation. Organisational intellectual property that has financial or reputational consequences.	Addresses that would facilitate spamming Information that the organisation sells Internal emails	Customer email, address, mobile number, date of birth, professional details Organisation email addresses and email inboxes Organisational financial and strategic information/data/reports
Black	Publicly accessible data	Non-sensitive information	**Externally accessible, non-sensitive information**

APPENDIX B: CYBER SECURITY RISK MANAGEMENT & MONITORING

System	Data type	Method of risk management controls
All systems	All data types	• Limited administrator user access • Unique user log ins • Multi-factor log in authentication • Secure Password manager and best practice passwords • AARE office to conduct annual audit of user access profiles, data storage/hygiene and data classification; January • Regular system updates/maintenance/security testing; performed by Web Developer/IT service providers • PCI compliant eCommerce and financial systems • Up to date Cyber Security & Privacy Policies • System user compliance with Cyber Security & Privacy Policies and Procedures • Cyber Security and Privacy Training

AARE Silverstripe Membership Administration Portal	Confidential Customer and financial information	• Limited administrator user access:
		  ○ Association Management service providers
		  ○ Web Development service providers
		• No shared log ins
		• MFA for all administrators
		• Annual Web Developer system tests and maintenance
		• eCommerce functionality sits outside of website/database (diverts to eWAY); credit card details not stored in website/database
		• Consent to collection of data in membership and other eCommerce forms

AARE Office365 SharePoint	Confidential customer information and organisational financial and strategic information/data	• Limited administrator user access: Association Management service providers only • MFA for all administrators • FineHaus IT support to ensure secure configurations • Limited file access for Executive Committee (need to know); annual audit • Password protection on sensitive files shared externally; annual audit

XERO Financial System	Confidential organisational and customer financial data	• Limited administrator user access:
		  ○ Association Management service providers
		  ○ Financial Auditor; time limited
		• No shared log ins
		• MFA for all administrators
		• Robust Security via system functionality
		  ○ Data encryption
		  ○ System notifications about phishing/scams and security recommendations
		  ○ Access to independent security assurance audit reports
		  ○ Certified compliance with ISO/IEC 27001:2013, the premier global information security management system (ISMS) standard
		  ○ PCI DSS v3.2, SAQ A compliance
		  ○ Network and data centre security features (firewalls, intrusion protection systems, network segregation, hardware redundancy technologies, networks and infrastructure)

EWAY Payment Gateway	Confidential organisational and customer financial data	• Limited administrator user access: Association Management service providers only
		• MFA for all administrators
		• System Security Features
		  ○ Bank-level Protection - customer and business information secured with the same levels of data security of the biggest banks in the world
		  ○ Certified with level 1 PCI DSS compliance - the highest level of encryption available.
		  ○ Eway partnership with Akami – the global leader in DNS assurance – guarantees that traffic passing through the Eway gateway is routed to the correct location
		  ○ Clustered web architecture supported by multiple backups and duplicates of every device, Eway data centre can instantly divert traffic if any system should fail, customer information is never lost
		  ○ Merchant Trust Initiative (MTI) program - suite of learning material, tools, and one-on-one support to become PCI DSS compliant; SecureTrust PCI Manager tool

CBA Banking portal	Confidential organisational and customer financial data	• Limited administrator user access:
		  ○ Association Management service providers
		  ○ 2 Authorised Executive members: Treasurer, Secretary
		• No shared log ins
		• MFA for all administrators; netlock device
		• Bank-level Protection

EventsAir	Confidential Customer and financial information	• Limited administrator user access:
		  ○ Association Management service providers
		  ○ Conference Managers; time limited
		• No shared log ins
		• Confirm scope of data collected in system
		• System Privacy Policy
		  ○ Confirm system security features
		  ○ Use of reCaptcha screen in all registration forms that include a payment gateway to block any automated tools attempting to access event registration pages
		• Consent to collection of data in registration forms

Survey Monkey	Confidential customer and organisational financial and strategic information/data	• Limited administrator user access: Association Management service providers only
		• Shared log in; only two devices authorised at a time (2 AARE office contractors)
		• OTP via one administrator only
		• Data to be logged and deleted quarterly
		• System Security Features
		  ○ SOC 2 accredited data centres
		  ○ Collected data transmitted over a secure HTTPS connection
		  ○ User logins protected via TLS
		  ○ Encryption of data at rest and in motion; industry standard algorithms and strength
		  ○ Vulnerability and penetration testing
		  ○ Breach notification
		  ○ ISO 27001 International Organization for Standardization
		  ○ GDPR compliance
		  ○ PCI DSS 3.2 Payment Card Industry Data Security Standards

Association Management Service Provider Sub Contractor PCs	Access to all RED systems	• User PC virus protection • Compliance with Cyber Security and Privacy Policies & Procedures • Cyber Security and Privacy Training

Last Pass password manager	Access to all RED systems	• Limited administrator user access: Association Management service providers only
		• No shared log ins
		• MFA for all administrators
		• System Security features
		  ○ LastPass operates on a zero-knowledge security model; i.e. no one has access to the decrypted Master Password, vault or vault data except authorised administrator/s.
		  ○ Certified compliance: SOC 2 Type II, SOC3, BSI C5, APEC CBPR and PRP Privacy Certification, TRUSTe Enterprise Privacy Certification, GDPR, AES-256 encryption, PBKDF2 hashing plus salting, and ISO/IEC 27001:2013.
		  ○ Audits and Penetration Tests
		  ○ Protection of infrastructure through regular upgrading of systems and redundant data centres across the globe to reduce the risk of downtime or a single point of failure.
		  ○ Breach notification
		• Bi-annual password change for all systems; January/July

Domain management Service provider Administration Portals (Digital Pacific, Vodien, Domainname.edu.au)	Access to RED system 1	• Limited administrator user access:
		  ○ Association Management service providers
		  ○ Restricted access by Web Development service providers (cPanel only)
		• Shared administrator log in
		• cPanel log in controlled by administrators
		• Confirm System Security features

Web Central Email Console	Access to all email accounts, and password reset for RED systems 1, 2, 4 & 5	• Limited administrator user access: Association Management service providers only • MFA for all administrators • Confirm System Security features Limited email account diversion for Executive Committee (based on role; need to know); annual audit • Password protection on email accounts managed by AARE Office; annual audit
MailChimp	Customer email addresses	• Limited administrator user access: Association Management service providers only • OTP via one administrator only • Confirm System Security features

AARE Silverstripe Conference Website Administration Portal	Customer email addresses	• Limited administrator user access:
		  ○ Association Management service providers
		  ○ Web Development service providers
		  ○ External Conference Managers; time limited
		• No shared log ins
		• Enable MFA
		• Annual Web Developer system tests and maintenance
		• eCommerce functionality sits outside of website/database (diverts to PCO payment gateway); credit card details not stored in website/database

AARE Blog Website Administration Portal	Subscriber email addresses	• Limited administrator user access:
		  ○ Association Management service providers
		  ○ Web Development service providers
		  ○ Blog Editor
		• No shared log ins
		• Enable MFA
		• Annual Web Developer system tests and maintenance
		• No eCommerce functionality
		• Privacy Policy; Consent to collection of data
		• Process for managing subscriber data

Loomly Social Media Manager	AARE & SIG Social Media Account administrator access	• Limited administrator user access:
		  ○ Association Management service providers
		  ○ Log in shared with Executive Communications Coordinator
		• MFA enabled; verification to aare@aare.edu.au
		• Confirm System Security features

Zoom	Customer email addresses	• Limited administrator user access: Association Management service providers only
		• Shared log in
		• OTP via one administrator only
		• System Security features
		  ○ End to end encryption of meetings and data
		  ○ Meeting privacy/security configurations
		  ○ Password protection and authentication
		  ○ Compliance certifications

AARE website	Externally accessible, non-sensitive information	Administrator controls as above
AARE conference website		
AARE Blog website		
AARE & SIG Social Media Accounts		

AUDIT STATUS

Date of last Audit: 18/07/2023
Amanda Mehegan, Association Manager
Australian Association for Research in Education