Privacy Policy

1. Applicability

The Australian Information Security Association (**AISA**) is a public company limited by guarantee and registered as a charity and not-for-profit. The charitable purpose relied upon is set out in section 12 of the Charities Act 2013 as "*the purpose of advancing education"* and "*advancing the security or safety of Australia or the Australian public*".

To achieve its purpose AISA is governed by a Constitution, under the direction of an operational Board, with representation across Australia in all major centres, comprising Branch Committees, headed by Branch Chairs. These management structures provide for a direct relationship with AISA Members.

AISA (We, Our, Us) are not obliged by law to comply with the *Australian Privacy Act 1988*. We have however elected to adopt the Australian Privacy Principles and to adopt privacy law and risk management best practice because we know the importance of privacy (personal information) and its relationship to security. As a security association, we believe that privacy is about trust and that trust is core to the AISA purpose.

Our Privacy Policy (Policy) is published on Our website for the benefit of anyone interested. Please see also Our Email Legal Notice and Website Terms of Use which are related notices.

Information for Individuals Located in the European Union.

If You are an individual protected under European Union privacy law, We will make special arrangements to accommodate you in the exercise of Your rights. In all respects, this policy is intended to accord you privacy protection equivalent to European Union privacy law. Contact details are provided in section 11 below.

2. Personal Information, Privacy and Employee Records

Our Privacy Policy concerns information or an opinion about an identified individual or an individual that is reasonably identifiable. We make no distinction between employee records and other sources of personal information. Neither do we discriminate between different forms of personal information (electronic records, paper records, voice files etc.), nor between whether the information or opinions are true or not.

All personal information that We collect, hold (where We have possession or control of a record), use and disclose (where the information is outside of Our possession or control) is treated with the same respect.

For the purpose of this Policy 'privacy' and 'personal information' have the same meaning.

3. Scope and Purpose of Collection

The scope of this Policy extends to all personal information that We collect, hold, use and disclose in the course of fulfilling AISA's purpose and in complying with law and managing risk.

In fulfilling AISA's purpose Our activities include our Member relationships, internal operations (management, employees, temporary staff, contractors) and external operations (third parties such as business partners and service providers).

The scope of this Policy extends to our external client-facing activities such as Our online presence at www.aisa.org.au and to the personal information that is collected through Our

Social Media, Website and through the use of email for general communications, marketing and Member purposes. It also extends to conferences and public events that We arrange and host across Australia.

This Policy does not extend to third party websites or to social media accessed via links on Our Website or email communications. Use of third party links and social media will be governed by the privacy policies and terms of use of the relevant service providers.

4. About this Privacy Policy

This Policy is written in simple language so that it is easy to understand. If something is not clear, We invite individuals to contact Us so that We can provide assistance. Our contact details are provided in section 11 below. They will also be provided every time that We make contact with, an individual.

This Policy outlines the current personal information handling practices of AISA. We will update this Policy when Our information handling practices change and We will publish updates on Our Website and through Our email lists.

While We publish Our Privacy Policy on Our Website so that it is easily accessible, We also make copies available on request in paper format. In most circumstances We do not charge a fee for providing a copy of the Policy. If however, a request is made for a copy in some other format (foreign language requirements or those linked to disabilities such as sight or hearing impairment), special arrangements may need to be made and a charge may apply.

5. Consent

In all cases where consent is required, whether it be express consent (verbal, in writing, click-wrap tick box) or implied consent (browse-wrap without a tick-box and other behaviour which indicates consent through continued use), it must be voluntary, current, specific and based upon adequate information about the circumstances and choices available to You as an individual. Naturally, You, the individual must have the capacity to understand and to give consent (for example be 16 years or older) and be able communicate consent. Individuals who are not sure about giving consent are encouraged to contact Us. See section 11 for contact details.

6. The Australian Privacy Principles Governing the Handling of Personal Information

AISA is committed to making every reasonable effort to manage personal information in an open and transparent way.

6.1 Open and Transparent Management of Personal Information

To support this commitment, We have implemented practices, procedures and systems to align Our handling of personal information with principles that have been derived from Australian and international privacy law, international standards and best practice.

These practices, procedures and systems are intended to regulate Our internal and external business operations through the use of administrative, technical and physical controls. The legal notices published on Our Website are examples of Our administrative controls. Technical and physical controls are generally not made publicly available for security reasons.

This Policy, together with Our Website Terms of Use and Email Legal Notice, sets out how We provide for open and transparent management of personal information, to give individuals the ability to make informed choices about AISA services and communications.

6.2 Anonymity and Pseudonymity

As an individual, You can choose to remain anonymous (You cannot be identified and We do not collect personal information), or You can choose to use a pseudonym (You can use a name, term or description that is different from Your own) when dealing with Us.

Circumstances where We give individuals the option to remain anonymous or to use a pseudonym include, for example, where individuals prefer not to be identified, to be left alone, to avoid direct marketing, to keep their whereabouts and choices from others, and to express views in the public arena without being identified.

Examples of circumstances where We Will need to know the identity of the person that We are dealing with relate to the provision of the AISA services, where identification is required or authorised by law, where a refund is requested, for dispute resolution, where access to information is requested for correction and where cost becomes excessive or impractical without knowing the identity of an individual We are dealing with.

6.3 Collection of Solicited Personal information

We are committed to collecting personal information by lawful and fair means and wherever possible only collecting it directly from the individual concerned.

We collect personal information from individuals where the information is reasonably necessary for one or more of the AISA functions, activities and legal obligations relating to the services We provide. Most particularly, we collect personal information to provide Member services.

In providing AISA services to individuals and to organisations, partners and other stakeholders, it is generally not necessary to collect sensitive personal information.

For internal human resourcing, We do collect sensitive personal information, such as religious beliefs, trade union memberships and health information when it is required for employment reasons, or by law. We may solicit or request personal information from a third party such as an employment agency or referees in the context of employment. We may collect dietary and other information pertaining to religion in relation to catering services at various conferences and other AISA events.

In most instances where We collect personal information, We only do so after a direct request to, and with the consent of the individual to whom the information relates. In exceptional circumstance and for human resourcing, or when authorised or required by law, We may collect personal information from some source other than the individual themselves.

In circumstances where We provide AISA services to an organisation, We may solicit personal information from the organisation about an individual, but We still require the consent of each individual before their personal information is shared with Us.

6.4 Dealing with Unsolicited Personal information

Personal information is sometimes provided to Us in circumstances where We have not requested it. In these circumstances, where the information is unsolicited, We will examine whether it could have been collected under the Policy outlined in section 6.3 above. We will then apply Our minds and decide whether this unsolicited information should be retained, de-identified or destroyed. Having made that decision, We will implement the decision within a reasonable time.

We do not actively seek to collect unsolicited information.

6.5 Notification of the Collection of Personal Information

This Policy, other legal notices published on Our website and Our internal practices, procedures and systems (administrative controls) are Our way to ensure that individuals know about the personal information that AISA collects.

We are committed to making all reasonable efforts to inform individuals about the personal information We collect before We collect it, for example by making this Policy and Our other Legal Notices available. We will also inform individuals about collection at the time We collect personal information, for example when individuals engage Us to provide AISA services, including membership, conference registration and attendance, through website activity and other forms of communication such as email and text messaging.

In exceptional circumstances where this does not happen, for example, when We receive unsolicited personal information from a third party which We decide to retain, We will inform individuals as soon as reasonably possible after the collection of personal information.

Through this Policy and other legal notices published on Our Website, We seek to ensure that individuals are informed about the reasons for the collection, and that they know how to contact the accountable office bearers at AISA. See section 11 below for details.

6.6 Use or Disclosure of Personal Information

Where We hold personal information about an individual that was collected for a particular purpose (the primary purpose) We will not use or disclose the information for another purpose (a secondary purpose) unless required or authorised by law, the individual has consented, or the individual would reasonable expect Us to use or disclose it for a related purpose. An example of a related purpose in these circumstances might be disclosure to a next-of-kin or health care provider in the case of an employee.

In some circumstances, for example, where We believe that the AISA service may be improved through new technologies such as data science (analytics), or where We see a benefit to individuals, We may use personal information that has been provided to Us by the individual themselves or received from third parties for a purpose that is different form the purpose for which it was given to Us in the first place. Where We do this, We will use and/or disclose the personal information in a de-identified format.

Broadly speaking, We use (handle and manage) personal information internally for 3 reasons:

- To provide AISA services to Members, including for conferences and events:
  - Examples include: Name, address (physical, postal, email and Internet Protocol address), telephone numbers, cookies, change management, assessments, reports and device related information, such as a MAC address and/or geolocation;
- To build relationships with third party organisations that will benefit Members and help fulfill AISA's purpose:
  - Examples include: Name, address (physical, postal, email and Internet Protocol address), telephone numbers of responsible administrative and other individuals at universities, TAFEs, sponsor and partner organisations; and
- For internal human resourcing:
  - Examples include: Name, address (physical, postal, email and Internet Protocol), health information, medical service provider and counselor details, next-of-kin, spouse or partner, banking details, tax, photo identity, trade union membership, religious beliefs, gender, cultural and ethnic identity, qualifications, training and the like.

We do not collect biometric forms of personal information such as fingerprints.

We also use and retain personal information records which are required to be retained for legal, business and evidential reasons. Sometimes these come from external sources and third parties.

Broadly speaking We disclose personal information (release it outside of Our possession or control) for the same primary reasons listed above, providing AISA's services, fulfilling AISA's purposes (for example, by forming relationships with government, sponsors, business and conference organisers), for human resourcing and where there is a legal obligation to do so.

6.7 Direct Marketing

In seeking to fulfill AISA purposes and dealing with Members, other individuals and organisations, We ask for consent to communicate directly with the individuals concerned in order to provide information and to promote AISA.

Whenever We do, We allow individuals to opt-out of receiving direct communications and direct marketing notifications. When individuals request Us to stop communicating with them, We will comply with that request.

If an individual requests information about how We came to have their personal information, We will respond, and provide the source of an individual's personal information wherever possible. We will respond to these requests within a reasonable time (thirty (30) business days).

We do not disclose, sell or share personal information to third parties for direct marketing purposes.

6.8 Cross-border Disclosure of Personal Information

AISA operates from various locations in Australia. These operations include all aspects of internal operations that support AISA's purposes as well as the provision of management and Member 'live' services such a video and telephone conferencing and electronic voting (where personal information travels over telecommunications lines) and the storage of static personal information in data warehouses and on information systems.

AISA Members are individuals, located in Australia and abroad, with the result that personal information may flow from Australia to other countries, especially as a result of international travel and conferencing.

AISA relies on various third party service providers such as telecommunication service providers and Internet Service Providers. These are primarily based in Australia and the United States, but may also be in other countries.

Because information systems enable Our services, personal information may be located or disclosed in transit and in a static format. Individuals are cautioned to consider how their personal information moves and is stored on global information systems and to make appropriate choices.

6.9 Adoption, Use or Disclosure of Government Identifiers

We do not adopt, use or disclose government identifiers of an individual as Our own identifiers.

We do use and disclose government identifiers such as Australian Tax File Numbers, for example, for human resource purposes and where required or authorised by law.

6.10 Quality of Personal Information

We are committed to taking such steps as are reasonable in the circumstances to ensure that the personal information We collect, hold, use and disclose is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

To do this, We ask individuals to assist Us. We provide various technical means, including email notifications and user registration access where individuals can access, verify and update the personal information records that We hold. We ask individuals to participate by ensuring their information is accurate, up-to-date, complete and relevant. Individuals are also encouraged to use the access and correction facilities that We provide. See sections 6.12 and 6.13 below. This is particularly important in the event that AISA information systems are breached so that We know how to contact You and provide You with information that will help protect you.

6.11 Security of Personal Information

We are committed to taking reasonable steps to protect personal information that We hold from misuse, (wrong or improper use) interference (access even where the content is not necessarily modified) and loss (accidental, inadvertent, misplaced personal information).

We are also committed to securing personal information from unauthorised access (by someone that is not permitted access the information), modification (alteration by someone that is not permitted to do so, or who acts beyond the scope of their authority to modify personal information) and unauthorised disclosure (where personal information is released from Our effective control without authority).

To comply with law and manage risk, Our practices, procedures and systems aim to protect the confidentiality, integrity and availability of Our information systems and information, especially the personal information that We collect, hold, use and disclose.

Where there is no legal obligation to retain records and evidence, and in circumstances where We no longer need personal information to provide AISA services or for any purpose for which the information may be used or disclosed under Australian law, We take reasonable steps to destroy the information or to ensure that the information is de-identified.

Our information security and privacy practices include circumstances where Our data handling practices are outsourced to third parties. Because of this We endeavour wherever possible to bind third party service providers through appropriate legal agreements. We also endeavour to monitor their privacy and security practices where possible.

6.12 Access to Personal Information

Where We hold, or have the right and power to deal with personal information (for example, where it is stored by one of Our third party service providers), We will, on request by an individual, normally give that individual access to their information.

We do this so that individuals know what information We hold on them and because it assists Us to ensure that the personal information that We hold is up-to-date, complete and relevant.

In considering a request for access to personal information by an individual, We will require identification. We reserve the right not necessarily to give access to an individual to their personal information in circumstances, for example, where provided for in law, in instances of commercial sensitivity and where a third party may be negatively affected.

We will respond to an individual's request for access to their information within a reasonable time (thirty (30) business days), and We will consider reasonable requests for access to be given in a particular format, for example, through user registration login, by facsimile, email and postal services. As a matter of courtesy, We will provide reasons for the refusal if access is refused.

No charge will apply when an access to information request is received. We do however reserve Our rights to charge a fee where We incur costs, for example, for photocopying, postage and costs associated with using an intermediary if one is required.

6.13 Correction of Personal Information

Where We hold personal information, We will take reasonable steps to correct it to ensure that, having regard to the purpose for which We hold it, it is accurate, up-to-date, complete, relevant and not misleading.

You, as an individual may request that We correct personal information that We hold about You in circumstances where You believe that the information is inaccurate, out of date, incomplete, irrelevant or misleading.

In considering a request for the correction of personal information that We hold, We will require identification of the requesting individual. We reserve the right not necessarily to effect the changes sought, but undertake to consider reasonable requests and to associate a statement to the record reflecting Our refusal to correct the failed request for correction if We consider refusal the appropriate action.

We will respond to a request to change information within a reasonable time (sixty (60) business days) although changes sought may take longer, for example, because We may need to contact and notify other organisations and individuals about the request.

No charge applies for making a request, correcting personal information or associating a statement for refusal to change a record.

As a matter of courtesy, We will provide reasons for the refusal if correction is refused, and also a reminder of the complaint process available to individuals that feel aggrieved by the refusal.

7. Complaints, Enquiries and Access to Information Requests

In most circumstances, the Australian Information Commissioner will not investigate a complaint if an individual has not first raised the matter with Us. For this reason, We ask individuals to agree to submit all complaints relating to this Policy to Us first, so that We have an opportunity to resolve complaints before individuals proceed to any relevant authority. Individuals are asked to direct all complaints and enquiries to Us at legal@aisa.org.au and to see sections 8 and 11 below for further details.

8. How to make a Complaint, Enquiries and Access to Information Requests

Individuals wanting to lodge a complaint can make general enquiries, request access to their information and complain to Us in writing. This includes email communications, but excludes text and social media.

We will respond to complaints within a reasonable time (thirty (30) business days). As in the case of requests to change information, a longer response time may be needed, for example, because We may need to contact and notify other organisations and individuals affected by the complaint. In this case We will endeavor to respond within sixty (60) business days.

9. Skill, Diligence, Care

AISA will exercise reasonable skill, diligence and care as may reasonably be expected from a similar charitable association.

10. Breach

If, and when, AISA suspects, or becomes aware of a breach of its network or information systems resulting in unauthorised access to, or unauthorised disclosure of personal information

likely to result in serious harm to any individuals to whom the information relates; or where information is lost in circumstances that may lead to unauthorised access to, or unauthorised disclosure of personal information, AISA will:

- Take remedial action;
- Where remedial action fails to adequately limit the risk, notify the individuals concerned, and notify the Office of the Australian Information Commissioner (**Commissioner**): and
- Work with the individuals concerned and the Commissioner to protect everyone and everything concerned.
-

If You suspect or become aware of a breach or an impending breach, please contact us as a matter of urgency on legal@aisa.org.au.

11. How to Contact us

Name	Australian Information Security Association (AISA)
Physical address and the address for receipt of legal service of documents	Level 8, 65 York Street, Sydney, NSW., 2000. Australia
Postal address	Level 8, 65 York Street, Sydney, NSW., 2000. Australia
Phone numbers	+61 (02) 8076 6012
Website address	www.aisa.org.au
Email address	legal@aisa.org.au
ABN	181 719 35 959
Directors	Damien Manuel (Chair)
	Alex Woerndle (Deputy Chair)
	Alex Hoffmann
	Helaine Leggat
	Michael Trovato
	Stephen Knights
	Tracey Edwards
	Nicole Murdoch
Officer	Joshua Craig (Company Secretary)