Aircraft Maintenance Engineers Association of Ontario (AMEAO)

Privacy and Security Standard of Conduct

Original:	April 2025
Revised:	19 April 2026

This Privacy and Security Standard of Conduct is applicable to all representatives, volunteers, unpaid placement students, independent contractors and organizations and their employees and representatives (Personnel) who receive access to personal and confidential information in order to fulfill the scope of their position or contracted services with Aircraft Maintenance Engineers Association of Ontario (AMEAO).

Note: This Standard replaces the previous Privacy Policy of the Aircraft Maintenance Engineers Association of Ontario

Table of Contents

Purpose 4
Scope 4
Definitions 5
Roles and Responsibilities 6
AMEAO's Privacy and Security Standard of Conduct 7
Reporting Privacy and Security Breaches 9
Violations and Disciplinary Measures 10
Safeguards and Controls 10
Protecting Personal Information 10
Retention and Destruction of Personal Information 11
Handling Personal and Confidential Information 12
Clean Desk Policy 12
Secure Wi-Fi Networks Only 13
Transferring Information 13
Reporting an actual or suspected Malicious email 13
Work-from-Home Privacy and Security Protocols 14
Generative Artificial Intelligence 15
Policy Audit 16
Privacy and Security Standard of Conduct Acknowledgement and Agreement 17
Appendix A: Contact and Organization Information 18
Appendix B: Magazine Subscriptions 20

Appendix C: Aviation & Aerospace Workforce Development (AAWD) Program 23
Reporting Privacy and Security Breaches 24
Safeguards & Controls 25
Protecting Personal Information 25
Retention and Destruction of Personal Information 27
Transferring Information 28
Reporting an Actual or Suspected Malicious Email 28
Pre-Approval to Access EOIS-CaMS 29
BIStrainer – Learning Management System (LMS) 30
Computer Elite – Website Security 31
Third Rock Consulting – Website Security 33
Appendix D: Sharing information with Third Parties for Marketing Purposes 36

Purpose

This Privacy and Security Standard of Conduct ("the Standard") supports AMEAO's commitment to privacy and security by establishing clear protocols and behavioural expectations for volunteers, unpaid placement students, and independent contractors and organizations and their employees and representatives who have access to personal and confidential information while fulfilling the scope of their positions and conducting AMEAO business.

AMEAO's Privacy and Security Standard of Conduct is based on the Canadian Standards Association (CSA) Model Code and reflects requirements of applicable legislation, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Freedom of Information and Protection of Privacy Act (FIPPA) and Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)

Protecting privacy and security of personal and confidential information in every aspect of our organization must always remain of critical importance.

All personnel have a duty to protect the personal and confidential information that they are given access to in the course of carrying out their work with AMEAO.

This Standard identifies the following:

- AMEAO's legal and policy requirements relating to privacy and security.
- Responsibilities to protect the privacy and confidentiality of the information handled in the work or scope of services with AMEAO.
- Policies and protocols that must be adhered to in order to ensure that all personal and confidential information that is created, accessed, disclosed, or otherwise handled is protected at all times.

Failure to adhere to the privacy and security protocols outlined in this Standard will result in disciplinary measures, up to and including immediate termination of participation or service contract.

Scope

The requirements, expectations, and responsibilities described in this Standard apply to all personnel of AMEAO, including representatives at all levels, directors, casual employees, volunteers, and placement students who are hired or engaged to work with AMEAO.

Protocols and expectations outlined in the Standard also apply to independent contractors that require access to personal information in order to fulfill the scope of services that they have been contracted to provide.

Definitions

Confidentiality:
Confidentiality means information is available or disclosed only to authorized individuals, entities or IT processes. Examples of threats against confidentiality include, but are not limited to, unauthorized access to information, eavesdropping, and unsecured disposal of documents.

Information Security:
Information security is concerned with managing risks and limiting harm related to potential or actual compromise of the confidentiality, integrity, or availability of information and systems. AMEAO is committed to ensuring that the proper security structures and protocols are in place in order to respect and administer the protection of personal information that we must collect.

Personal Information:
Personal information is any information about an identifiable individual that is recorded in any form, such as name, social insurance number, address, phone number, gender, age, education, and employment history.

Privacy:
Privacy is the right of the individual to control the collection, use and/or disclosure of their personal information. AMEAO is committed to respecting privacy and protecting personal information of all individuals.

Privacy Breach:
A privacy breach is the loss of, unauthorized access to, or disclosure of, personal information. Privacy breaches can happen when personal information is stolen, lost or mistakenly shared.

Security Breach:
A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices. It results in information being accessed without authorization.

Roles and Responsibilities

All Personnel (Representatives, Placement Students, Volunteers and Independent Contractors): All representatives (including management and directors), volunteers, unpaid placement students, and independent contractors and organizations and their employees and representatives that are engaged by AMEAO must be aware of and comply with the requirements of the Standard.

Management: Directors (and Project Managers as applicable) have the added responsibility to ensure that all personnel and independent contractors in their program comply with the Standard. All contractors and volunteers have executed agreements with AMEAO in which confidentiality is included and agreed to by signature. Management must take disciplinary actions, as appropriate, when deviations from required policies and protocols occur, even if no actual privacy or security incident has occurred.

Privacy Officer: AMEAO's designated Privacy Officer must ensure that the Standard is maintained and kept up to date to be relevant and consistent with AMEAO's working conditions, business objectives, contractual obligations, and legislative requirements. The Privacy Officer for AMEAO is the President. Refer to Appendix A for Privacy Officer contact details.

AMEAO's Privacy and Security Standard of Conduct

AMEAO's Privacy and Security Standard of Conduct: AMEAO's Privacy and Security Standard of Conduct is based on the Canadian Standards Association (CSA) Model Code and reflects requirements of applicable legislation, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and the Freedom of Information and Protection of Privacy Act (FIPPA).

As part of AMEAO's commitment to ensure that personal information is kept confidential and maintained pursuant to its privacy standards, AMEAO has adopted the 10 Privacy Principles contained within the Canadian Standards Association Model Code for the Protection of Personal Information, which is a national standard of Canada.

AMEAO'S 10 Privacy Principles are as follows:

1. Accountability: AMEAO is responsible for the protection of personal information collected through program activities and the AMEAO website. This responsibility extends when required transfers of personal information to third parties are made.

2. Identifying the purposes for collecting Personal Information: We must explain the purpose(s) for the collection of any personal information that we are required to collect before we ask the individual to disclose it to us.

3. Obtaining Consent: The only personal information that AMEAO can collect is with an individual's knowledge and consent. Participants can choose not to disclose any personal information that we ask them to provide, even though a decision to withhold some personal information may result in AMEAO's inability to provide them with services.

4. Limiting Collection: AMEAO must only collect the type of personal information that is necessary to fulfill the objectives at hand and must ask for and collect personal information directly from the individual that we require it from. As outlined in Principle # 3, an individual has the right to withhold their personal information that is requested from them, even though it may result in an inability to provide them with services.

5. Limiting Use, Disclosure and Retention of Information: The personal information that is collected must only be used for the purpose(s) that were explained to the individual from whom it was collected. Personal information must never be shared for any other purpose(s) without the individual's knowledge and consent, except as permitted by law. The retention period for which an individual's personal information is held on record by AMEAO, before it is securely and irreversibly destroyed, depends upon the retention requirements specific to the program/service that the person accesses, at the time they access it.

6. Ensuring accuracy of Personal Information: As the personal information that we collect is provided directly from the individuals for whom it pertains, it must be assumed that the information provided is correct at the time that it is provided. If we suspect there has been a mistake, we will ensure best efforts are made to work with the individual to ensure the data provided is current and correct.

7. Safeguarding Personal Information: AMEAO must use necessary safeguards and controls to protect the personal information that is in their possession. (See the Safeguards and Controls section of this Standard).

8. Openness about AMEAO Privacy and Security Standard of Conduct and Practices: AMEAO must make their Privacy and Security Standard of Conduct available to the public at all times.

9. The Right of an Individual to Access Their Personal Information: Upon the written request of an individual, AMEAO will confirm any personal information that it has about them in our possession. AMEAO will also provide the individual with access to their personal information and explain again what it is being used for, if applicable. Anyone who wishes to access their personal information on record with AMEAO must make a written request to AMEAO's Privacy Officer (or assigned delegate).

Note: *If an AMEAO representative receives a request from an AAWD Participant requesting a copy of their personal information on record with AMEAO, the representative must forward the request to the Privacy Officer* (or assigned delegate).

10. AMEAO Compliance: AMEAO must provide a contact for whom people can submit any concerns they might have regarding our compliance to our Privacy and Security Standard of Conduct. AMEAO mailing address and contact information is provided on their publicly available website for this purpose as well.

Reporting Privacy and Security Breaches

The protocols outlined below for reporting a **potential or actual privacy or security breach** must be followed by all volunteers, unpaid placement students, and independent contractors and organizations and their employees and representatives with AMEAO.

PART A – PRIVACY BREACHES:
A privacy breach is the loss of, unauthorized access to, or disclosure of, personal information. Privacy breaches can happen when personal information is stolen, lost or mistakenly shared. Examples of privacy breaches include clients' personal information being left near printers or placed in a recycling bin, the loss or theft of clients' personal information while being transported to an employer's site, personal information mistakenly being left on a meeting table after the meeting has adjourned, and other instances involving the loss of, unauthorized access to, or disclosure of, personal information.

PART B – SECURITY BREACHES:
A security breach is any incident that results in unauthorized access to computer data, applications, networks, or devices. It results in information being accessed without authorization. Examples of security breaches include inadvertent disclosure of passwords, suspected or actual malware or other cybersecurity threats, the loss or theft of an organization-owned laptop or cell phone, and other potential or actual breaches that relate to computer data, applications, networks and devices.

If a potential or actual privacy and/or security breach is suspected or has occurred, **the following steps must immediately be taken**:

1. Call the Privacy Officer (or assigned delegate) (Refer to Appendix A for contact information). If you are unable to reach the Privacy Officer for a live phone call, leave a voicemail to briefly explain the potential or actual security breach and proceed to step 2.

2. If email is accessible, send an **urgent** email to the following contacts to explain the potential or actual security breach. Time is of the essence with reporting security breaches, so be as succinct as possible. ***Be sure to mark the email as urgent.***

admin@ame-ont.com AMEAO Admin
president@ame-ont.com AMEAO President

Should an investigation reveal an actual breach, affected parties shall be notified of the extent of the breach.

Violations and Disciplinary Measures

All personnel and independent contractors that receive access to personal information in order to carry out their responsibilities or services to AMEAO have a duty to protect the personal information to which they are given access in the course of carrying out their role or scope of services.

Upon completion of an investigation, anyone found in violation of the Standard may be subject to remedial training and/or disciplinary action, up to and including immediate termination of participation in AMEAO activities or service contract.

Safeguards & Controls

Protecting Personal Information

When personal information is in AMEAO's care, the individual personnel are responsible for ensuring that it is maintained in a confidential and secure manner and that it is protected from unauthorized use or disclosure.

All personnel and independent contractors shall:

- ✓ Only use the limited personal information to which they have access as necessary in fulfilling the requirements of their position or scope of work with AMEAO.
- ✓ Only collect, use, and disclose personal information if/as necessary, to deliver AMEAO's and AAWD services.
- ✓ Have an individual's signed consent before releasing their personal information for any purpose.
- ✓ Inform your supervisor and AMEAO's Privacy Officer (or assigned delegate) of any verbal or written requests received from Participants requesting a copy of their personal information on record with AMEAO.
- ✓ Immediately report any suspected or actual privacy or security breach by following the required reporting protocols outlined in the 'Reporting Privacy and Security Breaches policy contained in the Standard.

All personnel and independent contractors shall not:

- ✗ Access personal information unless it is required in order to fulfil the requirements of the position or service agreement with AMEAO.

- ✗ Disclose personal information to which they have access to unless it is required to fulfil the requirements of the position or service agreement with AMEAO.
- ✗ Discuss a client's personal information with other individuals, including other members of personnel or independent contractors, unless it is required to fulfil the requirements of their position or service agreement with AMEAO. If they must discuss personal information, they must ensure that it is done in a private area and away from other workers and clients.

Retention and Destruction of Personal Information

Personal Information and Participant Records:
AMEAO has contractual obligations with AMEAO funders to retain for specific periods personal information that belongs to its clients. AMEAO must also ensure that those records are securely and irreversibly destroyed when they are no longer required to deliver their contracted services or to comply with retention obligations under their funding agreements. This applies to both paper and electronic records.
Personal Information will be uploaded to a secure, password-protected online account for secure storage and retrieval as required to deliver project services.

In order to ensure that no such original records are destroyed prior to contractual obligations being fulfilled, and to avoid improper destruction of such records, anyone outside of management with AMEAO is strictly prohibited from irreversibly destroying original paper and/or electronic records of such information.

The secure and irreversible destruction of files is only scheduled when records containing personal information are no longer needed to deliver AMEAO contracted services or to comply with the contractual retention period obligations.

Intellectual Property and Organization Records:
In order to fulfill business strategies, requirements and obligations, AMEAO creates, utilizes and retains important intellectual property and company records. Some examples include, but are not limited to, the following:

- Funding Applications
- Funder Reports
- Fundraising Lists
- Proposals
- Personnel & Independent Contractor Contracts and/or Records

Handling Personal and Confidential Information

In order to ensure that all personal and confidential information that AMEAO representatives, personnel and/or independent contractors handle in the course of fulfilling their position or service contract with AMEAO is kept protected and confidential, they **shall not**:

- ✗ Disclose or share personal information with unauthorized individuals who do not have a need to know the personal information for the purpose of fulfilling the requirements of the position or service contract with AMEAO.
- ✗ Access any personal information that is available to them in electronic format over an unsecured wireless connection.

Note: *As defined earlier in the Standard, personal information means any information about an identifiable individual, including, but not limited to, their name, address, gender, age, education, social insurance number, and employment history.*

Clean Desk Policy

As communicated throughout the Standard, all representatives, unpaid placement students, volunteers and independent contractors have an obligation to protect the personal information to which they are given access in the course of their employment or service agreement with AMEAO.

As part of this due diligence for the protection of personal information, AMEAO has adopted a "Clean Desk Policy" that they are required to follow in order to guard against unauthorized access to personal and confidential information. This requires that they:

- ✓ Use the screen lock functionality: press 'Ctrl – Alt – Delete' and click 'Lock Computer' when they leave their desk if there is the possibility that it may be accessed by another person.
- ✓ Remove all personal and confidential information from tables, whiteboards, and flipcharts, and ensure that conference calls are terminated after they have finished a meeting (virtual or in-person)
- ✓ Ensure that all personal and confidential documents are secured before they leave the office
- ✗ Shall not place photocopies of personal or confidential materials that are no longer needed in a recycling bin or the garbage. A shredder, or equivalent means of destruction, must be used.
- ✗ Shall not leave personal or confidential materials unattended on their desk or in any other open, unsecured area, such as near printers, copy machines, facsimile machines, or meeting rooms where they could be accessed by another person.

Computers Used by Independent Contractors:
Independent contractors, by nature of their service agreement with AMEAO, are responsible for providing their own tools, equipment, software, and insurance necessary to fulfill the provisions for the services they are contracted to provide. Independent contractors who receive access to personal information in order to fulfill their scope of contracted services are also required to adhere to AMEAO's protocols for protecting the personal information to which they are given access.

Secure Wi-Fi Networks Only

All personnel and independent contractors are required to **always use a secure Wi-Fi network** while conducting work or business for AMEAO online.

Personal information **must never** be accessed over an unsecure wireless connection. An unsecure wireless connection is one that is open to the public and can be accessed without a password. They are usually available in places such as cafés where people can join the Wi-Fi network for free without a password.

Transferring Information

In the event that representatives, personnel and/or independent contractors need to communicate a password for a protected file among project team members in order to fulfill their services, they must Communicate the password in a separate email or by phone call. You must never include the password in the same email as the password-protected document.

Reporting an Actual or Suspected Malicious Email

If a malicious email or suspected malicious email has been clicked on, it must be reported immediately to the Privacy Officer (or assigned delegate) so that an investigation can be initiated to determine if any further action is required. This is imperative because clicking on a malicious email can result in a security breach, such as unauthorized access to computer data, applications, networks, or devices.

If a malicious email or suspected malicious email has been clicked on, the representative, personnel and/or independent contractor must **immediately take the following steps**:

1. Call the Privacy Officer (or assigned delegate) (Refer to Appendix A for contact information). If you are unable to reach the Privacy Officer for a live phone call, leave a voicemail to briefly explain the potential or actual security breach and proceed to step 2.

2. If email is accessible, send an **urgent** email to the following contacts to explain the potential

or actual security breach. Time is of the essence with reporting security breaches, so be as succinct as possible. ***Be sure to mark the email as urgent.***
admin@ame-ont.com AMEAO Admin
president@ame-ont.com AMEAO President

Work-from-Home Privacy and Security Protocol

The work-from-home protocols described in this policy apply to all volunteers, unpaid placement students, and independent contractors and organizations and their employees and representatives who work remotely at any time.

All obligations to protect all personal information, where access is required fulfill a role or scope of services, remain in effect while working or performing services remotely and/or from home. To ensure that all personal and confidential information remains protected at all times while working remotely, the following protocols must be followed:

Using a Secure Wi-Fi Network:
While working or performing services remotely, use of a secure Wi-Fi network must be ensured at all times.

Personal information **must never** be accessed over an unsecure wireless connection. An unsecure wireless connection is one that is open to the public and can be accessed without a password. They are usually available in places such as cafés where people can join the Wi-Fi network for free without a password. It is not permitted to conduct any remote-based work or services for AMEAO until a secure Wi-Fi network is available.

No Removal of Client Files and No Saving Personal Information:
As AMEAO handles sensitive personal and confidential information, it is **prohibited to print** client files for use at home or anywhere else.
All personnel are strictly prohibited from saving personal information on portable memory sticks (USBs), laptops, computer desktop, or cell phones that are not password protected.

Printing Confidential Information:
Printing of documents that contain personal information may be permitted by authorized representatives, personnel and independent contractors only if required to fulfill project services. Once utilized, all documents must be either shredded, destroyed by equivalent means, or locked in locking filing cabinets.

Logging Out of Work Accounts:
All personal information in representatives, personnel and independent contractors' control must be secured at all times while they work. Therefore, if their computer will be unattended and accessible by another person, they must ensure that it is locked. If the computer is to be

used by another person they must log out of all accounts and systems to ensure the privacy and security of personal information.

Non-Disclosure of Personal Information:
If representatives, personnel, and/or independent contractors hold a position that requires them to provide services to clients over the phone or through online technology while they are working remotely and they anticipate discussing personal information, they **must have a private space** where they are not in hearing distance of other people.

It is **strictly prohibited** to share personal information with unauthorized individuals who do not have a need to know for the purpose of fulfilling the requirements of their role with AMEAO. This means that all personal information that is handled must **not** be discussed in any way or shared with family, friends, or other known individuals to the representatives, personnel and independent contractors.

Note: *As defined earlier in the Standard, personal information is any information about an identifiable individual that is recorded in any form, such as name, social insurance number, address, phone number, gender, age, education, and employment history.*

Generative Artificial Intelligence

Purpose
Publicly available applications driven by generative artificial intelligence (GenAI) such as chatbots or image generators are becoming increasingly popular. While these content-generating tools may offer attractive opportunities to streamline work functions and/or increase our efficiency, they come with serious security, accuracy and intellectual property risks.

This policy applies to the use of any third-party or publicly available GenAI tools, and other similar applications that mimic human intelligence to generate answers, work, or perform certain tasks (ex. Note taking).

Guidelines

DO:

- ✓ Understand that GenAI tools may be useful but are **not a substitute** for human judgement and creativity.
- ✓ Understand that many GenAI tools are prone to false answers or information, or information that is stale, and therefore responses must always be carefully verified by a human.
- ✓ Inform others when you have used or plan to use a GenAI tool to help perform a task (ex. Note taking)

✓ Verify that any response from a GenAI tool that you use is **accurate, appropriate, not biased, not in violation of any other individual or entity's intellectual property or privacy and consistent** with policies and applicable laws.

DO NOT:

✗ Do not upload or input any **confidential, proprietary, or sensitive** information into any GenAI tool. (Ex. Passwords and other credentials, non-public information)

✗ Do not upload or input any **personal information** (names, addresses, etc.) about any person into any GenAI tool.

✗ Do not represent work generated by a GenAI tool as being your own original work.

Violations

Anyone found in violation of the this policy may be subject to remedial training and/or disciplinary action, up to and including immediate termination of participation in AMEAO activities or service contract.

Policy Audit

AMEAO will endeavour to have the policy audited at an interval not to exceed 5 years, or sooner if there are major revisions required.

Privacy and Security Standard of Conduct Acknowledgement and Agreement

I expressly acknowledge that:

(i) I have received a copy of AMEAO's Privacy and Security Standard of Conduct (the "Standard") and understand its full contents.

(ii) I am required to protect all personal and confidential information to which I receive access for the purpose of fulfilling the scope of my position or contracted services with AMEAO, including full compliance with the policies and protocols of the Standard and AMEAO's Privacy and Security Standard of Conduct.

(iii) Anyone found in violation of the Standard will be subject to disciplinary action, up to and including termination of employment or service contract.

(iv) I will immediately report any suspected or actual privacy or security breach by following the required reporting protocols outlined in the 'Reporting Privacy and Security Breaches policy of the Standard.

Name (please print)

Signature

Date of Signature

Aircraft Maintenance Engineers Association of Ontario (AMEAO)

Privacy and Security Standard of Conduct

Appendix A
Contact and Organization Information

Original: April 2025
Revised: 31 October 2025

AMEAO Contact and Organization Information

AMEAO Privacy Officer:
Louis Anderson
(416) 892-8061
president@ame-ont.com

AMEAO Administrator:
Drea Reid-Sneath
(807) 738-0070
admin@ame-ont.com

Aircraft Maintenance Engineers Association of Ontairo:
403-7360 Bramalea Road
Mississauga ON L5S 1M7
(647) 250-7488

Aircraft Maintenance Engineers Association of Ontario (AMEAO)

Privacy and Security Standard of Conduct

Appendix B
Magazine Subscriptions

Original: April 2025
Revised: 31 October 2025

Magazine Subscriptions

As a member benefit, the Association has supplied mail addresses of its members to various publications. The Association has signed confidentiality agreements with these publishers requiring them to keep this list confidential and to ensure that this subscription list is not used to solicit or advertise to the members. A sample of this confidentiality agreement follows:

NONDISCLOSURE AGREEMENT

THIS NONDISCLOSURE AGREEMENT (THE "AGREEMENT") IS ENTERED INTO BY AND BETWEEN AIRCRAFT MAINTENANCE ENGINEERS ASSOCIATION OF ONTARIO WITH ITS PRINCIPAL OFFICES AT 403 – 7360 BRAMALEA ROAD, MISSISSAUGA, ONTARIO L5S 1M7, ("DISCLOSING PARTY") AND [INSERT NAME OF PUBLISHING COMPANY HERE], LOCATED AT [INSERT PUBLISHERS ADDRESS HERE] ("RECEIVING PARTY") FOR THE PURPOSE OF PREVENTING THE UNAUTHORIZED DISCLOSURE OF CONFIDENTIAL INFORMATION AS DEFINED BELOW. THE PARTIES AGREE TO ENTER INTO A CONFIDENTIAL RELATIONSHIP WITH RESPECT TO THE DISCLOSURE OF CERTAIN PROPRIETARY AND CONFIDENTIAL INFORMATION ("CONFIDENTIAL INFORMATION").

CONFIDENTIAL INFORMATION:

ASSOCIATION MEMBER NAMES, EMAIL ADDRESSES AND OTHER PERSONAL CONTACT INFORMATION, INCLUDING THOSE OF THE BOARD OF DIRECTORS AND SUPPORT PERSONNEL, WITHOUT THE EXPRESSED WRITTEN PERMISSION OF THE PRESIDENT, VICE-PRESIDENT OR NAMED DESIGNATE

1. Definition of Confidential Information. For purposes of this Agreement, "Confidential Information" shall include all information or material that has or could have commercial value or other utility in the business in which Disclosing Party is engaged. If Confidential Information is in written form, the Disclosing Party shall label or stamp the materials with the word "Confidential" or some similar warning. If Confidential Information is transmitted orally, the Disclosing Party shall promptly provide a writing indicating that such oral communication constituted Confidential Information.

2. Exclusions from Confidential Information. Receiving Party's obligations under this Agreement do not extend to information that is: (a) publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party; (b) discovered or created by the Receiving Party before disclosure by Disclosing Party; (c) learned by the Receiving Party through legitimate means other than from the Disclosing Party or Disclosing Party's representatives; or (d) is disclosed by Receiving Party with Disclosing Party's prior written approval.

3. Obligations of Receiving Party. Receiving Party shall hold and maintain the Confidential Information in strictest confidence for the sole and exclusive benefit of the Disclosing Party. Receiving Party shall carefully restrict access to Confidential Information to employees,

contractors and third parties as is reasonably required and shall require those persons to sign nondisclosure restrictions at least as protective as those in this Agreement. Receiving Party shall not, without prior written approval of Disclosing Party, use for Receiving Party's own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of Disclosing Party, any Confidential Information. Receiving Party shall return to Disclosing Party any and all records, notes, and other written, printed, or tangible materials in its possession pertaining to Confidential Information immediately if Disclosing Party requests it in writing. AME Association of Ontario Privacy Policy

4. Time Periods. The nondisclosure provisions of this Agreement shall survive the termination of this Agreement and Receiving Party's duty to hold Confidential Information in confidence shall remain in effect until the Confidential Information no longer qualifies as a trade secret or until Disclosing Party sends Receiving Party written notice releasing Receiving Party from this Agreement, whichever occurs first.

5. Relationships. Nothing contained in this Agreement shall be deemed to constitute either party a partner, joint venturer or employee of the other party for any purpose.

6. Severability. If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted so as best to affect the intent of the parties.

7. Integration. This Agreement expresses the complete understanding of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations and understandings. This Agreement may not be amended except in a writing signed by both parties.

8. Waiver. The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights.

This Agreement and each party's obligations shall be binding on the representatives, assigns and successors of such party. Each party has signed this Agreement through its authorized representative.

Aircraft Maintenance Engineers Association of Ontario (AMEAO)

Privacy and Security Standard of Conduct

Appendix C
Aviation & Aerospace Workforce Development (AAWD) Program

Original: April 2025
Revised: 31 October 2025

Aviation & Aerospace Workforce Development (AAWD) Program

Additional Clauses to AMEAO Privacy and Security Standard of Conduct

Addendum specific to AAWD

All AAWD Participants must review and sign the government provided Participant Form including a Consent to Release Information form before any personal information is released to third parties for the purpose of providing AAWD program participation, reporting or otherwise.

Reporting Privacy and Security Breaches

PART A – PRIVACY BREACHES:

A privacy breach is the loss of, unauthorized access to, or disclosure of, personal information. Privacy breaches can happen when personal information is stolen, lost or mistakenly shared. Examples of privacy breaches include clients' personal information being left near printers or placed in a recycling bin, the loss or theft of clients' personal information while being transported to an employer's site, personal information mistakenly being left on a meeting table after the meeting has adjourned, and other instances involving the loss of, unauthorized access to, or disclosure of, personal information.

PART B – SECURITY BREACHES:

A security breach is any incident that results in unauthorized access to computer data, applications, networks, or devices. It results in information being accessed without authorization. Examples of security breaches include inadvertent disclosure of passwords, suspected or actual malware or other cybersecurity threats, the loss or theft of an organization-owned laptop or cell phone, and other potential or actual breaches that relate to computer data, applications, networks and devices.

If a potential or actual privacy and/or security breach is suspected or has occurred, **the following steps must immediately be taken**:

Note: If you are unable to reach the listed party for a live phone call, leave a voicemail to briefly explain the potential or actual security breach, proceed to the next step.)

1. Call the AAWD Privacy Officer (Leigh Kras) at 905-975-3880.
2. Call the AAWD Project Manager (Marlene Conway Diels) at 905 536 1371.
3. Call the AAWD Project Administration (Drea Reid-Sneath) at 807 738 0070.
4. Call the Learning Management System (LMS) Service Provider (Stephan McGarvey) at 705 955 0277.
5. Call the AAWD Microsite Service Provider (Rocky Singh) at 416 476 7326.
6. If email is accessible, send an **urgent** email to the following contacts to explain the potential or actual security breach. Time is of the essence with reporting security breaches, so be as succinct as possible. ***Be sure to mark the email as urgent.***

admin@ame-ont.com AMEAO Admin
president@ame-ont.com AMEAO President
marlene.sdf@ame-ont.com AAWD Project Manager (Marlene Conway Diels)
leigh.sdf@ame-ont.com AAWD Privacy Officer (Leigh Kras)
drea.ame.sdf@gmail.com AAWD Project Administration (Drea Reid-Sneath)

Should an investigation reveal an actual breach, affected parties shall be notified of the extent of the breach.

Safeguards & Controls

Protecting Personal Information

When personal information is in AMEAO's care, the individual personnel are responsible for ensuring that it is maintained in a confidential and secure manner and that it is protected from unauthorized use or disclosure.

All personnel and independent contractors shall:

- ✓ Only use the limited personal information to which they have access as necessary in fulfilling the requirements of their position or scope of work with AMEAO.
- ✓ Only collect, use, and disclose personal information if/as necessary, to deliver AMEAO's and AAWD services.
- ✓ Have an individual's signed consent before releasing their personal information for any purpose. If the purpose for which the personnel must release an individual's personal information has been stated to them on the government provided Participant Form/Consent

to Release Information Form(s) used by the designated program, personnel must have the individual's signed consent before releasing their information for the new purpose at hand. For example: AAWD, as funded by the Ministry of Labour, Immigration, Training and Skills Development, must ensure that each Participant is provided with the Notice of Collection of Personal Information and obtain their consent to the indirect collection of personal information set out on the Participant form.

- ✓ Inform your supervisor and AMEAO's Privacy Officer (or assigned delegate) of any verbal or written requests received from Participants requesting a copy of their personal information on record with AMEAO.

- ✓ Immediately report any suspected or actual privacy or security breach by following the required reporting protocols outlined in the 'Reporting Privacy and Security Breaches policy contained in the Standard.

AAWD Project Manager and Program Personnel that manage the Ministry of Labour, Immigration, Training and Skills Development programs shall also ensure that:

- ✓ All signed Participant Registration forms are retained for a period of seven (7) years and are available to the Ministry upon request.
- ✓ Only the Service Provider Registration Authority (SPRA) and employees authorized by the SPRA have access to the EOIS-CaMS, using their assigned EOIS-CaMS Enrolment Numbers and PIN IDs, and that the SPRA and the authorized users abide by the SPRA Terms and Conditions, and the representations made by AMEAO on the SPRA EOIS-CaMS Registration form.

Please see Learning Management System Appendix for security and storage processes and information

All personnel and independent contractors shall not:

- ✗ Access personal information unless it is required in order to fulfil the requirements of the position or service agreement with AMEAO.
- ✗ Disclose personal information to which they have access to unless it is required to fulfil the requirements of the position or service agreement with AMEAO. If the purpose for which they must release an individual's personal information has not yet been explained to them on the Intake and/or Consent to Release Information Form(s) used by the designated program, they must obtain the individual's signed and voluntary consent before disclosing their personal information for the purpose at hand. Consult with AAWD Project Manager in all such cases.
- ✗ Discuss a client's personal information with other individuals, including other members of personnel or independent contractors, unless it is required to fulfil the requirements of their position or service agreement with AMEAO. If they must discuss personal information, they must ensure that it is done in a private area and away from other workers and clients.

Retention and Destruction of Personal Information

Personal Information and Participant Records:
AMEAO has contractual obligations with AMEAO funders to retain for specific periods personal information that belongs to its clients. AMEAO must also ensure that those records are securely and irreversibly destroyed when they are no longer required to deliver their contracted services or to comply with retention obligations under their funding agreements. This applies to both paper and electronic records. Examples of these records, whether in paper form and/or secure electronic form, containing personal information, that are retained by some of their programs to deliver contracted services include, but are not limited to, the following:

- Consent to Release Forms
- Government Participant Forms
- Résumés
- Training Placement Agreements
- Participant Progress Tracking

Personal Information will be uploaded to a secure, password-protected online account for secure storage and retrieval as required to deliver project services.

In order to ensure that no such original records are destroyed prior to contractual obligations being fulfilled, and to avoid improper destruction of such records, anyone outside of management with AMEAO is strictly prohibited from irreversibly destroying original paper and/or electronic records of such information.

Only Project Administration and Project SDF Service Provider Case Worker are permitted to coordinate secure, irreversible destruction of original records with prior, written approval from their Project Manager, the SDF Service Provider Manager.

The secure and irreversible destruction of files is only scheduled when records containing personal information are no longer needed to deliver AMEAO contracted services or to comply with the contractual retention period obligations, and the appropriate Project Administration and Project SDF Service Provider Case Worker have received prior, written approval as outlined above.

Intellectual Property and Organization Records:
In order to fulfill business strategies, requirements and obligations, AMEAO creates, utilizes and retains important intellectual property and company records. Some examples include, but are not limited to, the following:

- Funding Applications
- Funder Reports

- Fundraising Lists
- Proposals
- Personnel & Independent Contractor Contracts and/or Records

Transferring Information

In the event that representatives, Personnel and/or independent contractors need to communicate a password for a protected file with an authorized external party, such as providing an authorized funder representative with a password to access a document they have requested containing clients' personal information, these are the options:

1. Communicate the password in a separate email or by phone call and must never include the password in the same email as the password-protected document.
2. Alternatively, utilize funder secured 'Secure Messaging Portal' as directed.

Reporting an Actual or Suspected Malicious Email

If a malicious email or suspected malicious email has been clicked on, it must be reported immediately to the Project Manager, Project Administration, and Privacy Officer (or assigned delegate) so that an investigation can be initiated to determine if any further action is required. This is imperative because clicking on a malicious email can result in a security breach, such as unauthorized access to computer data, applications, networks, or devices.

If a malicious email or suspected malicious email has been clicked on, the representative, personnel and/or independent contractor must **immediately take the following steps**:

Note: If you are unable to reach the listed party for a live phone call, leave a voicemail to briefly explain the potential or actual security breach, proceed to the next step.)

1. Call the AAWD Privacy Officer (Leigh Kras) at 905-975-3880.
2. Call the AAWD Project Manager (Marlene Conway Diels) at 905 536 1371.
3. Call the AAWD Project Administration (Drea Reid-Sneath) at 807 738 0070.

admin@ame-ont.com AMEAO Admin
president@ame-ont.com AMEAO President
marlene.sdf@ame-ont.com AAWD Project Manager (Marlene Conway Diels)
leigh.sdf@ame-ont.com AAWD Privacy Officer (Leigh Kras)
drea.ame.sdf@gmail.com AAWD Project Administration (Drea Reid-Sneath)

Pre-Approval to Access EOIS-CaMS:

Certain roles at AMEAO require access to Employment Ontario's Information System (EOIS-CaMS).Only the Service Provider Registration Authority (SPRA) and employees authorized by the SPRA have access to the EOIS-CaMS, using their assigned EOIS-CaMS Enrolment Numbers and PIN IDs, and that the SPRA and the authorized users abide by the SPRA Terms and Conditions, and the representations made by AMEAO on the SPRA EOIS-CaMS Registration form.

BIStrainer - Learning Management System (LMS)

System Overview

BIStrainer is an online learning management system developed by Business Improvement Solutions Inc., an Alberta-based training and development company. BIStrainer is used by multinational organizations to provide training to employees and clients in many countries including the United States, Canada, Australia, the United Kingdom, and Germany. The keys to the success of this system include its advanced functionality and scalability.

System Security

System and data/information integrity are one of our top priorities. To secure our system and the data housed on it as well as client and company employee details, we have implemented the following safeguards:

- The system is hosted by independent fully managed firm specializing in providing hosted solutions. Servers are located within Canada and, therefore, are not subject to US laws that permit the US government to access stored data.
- Managed servers have 24/7 support and performance monitoring.
- The entire system, including all data, is backed up nightly.
- Firewalls are set up on the system.
- All software is loaded with secure passwords
- The software is fully patched with updates and safe managed
- Encryption is included in the source code and in the URLS.
- Server access is limited to secured access points with multiple levels of authentication.

Information Integrity

The reporting data and end user information is the heart of the online learning system, therefore, the following measures have been taken to ensure information integrity:

- No user account is permanently deleted to ensure all training records can be retrieved.
- Course completion information is backed up daily onto a separate storage system to ensure no reporting information is lost.
- Proctoring functionality allows courses to be locked for compliance reasons. A predetermined Proctor Manager verifies the identification of the end user, unlocks the training course, and ensures the end user who provided the identification is the one who completes the course.
- Limited access is granted to end users based on their user role in the system.

COMPUTER ELITE - WEBSITE SECURITY

How Computer Elite protects your ame-ont.com website data:

We have deployed HTTPS/SSL security on 'ame-ont.com' to encrypt all website traffic while it is in-transit. This prevents anyone from eavesdropping on website data being sent and received.

Technical: The HTTPS/SSL security on ame-ont.com uses RSA 2048-bit encryption on all website traffic to and from the site.

Technical: The server settings combined with a plugin installed in WordPress ensures that all hyperlinks on the website are using the 'https:' protocol.

The website content (web pages, images, files, scripts/styles) are stored on our web hosting server. The server is located inside Canada and is not physically accessible. Access to the content is only available to select users/groups and selectively to general public. Admin level pages are only available to authorized admin users. Logins are protected by brute force protection that prevents anyone from guessing passwords of other users. All user's passwords are required to meet a baseline security level, with admins requiring a higher level.

Technical: Users and groups are defined within WordPress and determines what pages on the site they have access to and what level of admin access they have if any.

Technical: The web hosting server admin user that can access all content is only accessible by an authorized user of Computer Elite's web department.

Technical: A plugin installed in WordPress called 'WordFence Security' provides the brute force protection and optional multi-factor authentication for admins.

The website database contains all user data and personal account information, is secured behind the web hosting server, and is only accessible to the programming of the website itself, and an authorized user of Computer Elite's web department for development purposes.

Technical: The database is using MySQL and only accepts connections internally within the hosting server so that the code can access it, but is not accessible to anyone outside the server. Data is only pulled out and shown on the website after the user has authenticated with WordPress and depends on the user's level of access.

The login to the web hosting server is protected by brute force protection and multi-factor authentication. This prevents anyone from guessing passwords to log in and must be authorized as/by a staff member of the Computer Elite web department. All accounts on the web hosting server are separated so that they cannot access each other's files or databases.

Technical: The website's files and database are stored on a cPanel Web Hosting platform. The web hosting platform also uses HTTPS/SSL with RSA 2048-bit encryption on all traffic to and from the platform. The logins to the web hosting are protected by cPHulk Brute Force protection which prevents anyone from guessing passwords and automatically blocks an attacker's IP address, as well as employs Geo-IP blocking that only allows authorized countries to reach the login system and blocks all other countries.

The website and server software is monitored for vulnerabilities/patches and provides us an alert when action is required. We then take appropriate action if updates are required to maintain the security or contact you if further work is required to make this happen. There is an antivirus on the server that scans the system for malware and viruses and quarantines any detected risks.

Technical: A plugin is installed in WordPress to check for and alert for vulnerabilities, as well as the server software itself does the same on the server side of things.

The web hosting server is redundant so that if there was a major system crash or data loss event we could restore the system and the websites back onto a different server to get it all back online.

Technical: We use Acronis software to replicate/make a copy of the server each night to our secure offsite storage. This storage is encrypted so that it is not physically accessible and can only be restored by an authorized Computer Elite technician.

Technical: Note: This is not equivalent to a regularly scheduled backup which is an extra paid service. Redundancy allows us to recover the system onto a different system. A backup allows reverting individual files/data to a previous backup date in case of a non-major event such as a file corruption or an overwritten data record.

THIRD ROCK CONSULTING – WEBSITE SECURITY

Website Security, Storage & Automation Overview
Website: https://www.amesdfproject.ca/
Platform: Squarespace
Automation: Zapier
Data Storage (Secondary): Google Drive (Google Sheets / Excel)

1. Hosting & Core Infrastructure

- The AMESDF Project website is hosted on Squarespace, a commercial website hosting and content management platform.
- Squarespace operates on enterprise-grade cloud infrastructure with centralized security controls, monitoring, and regular updates.
- Website content and form submission data initially reside within Squarespace-managed servers.
- Google Drive is used to store the form submission data for processing in the backend. Zapier is used to automate email replies – storing only the name and email address provided in the forms.

2. Data Flow Overview (End-to-End)
Form submission process:

1. A user submits information via a form on the Squarespace website.
2. The submission is:
    - Stored temporarily within Squarespace; and
    - Transmitted securely to Zapier via encrypted API connections.
3. Zapier automates the email replies for form submission.
4. In parallel, Google Drive is linked to Squarespace to be used for program administration, reporting, and follow-up communications.

No data is sold, shared for advertising, or used for automated decision-making.

3. Data Collected
The website collects limited, non-sensitive personal information, which may include:

- Name
- Email address
- Organization (if provided)
- Message or inquiry content
- Technical metadata (e.g., IP address, browser type)

The site does not collect:

- Financial or payment data
- Government-issued identifiers
- Health or medical information
- Login credentials or passwords

4. Security Controls

a. Data in Transit

- All data transfers between:
    - User ↔ Squarespace
    - Squarespace ↔ Zapier
    - Zapier ↔ Google Drive
      are encrypted using HTTPS / TLS encryption.

b. Squarespace Security

- Site-wide SSL encryption
- Firewalls and intrusion detection
- Platform-level security monitoring
- Role-based access for site administrators
    - The site administrator is Rocky Singh (rsingh@thirdrockconsulting.ca)

c. Zapier Security

- Zapier acts as a data processor, facilitating automation between platforms.
- Key safeguards include:
    - Encrypted data transmission
    - Restricted access to automation workflows
    - SOC 2–aligned security controls
- Zapier only processes data as instructed and does not retain it beyond what is necessary for automation and logging.

d. Google Drive / Google Sheets Security

- Form submissions are stored in a spreadsheet hosted on Google Drive.
- Security features include:
    - Encryption at rest and in transit
    - Role-based access controls
    - Account-level protections (e.g., MFA where enabled)
- Access to the spreadsheet is restricted to authorized personnel only for administrative and reporting purposes.
    - The authorized person is Leigh Kras (leigh.sdf@ame-ont.com)

5. Data Storage & Residency

- Data may be stored or processed in multiple jurisdictions, including:
    - United States
    - Other countries where Squarespace, Zapier, or Google operate infrastructure
- Data residency is not user-selectable and is dependent on vendor infrastructure.

Privacy implication:
Personal information may be subject to the laws of the jurisdictions in which it is stored or processed.

6. Data Retention & Management

- Personal information is retained only as long as necessary to:
  - Support program outreach
  - Respond to inquiries
  - Meet administrative and reporting requirements
- Data can be:
  - Deleted from Squarespace
  - Removed from Google Drive spreadsheets
- No automated profiling, scoring, or eligibility decisions are made based on website data.

7. Third-Party Service Providers

The website relies on the following third-party service providers:

Provider	Role
Squarespace	Website hosting and form collection
Zapier	Secure automation and data transfer
Google	Secure cloud-based spreadsheet storage

All providers:

- Use industry-standard security practices
- Act as data processors
- Are contractually bound by privacy and security obligations

8. Compliance Alignment

The overall setup aligns with:

- PIPEDA principles (limited collection, safeguards, purpose limitation)
- Reasonable security expectations for a public-facing, non-sensitive website
- Common SaaS-based administrative workflows used by educational and workforce development organizations

9. Suggested Privacy Policy Language

You may include language such as:

“Personal information submitted through the AMESDF Project website may be processed using third-party service providers, including Squarespace (website hosting), Zapier (automation), and Google (cloud-based document storage). These service providers may store or process information outside of Canada. Reasonable administrative, technical, and physical safeguards are used to protect personal information from unauthorized access, use, or disclosure.”

10. Risk Summary for the Board

- Low to moderate risk, appropriate for the nature of data collected
- No sensitive personal information involved
- Strong encryption and access controls
- Transparent use of reputable third-party platforms
- Risks are mitigated through limited data collection and restricted access

Aircraft Maintenance Engineers Association of Ontario (AMEAO)

Privacy and Security Standard of Conduct

Appendix D
Sharing information with Third Parties for Marketing Purposes

Original: 19 April 2026

Sharing information with Third Parties for Marketing Purposes

From time to time, AMEAO may partner with organizations that may wish to contact our Members to offer value-added benefits. AMEAO will only release such information as is necessary to fulfill the benefit obligations/requirements. Information shared may consist of First Name, Last Name, Email Address, Mailing Address, and/or Phone Number. Additional information on Third Party partners is provided below.

Entente Education Canada

As a member benefit, the Association will supply First Name, Last Name, Email Address, and registered Region to Entente Education Canada for the purpose of providing information to our members regarding their Group Benefits program.

The Association has signed a confidentiality agreement with Entente requiring them to keep this list confidential and to ensure that this subscription list is not used to solicit or advertise to the members.

The following is an excerpt from the Privacy Policy of the Supplier (Entente Education Canada):

7.0.3 Entente will maintain strict confidentiality of the personal data provided and collected and will use collected data based on Entente's privacy policy, and the following items, unless agreed upon otherwise:
- The use of member data is limited strictly to administering the member benefits
- Appropriate safeguards are in place to protect the information
- Data will never be sold or used for any secondary purposes
- All applicable privacy laws are being respected

8.0 Communication with Members of the Participating Group
8.0.1 Entente will communicate directly only with Participants of the Program, unless the Participating Group requests additional assistance to communicate with all Group members.

This Agreement and each party's obligations shall be binding on the representatives, assigns and successors of such party. Each party has signed this Agreement through its authorized representative.