

Information Security Policy

STANDARDS AND PROCEDURES FOR
SAFEGUARDING CUSTOMER INFORMATION

UPDATED Mar 5, 2019

1. Document History

Date	Version	Change	Section/Page	Approved / Effective
4/2015	1	Creation	All	4/30/2015
1/2017	2	Update	Sections 3, 5.1, 5.2, 6.1, 7, 7.4, 7.5, 8, 8.1, 11.1	1/20/2017
3/31/2017	3	Update	9.2, 11	4/10/2017
5/16/2017	4	Update	7.1, 7.7	5/17/2017
3/12/2018	5	Add	Section 6.2	3/12/2018
3/5/2019	6	Update	Section 12.2	3/6/2019

2. Overview

This policy defines the measures that AIM and its associates take to protect sensitive customer information from unauthorized access. It includes technical measures, such as using encryption and strong passwords, as well as process controls for limiting access to private information.

3. Scope

This policy applies to all employees of the AIM institute and all contractors, workforce members, vendors and agents using AIM Institute-owned hardware or with access to AIM Institute network resources, and other individuals who have access to or may be reasonably expected to come into contact with AIM Customer Private Information.

4. Customer Private Information

Customer Private Information (CPI) includes any trade secrets, future business plans, or product development information created by a customer in AIM Institute software, or otherwise communicated to AIM Institute or one of its contractors, workforce members, vendors or agents.

5. Access Control

5.1 Granting Access

Access to CPI will be granted on a need-to-know basis, to personnel directly involved in serving the customer. AIM will maintain a list of employees and direct contractors granted access to each customer's CPI. Contactor organizations will maintain a list of their employees and contractors granted access to each customer's CPI, and provide that list to AIM on request.

5.2 Revoking Access

Access to systems containing CPI will be revoked when the person no longer requires access to CPI, or on termination of the person's relationship with AIM or its contractor. If the CPI is stored on a personal system, such as a coach's PC or laptop, the person controlling the system must

certify in writing to AIM that all copies of CPI have been destroyed. At the termination of a business relationship between AIM and a customer, AIM will notify the customer in writing of the intent to destroy any of the customer's CPI that remains in AIM's possession at the end of a 30-day response period. If the response period elapses without a request from the customer to retain the CPI, AIM will destroy the CPI.

6. Communication of CPI

6.1 Unencrypted communication

CPI shall not be shared over unencrypted communications, such as email. If an AIM employee or contractor receives CPI from a customer via unencrypted communications, that person shall delete the CPI from their device(s). If a response to the original communication requires CPI, the AIM person shall respond via a secured channel, such as secure file drop, or in person. If the response does not require CPI, the AIM person shall delete the CPI from the response.

6.2 Use of cloud-based file sharing services

The AIM Institute provides a secure means of file-sharing in the Client Center all learners receive access to. Use of other file sharing services such as Google Drive, Microsoft OneDrive, Dropbox or SugarSync to share CPI with customers is permitted, with the following conditions:

- **Use only approved cloud services.** Use of a service must be approved in writing by both customer and AIM. This approval may carry additional conditions for use.
- **Share only necessary information.** Share the minimum amount of information required to complete specific tasks
- **Share only with specific individuals.** Files should be shared only with specific individuals from the customer, using their work accounts. Never share files with "public" permissions or than "anyone" can view.
- **Review shared files and folders monthly.** Revoke access when no longer required.
- **Sync files only with laptops and devices that are subject to AIM security regulation.**

7. PC Security Standards

Except where noted, standards in this section apply to desktops, laptops and other personal systems used by AIM employees and contractors, regardless of whether or not these systems store CPI.

7.1 Password Protection

All systems must require users to authenticate individually, with a password unique to each user account. Two-factor authentication is highly encouraged. Passwords must conform to the standards set forth in the 10. Password [Standards](#) section below. Biometric security, such as fingerprint scanners, may be used to supplement system passwords or as the second factor in two-factor authentication.

7.2 Screen lock

All systems must lock the screen after no more than 15 minutes of idle time, and require the user to enter his/her password to unlock the screen.

7.3 Virus Scanning

All systems must have virus/malware scanning software installed and configured to run a scan at least weekly. Virus definition files must be updated at least monthly.

7.4 Removable Media

AIM employees and contractors shall not store CPI on thumb drives, CD-ROMs, memory cards, or other removable media.

7.5 No Unencrypted Storage

No CPI shall be stored on an unencrypted hard drive or other fixed storage device. Coach laptops and other devices that can be reasonably expected to store CPI, even inadvertently, must have their hard drives encrypted with a FIPS 140-2 compliant cryptography module. Microsoft BitLocker and Apple FileVault meet this standard.

7.6 Operating System Security Updates

All systems shall be configured to automatically install security updates on a weekly basis. These updates may be controlled by a corporate update server at AIM or one of its related entities.

7.7 Disposal

Storage devices owned by AIM that have contained CPI must be physically destroyed or erased with a utility that writes random data to all sectors of the drive, such as Blancco Drive Eraser.

Contractors who supply their own equipment to provide services on behalf of AIM must certify in writing the following when the equipment is retired from AIM use but retained by the contractor for other purposes:

- All copies of AIM files have been deleted
- All AIM applications have been removed
- All AIM-related email, calendar, and contact accounts have been removed
- Free disk space has been securely erased using BleachBit or another secure erasure utility

When the contractor equipment is sold, transferred to another person, recycled, or otherwise leaves the control of the contractor, storage devices attached to the equipment must be securely erased with a utility such as Blancco Drive Eraser.

8. Mobile Device Security Standards

Standards in this section apply to smartphones, tables and other mobile devices used by AIM employees and contractors for official business, regardless of whether or not these systems store CPI.

8.1 Passcode and Encryption

All mobile devices must have encryption enabled and be protected with an alphanumeric or biometric passcode. Alphanumeric codes must be at least 6 digits in length. The mobile device must be configured to lock automatically after 15 minutes of inactivity, per section 7.2 above. Biometric passcodes such as Apple TouchID or Nexus Imprint are acceptable substitutes for an alphanumeric passcode.

9. Server Security

The standards in this section apply specifically to servers that store or process CPI.

9.1 Communications Encryption

All application communication between Blueprinter and Launchstar clients and servers shall use transport-layer security (TLS) to authenticate the server and encrypt communications. Servers shall be configured to conform to current best practices for encryption algorithms and key exchange protocols, with a minimum of 128-bit encryption applied.

9.2 Limited Access

All servers that store or process CPI shall be protected by network firewalls or other appliances to prevent access to the servers on unauthorized ports and/or from unauthorized network addresses.

Administrative access to servers via secure shell (SSH) or remote desktop (RDP) shall be permitted only from specifically allowed network addresses. Only users with a specific need for access to the AIM server environment shall have access. Each user shall have an individual named account, and access to the production environment shall be logged.

9.3 Security Scans

Servers that store or process CPI shall be scanned at least once a quarter for known network security vulnerabilities. The scan shall be performed by an independent vendor. High risk vulnerabilities (as determined by the OWASP Risk Rating Methodology or NVC Common Vulnerability Scoring System) found in the scan will be remediated within 7 days of detection.

10. Password Standards

10.1 Password construction guidelines

All systems that store or process CPI shall require their user accounts to have passwords that meet the following restrictions:

- Contain at least eight (8) characters
- Contain both upper and lower case letters (A-Za-z)
- Contain at least one numeral (0-9)

Where possible, this policy will be enforced by system configuration.

10.2 Password rotation

Users shall be required to change their passwords at least every three months. Where possible, this policy will be enforced by system configuration.

10.3 Password protection

Passwords shall not be shared, even among authorized users. Passwords shall not be written down or inserted into electronic communication, such as email. Passwords may be stored encrypted in a vault application, but not stored in unencrypted electronic files.

11. Vendor Management

11.1 Vendor Management Policy

AIM maintains a Vendor Management Policy covering vendors whose services pertain to the delivery of systems containing CPI. This policy ensures that AIM retains proper oversight of activities that support the safeguarding of CPI.

12. Breach

12.1 Definition


Breach is defined as the access or disclosure of unsecured CPI to an unauthorized party. Breaches could include an unencrypted email containing CPI sent to an unintended recipient who is not authorized access to the CPI, or compromise of a server by a malicious third party.

12.2 Notification

Employees of the AIM institute and all contractors, workforce members, vendors and agents must report a breach to the AIM Information Security Officer within 24 hours of learning of a breach. The AIM Security Officer will notify affected customer(s) within 3 days of the initial report (or sooner if required by customer agreement), informing the customers of what information was compromised, how it was compromised and steps taken to secure the breach.

*The AIM Institute
2206 20th Street
Cuyahoga Falls, OH 44223*

 info@theaiminstitute.com

 @aim-institute