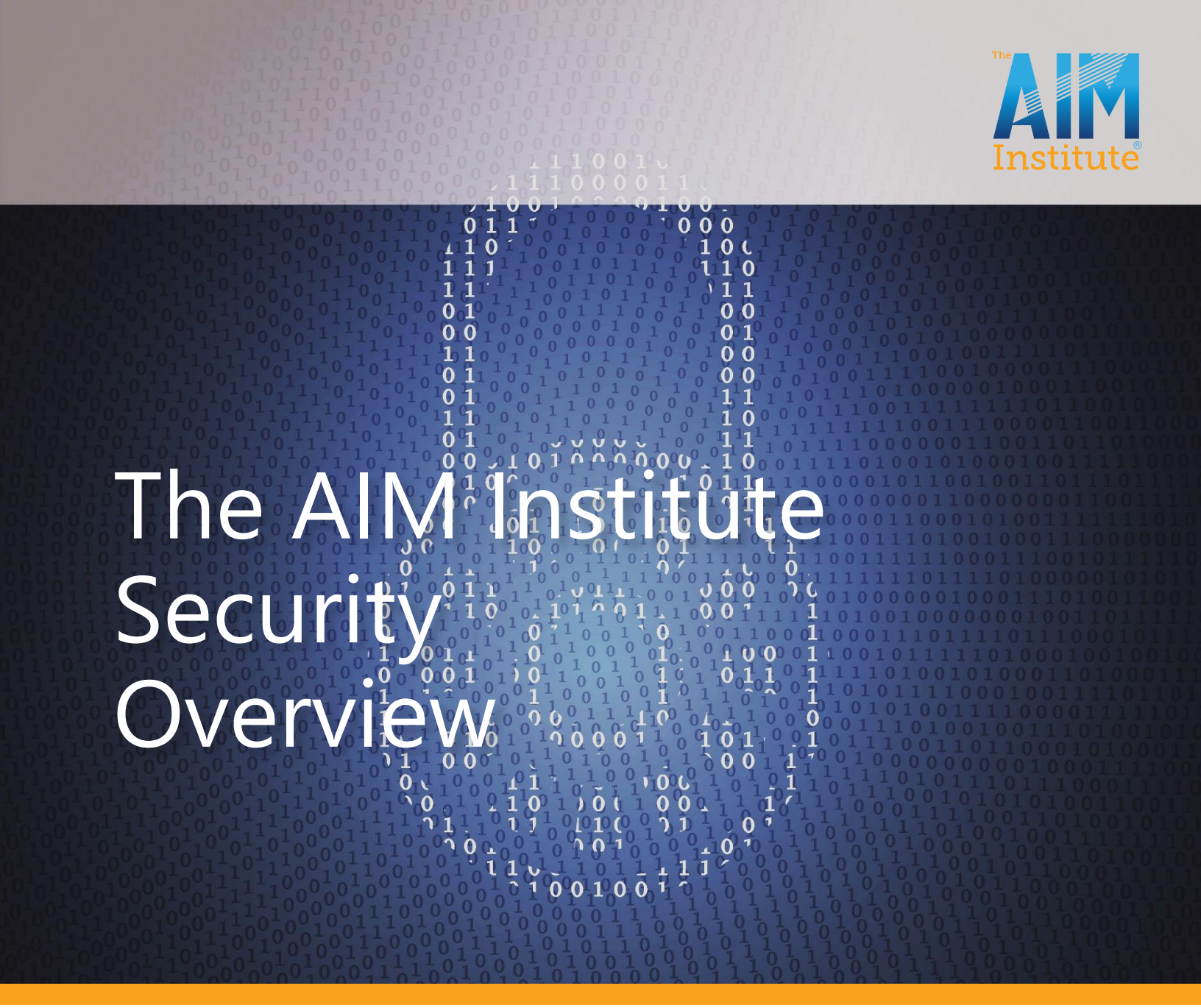


The AIM Institute Security Overview

HOW AIM PROTECTS YOUR INFORMATION

UPDATED January 2, 2018

Introduction

The AIM Institute applications, LaunchStar® and Blueprinter® software, guide organizations through the process of identifying market needs, defining new products, and bringing them to market. Customers trust AIM with their confidential business plans, and AIM understands the sensitive nature of the information that customers store in the applications. This paper describes the measures that AIM takes to safeguard that data against accidental or intentional unauthorized access. The Software Security section contains information about features in the applications that protect information at rest and in transit. The Facility Security section describes the measures implemented by AIM's hosting partner to provide a secure cloud platform. Finally, the Process Safeguards section discusses the business practices AIM implements to ensure that all employees and contractors take appropriate measures to ensure the privacy of customer information.

Certifications

AIM successfully completed a SOC 2 Type 2 evaluation for the April – September 2017 period. A copy of the report is available on request.

System Security

Browser Security

Blueprinter 5.0 is delivered via browser. The connection to the Blueprinter application server is protected by Transport Layer Security (TLS) using a 2048-bit key. TLS 1.2 is the preferred protocol, with modern cipher suites supported for session key exchange. Blueprinter uses browser local storage on the customer's PC to store project information. This information is protected by the user's Windows login credentials and any other safeguards that may be present on the user's PC, such as full-disk encryption.

Integrity of the LaunchStar Executable

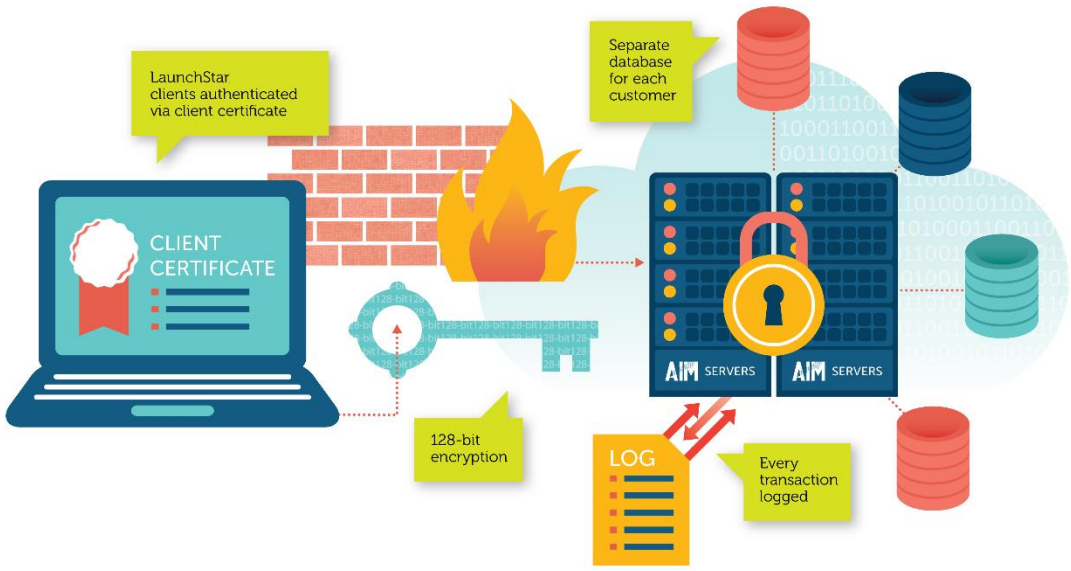
The LaunchStar 3.0 executable is digitally signed by AIM to ensure that the program has not been altered. Windows verifies this signature every time the application runs. This avoids the risk of a third party altering the executable to perform unauthorized operations. The client software is downloaded directly from the AIM website and authenticated with AIM's server certificate, providing further assurance that the software is genuine.

Least Privilege

LaunchStar does not require administrative privileges for installation or operation. This prevents the program from changing system configuration.

Client Authentication

LaunchStar clients authenticate to the server using X.509 v3 certificates. The first time the client runs, it generates a certificate and sends it to the server, along with the user's activation code and email address. The server verifies the activation code, signs the certificate, and returns it to the client. This client certificate is then used to authorize every API call to the server. The certificate is associated with a specific user, so the authenticated client is permitted to access only information associated with the user's customer.



The certificate is stored in the user's Windows Certificate store and protected by the user's Windows login credentials. This prevents unauthorized access to the authentication credentials and ensures that the requests are coming from the PC where the software was originally installed. It also avoids the need for a separate application user password that can be compromised.

Communications Security

Communications between the client and the server is encrypted using Transport Layer Security (TLS). TLS authenticates both the client and the server, and encrypts all communications between the two parties. Communications are encrypted with a strong cipher using a minimum 128-bit key length. This prevents third parties from intercepting communications.

Customer Data Segregation

Each customer's data is stored in a separate database. Application user access is restricted to a specified customer, so that a user may never gain access to another company's data.

Audit Logs

The application retains a complete audit log of changes to company information. Each save of the document is attributed to the user who performed the save. This enables a review of changes to determine who made a particular change, and at what time the change was made.

Network Security

The application servers are protected by network firewalls whose rules restrict access. Administrative access is granted only to known network addresses, and ports not in use by application services are blocked entirely. Network security scans are performed on a quarterly basis by an independent vendor. Any high-risk vulnerabilities identified by the scans are resolved within 7 days of detection.

Facility Security

AIM hosts the LaunchStar and Blueprinter applications in the Microsoft Azure cloud environment. Microsoft participates in a number of compliance programs to ensure that its data centers provide a secure and reliable infrastructure for enterprise applications. These compliance programs involve independent verification of requirements by outside auditors. Selected accreditations are detailed below. A full list of accreditations is available at http:// azure.microsoft.com/en-us/support/trust-center/ compliance/.

SOC 1 Type 2

The Service Organization Control (SOC) 1 report represents an audit of the organization's internal controls over financial reporting. The Type 2 reports examine policies and procedures for financial reporting, as well as an audit of the effectiveness of the controls defined by those policies. This audit is performed annually, in accordance with the Statement on Standards for Attestation Engagements (SSAE) No. 16 of the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402 put forth by the International Auditing and Assurance Standards Board (IAASB).

SOC 2 Type 2

The SOC 2 report covers controls relevant to the security, availability, processing integrity, confidentiality and privacy of data and services provided by Azure. The Type 2 report requires attestation of the organizational controls as well as an audit of the effectiveness of the controls. As with the SOC 1 Type 2 report, the audit is performed in accordance with SSAE 16 and ISAE 3402.

ISO 27001/27002

Azure is compliant with ISO 27001:2013 and ISO 27002:2013, which set forth controls in nineteen areas, including information security, human resources, and physical and environmental security. Azure also implements ISO 27018, which adds standards for the use, protection and disposal of personal information in a cloud environment.

Cloud Security Alliance Cloud Controls Matrix (CSA CCM)

The Cloud Security Alliance Cloud Controls Matrix provides a set of security guidelines for cloud providers. The CSA publishes the Security, Trust and Assurance Registry, a publicly accessible repository of security control reports provided by CSA members. Microsoft Azure is listed at the “self-assessment” level of CCM compliance.

Process Safeguards

Information Security

All AIM employees and contractors are required to adhere to the AIM Information Security Policy. This policy defines what constitutes customer private information and sets forth standards for securing PCs and servers that are used to process customer information. It also specifies encryption of customer data at rest and in transit. The Information Security Policy is reviewed and updated on a quarterly basis.

Access Grant and Revocation

Access to AIM applications is granted by request to an AIM administrator from a known customer representative. After validating the request, the administrator generates an activation code and sends it via email to the new user. A unique password for the download area is sent to the user via a separate channel.

An administrator may also revoke access for an individual user. The revoked user’s software will operate normally until the next time the user attempts to connect to the application server. At that time, the server will respond with a message that disables the client software.

Business Continuity

The AIM Business Continuity Plan provides guidance for continuing operations in the event of loss of key facilities or personnel. It lists important business contacts and locations for critical information and services, as well as who will assume business functions in the event an employee is not available. Key AIM suppliers are also required to maintain business continuity and disaster recovery plans, ensuring that AIM operations will continue in the presence of adverse events.

The AIM Institute
2206 20th Street
Cuyahoga Falls, OH 44223
info@theaiminstitute.com