Analog Informatics™ Corporation

Product Security Plan

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

analoginfo.com

Analog Informatics Corporation (AIC)

Field	Value
Version	1.7
Date	28 October 2026
Applies to	AIC Server, AIC Agent, and the configurators and installers shipped with them
Owner	Analog Informatics Corporation
Security contact	support@analoginfo.com
Review	At least once a year, and whenever a release changes how the product protects data

1. Purpose and Scope

This plan describes how Analog Informatics Corporation builds, ships, and maintains secure software, and how anyone can report a security problem in that software.

AIC offers AIC Enterprise Privilege Suite™ and AIC CMMC Complete™ in three hosting models: customer on premises, customer-run software on commercial Infrastructure as a Service, and an authorized application under a third-party FedRAMP or GCC cloud. AIC is not the Cloud Service Provider and not a Managed Service Provider.

In the customer-operated models, customers install and run AIC software in their own environments, including air-gapped sites. AIC does not operate those deployments, does not host their data, and has no standing access to their running systems. In the authorized-application model, the cloud provider remains the CSP and holds the authorization; shared duties are written in the engagement CRM alongside the cloud provider's CRM. See Shared responsibility.

This plan covers the software AIC ships. It is not a System Security Plan (SSP) for a customer's environment. Customers who need an SSP for their own system can start from the System Security Plan template in the AIC Cybersecurity Maturity Model Certification (CMMC) Level 2 enclave kit.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Each item below carries one status:

Status	Meaning
Available now	In the current release
Partial	In the current release with a stated limit
Planned	Not in the current release

2. Methodology and Framework Alignment

AIC follows a security by design methodology. Security requirements are part of the design of each feature, not added after it is built.

The secure development practices in section 3 follow the four practice groups of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-218, Secure Software Development Framework (SSDF) Version 1.1. SSDF is the basis of the Cybersecurity and Infrastructure Security Agency (CISA) Secure Software Development Attestation Form used for federal software purchases.

SSDF Group	Topic	Section
Prepare the Organization (PO)	Security requirements, roles, and tools	3.1
Protect the Software (PS)	Source code, release integrity, and provenance	3.2
Produce Well-Secured Software (PW)	Design, coding, and testing	3.3 and 3.4
Respond to Vulnerabilities (RV)	Finding, fixing, and disclosing problems	3.5 and 6

Vulnerability disclosure in section 6 follows International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standards ISO/IEC 29147 (vulnerability disclosure) and ISO/IEC 30111 (vulnerability handling). The machine-readable contact file follows Request for Comments (RFC) 9116.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

3. Secure Development

3.1 Prepare the Organization

Practice	Status
Security requirements are set by the NIST SP 800-53 Revision 5 moderate baseline. Security features are designed to that baseline, not to a smaller checklist	Available now
Revised Section 508 of the Rehabilitation Act is a release requirement for every user interface. See the Accessibility Conformance Report	Available now
Written engineering rules cover error handling, audit logging, cryptography, configuration storage, and test isolation	Available now

3.2 Protect the Software

Practice	Status
Source code is kept in access-controlled repositories with full change history	Available now
Production releases are digitally signed with Authenticode under AIC's code signing agreement with SSL.com	Available now
Each release publishes a SHA-256 checksum manifest of every shipped file, so a customer can confirm a download is unchanged	Available now
Each installer includes a Software Bill of Materials (SBOM) in CycloneDX 1.5 format for each shipped program, listing every third-party component and version	Available now
The product discloses every open source component and its license text in the product, regenerated from the build's dependency lock files	Available now

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Alpha, beta, and internal test builds are not always signed. These builds are tightly controlled and are never made available to the public.

3.3 Design Requirements

Every application programming interface (API) is designed to meet these requirements:

- **Authenticated.** No API accepts an unauthenticated request to read or change protected data.
- **Authorized.** Role-Based Access Control (RBAC) decides what each authenticated caller may do.
- **Rate limited.** Request rates are limited to resist abuse and denial of service.
- **Error limited.** Repeated failures, such as failed sign-in attempts, trigger lockout.
- **Alerting.** Security-relevant events raise alerts.
- **Routed to the customer.** Specific alerts can be routed to the customer's own event sinks, Security Information and Event Management (SIEM) systems, and trouble-ticket systems.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

3.4 Produce Well-secured Software

Practice	Status
Core components are written in Rust, a memory-safe programming language	Available now
A no-panic rule: code must handle unexpected input and errors without crashing the service, log the failure, and recover. Compiler lint rules enforce it	Partial. Lint rules enforced in core components; being extended to all components
Database access uses parameterized queries	Available now
Passwords are stored as PBKDF2-HMAC-SHA-256 hashes with 600,000 iterations and a random salt, per NIST SP 800-132	Available now
Secrets at rest are encrypted under keys held in software or in a customer Hardware Security Module (HSM) through PKCS#11. Each encrypted record names the key that protects it, so keys can be rotated	Available now
Security-relevant actions are written to the Windows Event Log and can be forwarded as syslog (RFC 5424) to the customer's SIEM	Available now
Automated unit, integration, and browser tests run against built software before release	Available now
Penetration testing: automated testing in which multiple artificial intelligence (AI) models attack the software and repair what they find, plus manual testing by internal testers with Burp Suite and other industry tools	Available now
Third-party components are checked against published Common Vulnerabilities and Exposures (CVE) records and security advisories, using the SBOM	Available now
AI-assisted development: AIC developers use AI tools to write and test code. A human developer inspects all AI-generated code to confirm its functionality and that it matches the developer's intent before it is accepted. This review is part of the code review practice in SSDF practice PW.7	Available now

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

3.5 Respond to Vulnerabilities

Practice	Status
A public channel to report vulnerabilities (section 6)	Available now
A security advisory feed with an AIC identifier (AIC-SA-year-number), severity, affected versions, and fixed versions for each issue. The feed is readable in the product and through the administrator API	Available now
Root-cause review of each confirmed vulnerability, to find and fix the same class of problem elsewhere in the code	Available now

4. Cryptography

Federal Information Processing Standards (FIPS) 140-3 is the federal standard for cryptographic modules. The NIST Cryptographic Module Validation Program (CMVP) validates modules against it.

AIC does not represent its software as certified or validated. AIC shares the FIPS certificate of each cryptographic library or device the software uses or supports. A module validation applies to the module, not to an entire program.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Component	Cryptographic Module	Status
AIC Server and configurators	AWS-LC, the default cryptographic library, which holds a FIPS 140-3 certificate. AIC provides the certificate for the module version in each release on request	Available now
AIC Agent and elevation helpers	The operating system's cryptographic module (Windows Cryptography API: Next Generation, Apple corecrypto, or the Linux distribution's FIPS provider where the distribution ships one). Validation follows the operating system vendor's certificate	Available now
Hardware security modules (HSMs) and key management services (KMS)	Optional. A customer HSM or KMS used through PKCS#11 carries its own FIPS certification	Available now

The non-FIPS ring cryptographic library has been removed from the code.

It is the customer's responsibility to confirm the FIPS certification of any device or service the software uses under the customer's configuration, such as an HSM or a KMS.

5. Data Handling and Product Control

5.1 Customer Data

• AIC software runs in the customer's environment. Customer data, credentials, session recordings, and audit records stay in that environment.

In customer-operated models 1 and 2, AIC does not operate customer deployments and has no standing access to them. Duties for model 3 are assigned in the engagement CRM.

• When a customer asks for support, the customer decides what information to share. AIC uses it only to resolve that request.

• Air-gapped sites can install, license, and update the software without a network connection to AIC.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

5.2 Data Exchanged with AIC

No data is transmitted between a customer deployment and AIC except for billing and license compliance:

- **Azure Marketplace deployments:** the configuration and usage data that Microsoft Azure Marketplace provides for billing.
- **On-premises deployments:** license activation, either online or air-gapped.

Customer data, credentials, session recordings, and audit records are not sent to AIC. Connections that the customer configures to its own systems or to third-party services go to those destinations, not to AIC.

5.3 Updates, Backups, and Remote Access

AIC software does not update itself. The software is under the customer's direct control, so the customer decides when to install updates and when to run backups. AIC has no backdoor, remote control, or remote access to customer deployments.

5.4 No AI in the Product

AIC software contains no large language model (LLM). It uses heuristics: fixed rules and workflows that the customer configures. Nothing in the product acts autonomously or uses AI judgment independent of the customer's configuration. This is by design.

6. Vulnerability Disclosure Policy

6.1 How to Report

Email **support@analoginfo.com** with "Security" in the subject line. Please include:

- The product and version
- A description of the problem and its security impact
- Steps to reproduce it, with any proof-of-concept code
- How you would like to be credited, if at all

Do not include customer data or personal information in a report.

6.2 What Happens Next

AIC usually responds within 24 hours of a report, and fixes are generally released within 72 hours of a confirmed vulnerability. The commitments below are the outer limits.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Step	Commitment
Acknowledge receipt	Within 3 business days
Initial assessment and severity	Within 10 business days
Status updates	At least every 30 days until resolved
Fix and advisory	A fixed release and a published advisory. AIC requests a CVE identifier when the issue qualifies
Credit	Reporters are credited in the advisory unless they ask not to be

AIC asks reporters to allow up to 90 days from acknowledgment before public disclosure, and will agree a different date with the reporter when a fix needs more time or is ready sooner.

6.3 Scope

In scope: AIC Server, AIC Agent, and the configurators and installers AIC ships, in versions AIC currently supports.

Out of scope: customer deployments you are not authorized to test, denial-of-service testing, social engineering, physical attacks, and third-party services.

6.4 Good-faith Research

AIC will not pursue legal action against anyone who, in good faith:

- Tests only systems they own or are authorized to test
- Avoids privacy violations, data destruction, and service disruption
- Reports the problem to AIC promptly and does not exploit it beyond what is needed to show it exists
- Gives AIC reasonable time to fix the problem before public disclosure

7. Customer Notification

When AIC confirms a vulnerability in shipped software, AIC:

1. Publishes an advisory in the product's advisory feed and on the AIC security page.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

2. Notifies customers through their support contact, with affected versions, severity, the fixed version, and any interim mitigation.

3. Publishes the fixed release with its checksum manifest and SBOM.

AIC may limit the technical detail in an advisory. Full detail can put at risk customers who have not yet applied the update. An advisory may also state that an issue does not apply to some deployments, such as air-gapped sites that are not exposed to a given threat by design.

8. Limitations and Layered Defense

This section is one of several disclosures in this plan about the limits of any software, including AIC software. AIC software is not perfect. Even if it were, it runs on other software that is expected to contain flaws AIC cannot fix.

8.1 AIC Software

All software has flaws. AIC tests rigorously for them, but AIC software includes commercial and open source libraries and tools that AIC does not control, and AIC cannot guarantee that its software is free of defects or vulnerabilities. AIC monitors CVE records for the components it ships and responds as quickly as is commercially reasonable.

8.2 AI Models That Find and Exploit Unknown Vulnerabilities

A zero-day vulnerability is a flaw that is unknown to the people who develop the software, so no fix exists when it is first exploited.

A new class of artificial intelligence (AI) model can find zero-day vulnerabilities in source code and in compiled programs, and can then write working exploits for them, often with little or no human direction. These models read and reason about code the way a skilled security researcher does, but at far greater speed and scale. They find flaws that conventional commercial testing tools do not, including static code analyzers, vulnerability scanners, fuzzers, and manual penetration testing.

Claude Mythos, a model from Anthropic announced in April 2026, is a published example. Anthropic reports that in its testing Mythos found and exploited zero-day vulnerabilities in every major operating system and every major web browser. Many of those flaws had gone undetected for 10 to 20 years in heavily reviewed code, and the oldest was a 27-year-old flaw in OpenBSD, an operating system known mainly for its security. Anthropic reports that the model found nearly all of these flaws, and wrote many of the related exploits, without human steering.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Anthropic restricts access to Mythos to vetted organizations that use it for defense, through a program called Project Glasswing. Anthropic also states that similar capabilities are likely to spread, including to people who will not use them responsibly. AIC plans on the assumption that attackers either have this capability now or will have it soon.

AIC therefore acknowledges that its software may contain zero-day vulnerabilities that AIC does not know about and cannot detect with the commercial testing tools available to it. These vulnerabilities can be exploited even after the most capable penetration testing and red team and blue team exercises available to the civilian sector.

8.3 Underlying Technology AIC Cannot Fix

AIC software depends on technology that AIC does not build and cannot change. That includes:

- Operating systems, such as Windows and Linux, and their kernels, drivers, and system libraries
- Networks, including routers, switches, firewalls, virtual private networks (VPNs), wireless equipment, and the protocols they carry
- Databases, such as PostgreSQL
- Identity management systems, such as directory services, identity providers (IdPs), and multi-factor authentication (MFA) services
- Hardware and firmware, including processors, hardware security modules (HSMs), and the hypervisors that run virtual machines
- Cloud and hosting services, when the customer runs AIC software on them

This technology is expected to contain flaws, including zero-day flaws of the kind described in section 8.2. A flaw in it can expose AIC software and the data AIC software protects, even when AIC software itself has no defect. AIC cannot fix these flaws from inside its own software. Their vendors and maintainers issue the fixes, and the customer applies them. Where AIC can reduce the impact, for example by changing a default setting or adding a check, AIC does so and publishes an advisory.

8.4 How AIC Responds

AIC will listen to its customers and work with them to resolve issues quickly. AIC prioritizes that work by customer needs and market realities. AIC also uses AI tools in

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

its own testing, as described in section 3.4, so that it finds more of these flaws before attackers do.

8.5 Layered Defense

Customers should not rely on any single product for protection. AIC recommends a layered defense alongside AIC software. That includes:

- Detection systems that watch for anomalous behavior
- Network segmentation, so that one compromised system does not expose the rest
- Prompt patching of operating systems, networks, databases, and identity systems
- Least privilege for every account, including the accounts AIC software uses

9. Defect Correction, Performance, and Liability

9.1 Defect Correction

AIC will make commercially reasonable efforts to fix all reported bugs, including security vulnerabilities, in a timely manner where possible.

9.2 Performance

AIC software will perform substantially in accordance with the specifications and representations made in AIC's published documentation and on AIC's website.

9.3 Limitation of Liability

To the fullest extent permitted by law, AIC is not liable for damages of any kind, except damages caused by AIC's gross negligence.

Vulnerabilities and flaws in AIC software, and in the technology described in section 8.3, do not constitute gross negligence.

9.4 Governing Terms

The Software License Terms govern the license, warranty, remedies, and liability for AIC software. If this plan and the Software License Terms differ, the Software License Terms control.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

10. Related Documents

Document	Where
Accessibility Conformance Report (Voluntary Product Accessibility Template (VPAT) 2.5Rev, Revised Section 508)	analoginfo.com/accessibility
Company registration status (System for Award Management (SAM.gov) and Commercial and Government Entity (CAGE) code)	analoginfo.com/about
Security contact file (RFC 9116)	analoginfo.com/.well-known/security.txt
System Security Plan template for customer environments	CMMC Level 2 enclave kit

11. Plan Maintenance

AIC reviews this plan at least once a year, and when a release changes a status in this plan. Each revision updates the version and date at the top.

For more information about Analog Informatics Corporation, please go to analoginfo.com.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.