DATA SHEET

AEGIS SOFTWARE

Confidence Built In:

How Aegis Software Handles Customer Data for **Regulated and Proprietary Manufacturing Environments**

Secure. Compliant. Trusted.

Security in manufacturing is multifaceted, spanning infrastructure, personnel, operations, and encryption. For manufacturers working in regulated or IP-sensitive industries, it's not just about technology. It's about who develops the software, where it's developed, who has access to data (and how), and whether those protections stand up to scrutiny under standards like ITAR, DFARS, and CMMC. This document outlines how Aegis combines enterprise-grade technology and secure operational practices to deliver trusted data protection at every touchpoint.

Security means different things to different organizations, but for manufacturers in regulated or IP-sensitive industries, it's more than just firewalls and passwords. Aegis Software protects customer data not only through technology, but through secure business operations, strict personnel access controls, and cloud infrastructure aligned with U.S. regulatory expectations. Whether FactoryLogix is deployed on-premises or in the cloud, Aegis enables confidence through proactive, verifiable safeguards.

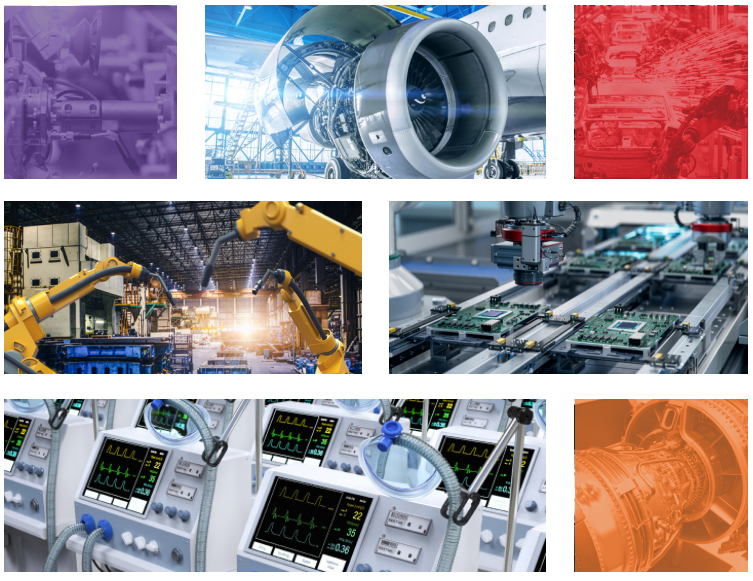
This protection is built on a holistic approach, one that incorporates administrative, technical, and procedural controls across all aspects of our operations. **These internal practices ensure that customer data is handled securely and in compliance with regulatory requirements during support interactions, cloud hosting, and internal system administration.**

Why Compliance Matters

Failure to meet regulatory obligations can result in serious consequences, including fines and penalties:

- **Loss of critical government contracts**
- **Reputational damage and legal consequences**
- **Criminal penalties for mishandled sensitive data**

Aegis' internal security and compliance practices help manufacturers meet regulatory requirements without compromising agility or support quality.



Protecting Customer Data Across the Lifecycle

Aegis Software recognizes that secure handling of customer data is essential, whether we are supporting contract manufacturers, OEMs, or manufacturers operating in highly regulated sectors. This includes organizations handling sensitive defense and aerospace information subject to export controls such as the International Traffic in Arms Regulations (ITAR), as well as those requiring rigorous protection of proprietary and operational data. Our internal practices are designed to align with data protection requirements, deployment models, and regulatory obligations.

Security Is More Than Just Technology

For manufacturers operating in regulated or IP-sensitive environments, true protection goes beyond firewalls and encryption. The operational controls and internal practices of your software provider are just as critical as the technology itself. The following sections outline how Aegis safeguards your data through both secure deployment models and disciplined internal procedures.

On-Premises Operational Controls

- Aegis requests only the minimum data required for effective support.
- Data shared for support purposes is transferred via secure upload portals and handled within isolated, access-controlled networks.
- For ITAR-regulated customers, any data shared with Aegis is accessed only by U.S. persons with verified clearance.
- After issue resolution, all data is securely deleted from Aegis systems, no backups or residual storage.

SaaS (Software-as-a-Service) Security Controls

- FactoryLogix Online is deployed in Microsoft Azure's commercial cloud or Microsoft Azure Government Cloud for ITAR-regulated customers.
- Access by Aegis personnel to cloud environments is protected by multifactor authentication, alongside access governance and continuous monitoring.
- Aegis applies role-based access control to its administrative and support functions, ensuring least privilege principles are upheld.
- Temporary data copies used for diagnostics are promptly removed after resolution.
- Aegis Software's employee access to cloud customer environments is logged and regularly audited.

Security Framework for ITAR and Non-ITAR Customers

Aegis differentiates its internal handling processes based on customer classification:

Non-ITAR Customers (SaaS or On-Premises)

- **All customer data is treated as confidential and proprietary.**
- **Interactions are supported through secure upload platforms** and remote diagnostic tools.
- **For SaaS customers, data is hosted in Microsoft Azure commercial regions,** with access restrictions based on job role and region.

ITAR Customers (SaaS or On-Premises)

- **All customer data, whether proprietary, regulated, or export-controlled, is treated as confidential** and protected under strict access and handling procedures.
- **Customers are identified during onboarding** for ITAR-specific operational handling to ensure appropriate internal safeguards are applied.
- **All ITAR SaaS data resides in Microsoft Azure Government Cloud**, with protections aligned to federal requirements.
- **For on-premises ITAR data, customers upload files to a dedicated and secure upload site** hosted in Microsoft Azure Government Cloud, protected by named login credentials, AES 256-bit encryption for stored files, and TLS 2.0 for in-transit transfers using private/public key encryption. Access to uploaded data is limited to authorized U.S. persons at Aegis.
- **Only verified U.S. citizens may access systems or data** flagged as ITAR-regulated.
- **Aegis' use of Microsoft Azure Government Cloud ensures compliance** with Microsoft's commitments to U.S.-only data residency and personnel access, as required for ITAR environments.

How Aegis Protects Customer Data

- **Verified U.S. citizen-only access** for ITAR environments.
- **Customer data is securely handled within Microsoft Azure** or Microsoft Azure Government Cloud environments, depending on regulatory requirements.
- **Continuous vulnerability scanning and endpoint protection** across Aegis' infrastructure.
- **Denied entity screening** embedded in Aegis' internal support and commercial operations to prevent engagement with restricted parties.
- **Mandatory security awareness training** and policy acknowledgment for all Aegis personnel with access to customer data.
- **TLS-encrypted upload portals and secure file transfer mechanisms** that ensure customer data is transmitted privately and protected from unauthorized access during support engagements.
- **Enforced data retention limits** and permanent deletion policies.
- **Internal documentation and access logging** within Aegis to support audit readiness and demonstrate compliance with internal procedures.
- **Defined incident response plan** to contain, resolve, and report any potential security incidents in a timely and compliant manner.

Why Manufacturers Trust Aegis

- **No Contractor Development** – All software development is performed exclusively by Aegis employees, no third-party contractors are used.
- **DFARS-Compliant Operating Footprint** – Aegis develops and delivers solutions solely from DFARS-compliant nations.
- **Enterprise-Wide Cyber Protections** – Advanced threat detection and telemetry monitoring are applied across all of our internal systems and infrastructure.
- **Integrated Protections** – Security and compliance are embedded in how Aegis manages all cloud and on-premises environments, not just during support.
- **Operational Transparency** – Controls aligned to ITAR and export compliance best practices.
- **CMMC Level 1 Certified** – Aegis has achieved Cybersecurity Maturity Model Certification (CMMC) Level 1, demonstrating compliance with foundational cybersecurity practices essential for safeguarding Federal Contract Information (FCI). Aegis is also on the path to achieving CMMC Level 2 certification, reinforcing our ongoing efforts to strengthen and evolve our security practices in line with defense industry expectations.
- **Dedicated U.S.-Based Compliance Handling** – All ITAR data is processed only by U.S. personnel.
- **Data Confidentiality Culture** – Aegis does not reuse or disclose customer data.
- **Experience Across Sectors** – Supporting compliance-sensitive industries for over 25 years.

Secure by Design. Compliant by Commitment.

As manufacturing becomes more connected and regulated, safeguarding sensitive data is more than a support function; it's a core operational imperative. Aegis Software ensures that your FactoryLogix environment and every interaction around it are protected by design.

Contact us to learn how Aegis protects what matters most: your data, operations, and reputation.

AEGIS SOFTWARE

www.aiscorp.com/contact-us