AXION

SECURITY · RELIABILITY · ENGINEERING GOVERNANCE

Axion Security & Reliability Overview

A transparent control overview for engineering, IT, security, procurement and quality teams.

VERSION	1.1
REVIEWED	26 August 2026
CLASSIFICATION	Public customer information
CONTACT	support@ax-i-on.com

ASSURANCE BOUNDARY	This overview describes implemented controls and remaining evidence. It is not an ISO/IEC 27001 certificate, IEC 62443 certificate, SOC 2 report, penetration-test report, GMP validation package or contractual SLA.

01 · EXECUTIVE OVERVIEW

Security is a system, not a feature.

Axion applies layered application, data, delivery and operational controls to protect customer engineering work. The platform uses signed time-bounded sessions, shared session revocation, recent-authentication gates for sensitive actions, authenticated project ownership, backend-only data access, private pre-storage upload inspection, connector target restrictions, tamper-evident security-event chaining, secure browser headers, abuse protection, change history, health probes, dependency isolation, backups and automated release gates. This document distinguishes implemented product controls from deployment configuration and external assurance.

Operating principles

- Least privilege and private-by-default customer data
- Secure defaults with explicit activation of external integrations and OT writes
- Traceable engineering changes, sources, versions and approvals
- Finite failure behavior, observable health and recoverable state
- Transparent limitations instead of unsupported compliance claims

Trust boundaries

BOUNDARY	PROTECTION
Browser to Axion	HTTPS, HSTS, strict-origin sessions, CSP, origin and Fetch Metadata checks
Axion API to data	Backend-only service credentials, private Supabase tables/storage, RLS lockdown, revisioned writes
Axion to providers	Finite timeouts, retries only where safe, circuit breakers, signed webhooks and scoped configuration
Axion to OT	Separate customer-site gateway; no direct public PLC connection; read-only and allowlisted by default

02 · CONTROL DOMAIN

Identity, session and access

CONTROL	STATUS	EVIDENCE / BOUNDARY
Time-bounded HMAC-signed sessions with issuer, audience, issued-at, expiry and unique session ID	Implemented	server.mjs; automated security tests
HttpOnly, Secure, SameSite=Strict browser session cookie and explicit logout/revocation	Implemented	server.mjs; backend tests
Rate limiting, bounded credential input, uniform login errors and temporary lockout	Implemented	server.mjs; automated security tests
Role, project ownership and subscription entitlement enforcement	Implemented	API authorization tests
Enterprise SSO and MFA	Deployment / external	Identity-provider configuration and customer acceptance required
Shared session revocation and account-wide invalidation across application instances	Implemented	Persistent session revocation/invalidation state; backend and security tests
Recent-authentication gate for admin, connector-secret and automation actions	Implemented	Sensitive route policy and automated security tests

03 · CONTROL DOMAIN

Application and API security

CONTROL	STATUS	EVIDENCE / BOUNDARY
Origin checks, Fetch Metadata protection, request limits, method allowlist and no-store API responses	Implemented	server.mjs; security-hardening tests
CSP, frame denial, MIME sniff protection, permissions policy and HSTS on HTTPS	Implemented	HTTP response headers
Idempotency keys, serialized mutations and structured error/request identifiers	Implemented	server.mjs; backend tests
Public-cloud connector URLs reject credentials, non-HTTPS targets, localhost and private/link-local addresses	Implemented	Connector URL policy and security tests
HMAC-chained security-event records for sensitive identity, upload and connector actions	Implemented	Persistent security event chain and normalized audit index
Independent penetration test and recurring DAST	External evidence required	No completed external report is claimed

04 · CONTROL DOMAIN

Data protection and model governance

CONTROL	STATUS	EVIDENCE / BOUNDARY
Supabase service credentials remain backend-only; public, anon and authenticated database grants are revoked	Implemented in migration	Supabase lockdown migration and tests
Private object storage, pre-storage type/signature/content inspection, provenance, timestamps, reviewers, branches, versions and audit records	Implemented	Application workflows and API tests
Independent malware scanning and customer-specific DLP	Deployment / external	Static application inspection is implemented; independent scanning service and DLP policy remain deployment controls
Customer-specific retention, deletion, DPA and data residency	Deployment / contract	Must be agreed and configured per customer
GMP electronic records/signatures qualification	External validation required	Customer intended-use validation and quality-system approval required

05 · CONTROL DOMAIN

Reliability and recovery

CONTROL	STATUS	EVIDENCE / BOUNDARY
Liveness, readiness, dependency timeouts, bounded retries, circuit breakers and overload response	Implemented	Health API, reliability runbook and scheduled smoke workflow
Revisioned compare-and-swap writes and duplicate-operation protection	Implemented	Supabase persistence implementation and tests
Database and private-storage backup, checksum verification and restore tooling	Implemented tooling	Backup/restore scripts and runbook
Point-in-time recovery, multi-instance failover and contractual SLA	Deployment / external	Managed hosting configuration and signed SLA required

06 · CONTROL DOMAIN

Secure development and supply chain

CONTROL	STATUS	EVIDENCE / BOUNDARY
Automated syntax, unit, integration, browser, container, performance and security checks	Implemented	GitHub Actions CI
Tracked-file secret scanning and production dependency audit	Implemented	CI security gate
CycloneDX software bill of materials	Implemented	Downloadable SBOM generated from the lockfile
Signed build provenance, vulnerability disclosure SLA and certification audit	Roadmap / external	Requires managed signing, triage operations and independent auditor

07 · CONTROL DOMAIN

Industrial and OT boundary

CONTROL	STATUS	EVIDENCE / BOUNDARY
Public Axion service does not connect directly to PLCs or safety systems	Architecture rule	Threat model and automation gateway design
Customer-site gateway, certificate trust, allowlisted tags, read-only default and commissioning checks	Implemented design	Gateway code, site-pack policy and CI container validation
Production OT commissioning, interlock review and IEC 62443 site qualification	Customer / external	Site network, certificates, node IDs and approved safety documentation required

08 · SHARED RESPONSIBILITY

Secure operation requires three parties to do their part.

PARTY	RESPONSIBILITY
Axion	Secure application development, hosted API controls, release gates, documented recovery tooling and transparent product limitations.
Hosting and service providers	Physical infrastructure, managed platform controls, provider availability and provider-side security configuration.
Customer	Identity lifecycle, endpoint security, least-privilege user assignment, lawful data upload, model review, validation, OT segmentation and safe operating decisions.

What Axion does not claim

- ISO/IEC 27001 certification
- IEC 62443 certification
- SOC 2 attestation
- Completed independent penetration test
- 24/7 security operations center
- GMP validation for a customer's intended use

CUSTOMER DUE DILIGENCE

Request current architecture, data-flow, subprocessor, backup/restore, incident, vulnerability and penetration-test evidence for the intended deployment. Regulated or safety-relevant use requires a customer-owned risk assessment and validation plan.

09 · FRAMEWORK REFERENCES

Controls are mapped to recognized secure-development practices.

These sources guide the control model; they do not constitute certification or endorsement.

NIST Secure Software Development Framework SP 800-218

https://csrc.nist.gov/pubs/sp/800/218/final

OWASP Application Security Verification Standard

https://owasp.org/www-project-application-security-verification-standard/

IEC 62443-4-1 secure product development lifecycle

https://webstore.iec.ch/en/publication/33615

BSI Cloud Computing Compliance Criteria Catalogue (C5)

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/ComplianceControlsCatalogue-Cloud_Computing-C5.html

EU Cyber Resilience Act

https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Siemens Product Security

https://www.siemens.com/en-us/products/grid-security/product-security/

Siemens Cybersecurity Baseline

https://developer.siemens.com/guidelines/cys-guidelines-external/overview.html

Document maintenance

The source of truth is docs/security/security-reliability-overview.json. Update the control status and review date, then run the security:document command. The generated PDF is published under Resources and should be regenerated after material architecture, hosting, identity, storage, payment, OT or incident-process changes.

https://ax-i-on.com/security