



PUBLIC CUSTOMER INFORMATION

Acatian Security & Reliability Overview

Implemented controls, deployment boundaries and shared responsibility

DOCUMENT BASIS

Product workflows, visible results, review criteria, evidence boundaries and controlled handover.

SEC-PUBLIC-1.4 | RELEASE 4.2

6 OCTOBER 2026



Document control

One controlled basis for public product guidance.

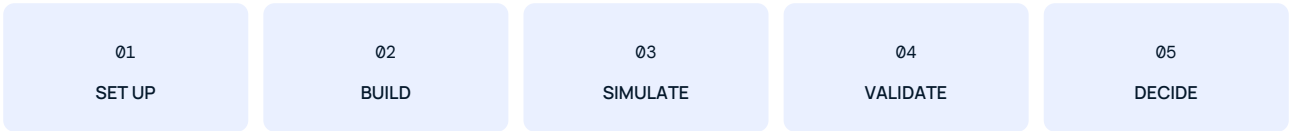
FIELD	VALUE
Document ID	SEC-PUBLIC-1.4
Release	4.2
Reviewed	6 October 2026
Audience	Customer security, procurement, engineering, IT and quality reviewers
Purpose	Public due-diligence overview of implemented controls, deployment responsibilities and explicitly unclaimed assurance
Owner	Acatian Product and Engineering

APPLICABILITY LIMIT

This manual explains the product workflow and the evidence needed to interpret its outputs. It does not replace qualified engineering judgement, customer quality systems, safety review, equipment-vendor data or validation for a regulated intended use.

Scope and use

Use the navigation path, input register, visible-result description, review criteria and handover record together. A screen or exported number without its model version, basis, unit, evidence status and limitations is not a controlled engineering result.



LANGUAGE

This document is written consistently in English. Product navigation names remain as displayed in the interface.

Executive overview

SECURITY POSITION

Acatian applies layered application, data, delivery and operational controls to protect customer engineering work. The platform uses signed time-bounded sessions, persistent login lockout, independently peppered password hashes, shared session revocation, token-bound checkout confirmation, authenticated project ownership, backend-only data access, private pre-storage upload inspection, connector target restrictions, signed and replay-protected OT write commands, 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.

Design principles

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

Architecture boundaries

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

READING RULE

Implemented means the product repository contains the named control and supporting automated checks. Deployment, contract and external statuses remain customer, provider or independent-assurance responsibilities.

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, persistent temporary lockout and independent script password pepper	Implemented	server.mjs; backend and security tests
Role, project ownership and subscription entitlement enforcement	Implemented	API authorization tests
Enterprise SSO or user-wide 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

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
Checkout confirmation requires a high-entropy, time-bounded token in addition to the Stripe session identifier	Implemented	server.mjs; Stripe checkout integration test
Independent penetration test and recurring DAST	External evidence required	No completed external report is claimed

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

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
Revised 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

Secure development and supply chain

CONTROL	STATUS	EVIDENCE / BOUNDARY
Automated syntax, unit, integration, browser, container, performance and security checks	Implemented	GitHub Actions CI
Expanded tracked-file secret scanning, build-artifact secret exclusion and production dependency audit	Implemented	CI security gate and deployment revision test
Exact direct dependency versions, SHA-pinned CI actions and automated dependency updates	Implemented	Package manifests, lockfile, GitHub Actions and Dependabot configuration
CycloneDX software bill of materials	Implemented	Downloadable SBOM generated from the lockfile
Release provenance and SBOM attestation workflow	Implemented tooling	Tag/manual GitHub Actions workflow; repository attestation support must be enabled
Signed build provenance, vulnerability disclosure SLA and certification audit	Roadmap / external	Requires managed signing, triage operations and independent auditor

Industrial and OT boundary

CONTROL	STATUS	EVIDENCE / BOUNDARY
Public Acatian 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
Physical write requests are HMAC-signed, time-bounded and nonce-protected against replay	Implemented	API and gateway write-signing implementation; automated gateway test
Production OT commissioning, interlock review and IEC 62443 site qualification	Customer / external	Site network, certificates, node IDs and approved safety documentation required

Shared responsibility

PARTY	RESPONSIBILITY
Acatian	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.

Assurance boundary

IMPLEMENTED BASIS

The repository contains the controls marked Implemented and automated checks for critical behavior.

NOT CLAIMED

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

Reference framework

These sources provide context for control design. A reference is not a certification claim.

REFERENCE	URL
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

CONTACT

support@acatian.com | <https://acatian.com/security>