Security & Deployment Overview

How Cabrillo Club protects your data, meets compliance requirements, and deploys on your infrastructure.

Prepared by Cabrillo Club | cabrilloclub.com

Deployment Modes

Cabrillo Club supports three deployment modes, each designed for different security postures and compliance requirements. All modes deliver the same platform capabilities with identical data boundary guarantees.

VPC Cloud

Dedicated single-tenant deployment within your cloud provider (AWS GovCloud, Azure Government). Infrastructure is provisioned inside your VPC with no shared resources. All data stays within your cloud boundary. Ideal for organizations with existing cloud infrastructure and FedRAMP-authorized environments.

On-Premise

Full platform deployment on your physical hardware behind your firewall. Complete network isolation with zero external dependencies at runtime. All AI inference, data storage, and audit logging runs on hardware you control. Recommended for organizations with strict data sovereignty requirements.

Air-Gapped

Fully disconnected deployment with no network access to external systems. Software updates delivered via verified media. Designed for classified or highly sensitive environments where any external connectivity is prohibited. All functionality operates without internet access.

Data Boundaries

Every deployment enforces strict data boundaries by design. The default posture is deny-external: nothing leaves your infrastructure unless explicitly configured.

What Stays Inside Your Boundary

[ ]	All CUI (Controlled Unclassified Information) and sensitive business data
[ ]	AI inference requests and responses - no external LLM calls
[ ]	Complete audit logs and compliance evidence
[ ]	User credentials, session data, and access control records
[ ]	Proposal content, pricing models, and competitive intelligence

Default Posture: Deny External

All outbound network connections are blocked by default. The platform operates fully within your infrastructure boundary without requiring external API calls, cloud services, or third-party data processors.

Optional External (Configurable)

SAM.gov read-only ingest -When enabled, the platform pulls publicly available contract opportunity data from SAM.gov via one-way read-only connection. No internal data is transmitted. This is the only optional external connection and can be disabled at any time.

Compliance Framework Alignment

The platform architecture is designed from the ground up to align with federal compliance frameworks. Every architectural decision -from data flow to audit logging -maps to specific control requirements.

Framework	Status	Details
NIST SP 800-171 Rev 2	110 controls addressed	See below
CMMC 2.0 Level 2	Architecture aligned	See below
FedRAMP Moderate	Readiness in progress	See below

NIST SP 800-171 Rev 2 -110 controls addressed

All 110 security controls from NIST SP 800-171 Rev 2 are addressed in the platform architecture. Controls span all 14 families including Access Control, Audit & Accountability, Configuration Management, and System & Communications Protection.

CMMC 2.0 Level 2 -Architecture aligned

Platform architecture aligns with CMMC 2.0 Level 2 requirements, which map directly to NIST 800-171 controls. System Security Plan documented and assessment preparation complete.

FedRAMP Moderate -Readiness in progress

Platform designed for FedRAMP Moderate authorization from inception. Boundary documentation, continuous monitoring capabilities, and System Security Plan preparation underway. 3PAO engagement planned for Q2 2026.

Audit Architecture

Every action taken by the AI system -and every human interaction -is logged to an immutable audit trail. This is not an afterthought; it is a core architectural requirement.

Every AI Action Logged

Each AI inference, recommendation, and automated action is recorded with full context: who triggered it, what data was accessed, what decision was made, and when it occurred.

Immutable Audit Trail

Audit records are append-only and cryptographically linked. Records cannot be modified or deleted, even by system administrators. This ensures evidence integrity for assessors.

Exportable for Assessors

Complete audit trails can be exported in standard formats for C3PAO assessors, internal auditors, and compliance reviewers. Reports are filterable by time range, user, action type, and data classification level.

Compliance Roadmap

We hold ourselves to the same compliance standards we help our clients achieve. Below is our current certification timeline.

Certification	Target	Status
FedRAMP Moderate Authorization	Q3 2026	Platform architecture designed for FedRAMP Moderate from inception. Readiness assessment
SOC 2 Type II	Q2 2026	Trust service criteria mapped. Security, availability, and confidentiality controls operational. Form
CMMC Level 2 Ready	Current	All 110 NIST 800-171 controls addressed. System Security Plan documented. Ready for assess

Learn More

Security & Deployment Architecture:

cabrilloclub.com/security-and-deployment

Schedule a Security Assessment:

cabrilloclub.com/proposal