Security Architecture

Security Architecture

Field	Value
Distribution	WCT English — OpenC5ISR
Product	OpenC5ISR
Release	0.15.1
Deployment	`openc5isr-en.wallacecorptech.com`
Source	`/srv/wct/releases/OpenC5ISR-v0.15.0`
Evidence	Reference controls and static security indicators
Source fingerprint	`63d2b1097707e25d666401cdc6362e395968600a40a08690210cd8c0b75fbf50`
Status	Generated baseline — human review required

> **Verification boundary:** This page combines platform design guidance with static evidence from the release. It does not prove that every detected interface is enabled, reachable, secure, or operational in the deployed environment.

Security model

Security must be applied across identity, content, interfaces, transport, deployment and evidence—not bolted onto the user interface. Each module should authenticate subjects, authorize actions and data, protect transport, minimize secrets, emit audit events and preserve provenance.

Observed indicators

Indicator	Observed

Secret-designated environment variables	ANTHROPIC_API_KEY, OPENAAR_SIGNING_KEY, OPENAI_API_KEY, OPENBUS_API_TOKEN, OPENCYBERSEC_AGENT_TOKEN, OPENCYBERSEC_OPERATOR_TOKEN, OPENCYBERSEC_READ_TOKEN, OPENKNOWLEDGE_EDITOR_TOKEN, OPENLLM_ANTHROPIC_API_KEY, OPENLLM_OPENAI_API_KEY, OPENLLM_OPENWEBUI_API_KEY, OPENLLM_OPERATOR_TOKEN, OPENPNT_AGENT_TOKEN, OPENPNT_TOKEN, OPENRF_AGENT_TOKEN, OPENRF_OPERATOR_TOKEN, OPENRF_READ_TOKEN, OPENSSA_SENSOR_TOKEN, OPENWEBUI_API_KEY, ROCKETCHAT_AUTH_TOKEN, ROCKETCHAT_OUTGOING_TOKEN, TOKEN
Security term counts	TLS: 1960, authorization/RBAC: 172, audit: 101, authentication: 64, CORS: 19
Potential sensitive file names	—

Required controls

Boundary	Minimum control
User/API identity	Named accounts or service identities, least privilege, revocable tokens and MFA where supported.
Transport	TLS for public and management interfaces; authenticated/encrypted links for operational buses where threat requires.
Content	Handling/release labels, role/attribute policy, object-level authorization and protected exports.
Secrets	No secrets in source, documentation, URLs or logs; use protected environment/secret stores and rotation.
Audit/evidence	Record actor, action, target, result, source time and correlation identifiers with tamper-aware retention.
Supply chain	Pinned dependencies/images, vulnerability review, signed release artifacts and reproducible deployment records.

Immediate review actions

- Rotate any token or password exposed in chat, shell history, logs or documentation.
- Verify BookStack/API credentials are stored only in the protected generator configuration.
- Test authorization for each edition so documentation and operational data do not cross unintended boundaries.

- Document incident response, backup confidentiality and restore authorization.

Maintainer Notes

Add human-reviewed deployment notes, corrections, decisions, screenshots, and links here. Content outside the generated block is preserved on future runs.

Revision #1
Created 2026-08-28 15:04:24 UTC by Nexus Ops Administrator
Updated 2026-08-28 15:04:24 UTC by Nexus Ops Administrator