

Distributed Systems, Inc. - Security Function Charter and Operating Controls

Effective: October 6, 2026

Owner and accountable lead: Arthur Colle, Founder & CEO

Contact: arthur@distributed.systems

Function: Infrastructure Security within Research & Engineering

Membership: Arthur Colle; one named person

Mandate and accountability

Infrastructure Security protects the company's autonomous-agent software, distributed AI infrastructure, identity services and tool-execution boundaries. Arthur Colle owns security-risk decisions, approves test engagements, triages vulnerabilities, directs remediation and patch verification, and receives security and model-misuse alerts. The signed officer attestation names the accountable lead and authorized function.

The separate Research & Engineering - Offensive Security Testing function is led by the same person. Both functions were formally documented October 6, 2026. This is one employee performing two functions; it does not imply independent assurance, a larger team, or historical operation of a dedicated red team.

Product scope and actual coverage

The function's mandate covers company-owned or maintained DSCO, Chimera, Tool Management API, GraphSub, authentication and authorization services, model-routing gateways and distributed execution infrastructure. Third-party or customer systems require explicit written authorization. The October 6 focused assessment executed only local Tool Management API, identity, OAuth and private-worker boundary tests; listing products in the mandate does not claim each product has been penetration tested.

Operating control register

Control	Owner and procedure	Current evidence / verification status
Security accountability	Arthur owns decisions, alerts and approved membership	Named public lead and signed officer attestation
Workspace membership	Restrict granted access to the named approved individual; document any addition and provider approval	One requested user; granted workspace access has not yet been verified
Test authorization	Record named targets/owners, authority, permitted techniques, data constraints, start/end times and stopping conditions before each engagement	Written rules and pre-execution record DSCO-SEC-2026-10-06-02
Boundary verification	Exercise negative cases and positive controls for identity, tenant isolation, tokens and execution transport	70 passed local checks in 17 case families; separately documented earlier 113-test suite; counts overlap
Vulnerability management	Record component/revision, reproducible steps, impact, severity and owner; escalate critical findings immediately; deliver report within ten days	Rules adopted; current run had zero failed assertions and no confirmed new vulnerability
Remediation closure	Verify the patch with an appropriate reproduction/regression check before closing a finding; record accepted residual risk	Procedure documented; no new vulnerability remediation performed in this run
Incident handling	Receive alerts, preserve evidence, contain/revoke affected access, assess impact, communicate and track recovery	Runbook documented below; live incident response and tabletop exercise not verified
Sensitive evidence	Use synthetic data and inert credentials for local adversarial tests; retain raw evidence privately and publish sanitized reports	Local engagement data constraints and sanitized public report; no universal secret-management claim
Secure credential use	Use attributable accounts, approved secret storage and least privilege; verify MFA and provider credential requirements before attesting	Operating rule; actual approved-workspace MFA and credential lifecycle remain unverified
Responsible disclosure	Prefer private reporting, reproduce within authorized scope and coordinate publication after remediation	Public DSCO repository SECURITY.md; response targets are policy, not historical performance evidence
Material changes	Update named users, scope and contact when they change; notify the provider within applicable program requirements	Documented procedure; no change-history compliance claimed

Control	Owner and procedure	Current evidence / verification status
Assurance readiness	Maintain a control register, asset scope and dated evidence; obtain independent assessment if required	Present first-party evidence; no current ISO 27001, SOC 2 Type II, qualifying annual filing or 12-month paid bounty supplied

Incident and misuse handling runbook

- 1 Arthur receives security or misuse alerts at the named work address, logs the source, affected systems, discovery time and severity, and establishes an incident record.
- 2 Preserve relevant logs and test evidence privately. Pause the affected testing/workspace and revoke or rotate implicated credentials where warranted; avoid destroying evidence.
- 3 Determine affected identities, systems and data, assign containment and remediation actions, and use provider notification deadlines applicable to the granted workspace. Do not defer a required report while waiting for full root cause.
- 4 Validate recovery, document residual risk and remediation ownership, and retain a closure record with regression evidence. Review scope, accounts and operating rules after an incident.

This runbook establishes a present procedure. An actual incident response, exercise completion or measured response time is not asserted.

Evidence and external research

- Security accountability: <https://distributed.systems/people#security>
- Signed officer attestation: <https://distributed.systems/documents/officer-attestation.pdf>
- Local assessment: <https://distributed.systems/documents/adversarial-assessment-2026-10-06.pdf>
- Testing rules: <https://distributed.systems/documents/security-testing-rules-of-engagement.md>
- Public responsible-disclosure policy: <https://github.com/arthurcolle/dsco/blob/main/SECURITY.md>
- Independently published research naming Arthur as co-author:
<https://apartresearch.com/project/detecting-piecewise-cyber-espionage-in-model-apis-a8gx>

Prior research establishes the lead's experience, not independent verification of the company's present security program. This charter and its control register are first-party operating records, not a certification or annual regulatory disclosure.