AI Governance Statement

GOVERNANCE | ARISE FRAMEWORK

High-level public commitment to ethical AI usage — CyberPlug DevSecOps Security AI

> *CyberPlug is committed to responsible, transparent, and accountable deployment of AI-powered security tooling within financial technology environments. This statement sets out the principles, structures, and obligations under which CyberPlug operates and through which all AI-driven activities are governed.*

1. Governing Principles

✓ Accountability

Every automated decision produced by CyberPlug is traceable to a named system process, model version, and responsible human owner. No security-critical action is taken without a defined accountable party.

✓ Risk-Proportionality

The depth of governance controls applied to any platform function scales with the potential harm of that function. High-risk outputs — such as deployment blocks or Critical vulnerability classifications — attract mandatory human review.

✓ Data Minimisation

CyberPlug collects only the data necessary to perform its stated security functions. Vulnerability metadata, scan results, and configuration data are not used for any purpose beyond securing the tenant's own environment.

✓ Transparency

Tenants and end-users are entitled to clear, plain-language explanations of what CyberPlug is doing, why it has flagged a finding, and how they can challenge or override a recommendation.

✓ Continuous Improvement

Governance controls are reviewed quarterly, with findings from audits, incident reviews, and user feedback incorporated into updated policy versions.

2. Governance Structure

CyberPlug governance is overseen by a designated AI Governance Lead who chairs a quarterly Governance Review Board (GRB). A dedicated Algorithmic Risk Committee (ARC) holds accountability for AI system design, monitoring, and audit compliance.

Role	Responsibility	Authority
AI Governance Lead / CISO	Chairs ARC; approves risk tolerance thresholds; can stop AAA System entirely	Full Human-in-Command authority
Compliance Officer	Maintains Human Interactions Log; signs off audit exports; monitors SLA adherence	Human-in-Command; Post Hoc Review
Security Engineer	Triages AI findings; approves/rejects recommendations; logs all human interactions	Human-in-the-Loop / Human-on-the-Loop
Asset Owner	Approves risk treatment decisions; countersigns Critical risk acceptance	Human-in-the-Loop for Critical findings

3. Regulatory Commitments

Framework	Applicable Requirement	CyberPlug Response

PCI DSS v4.0	Req. 6 & 11 — secure development & security testing	Automated scanning mapped to Req. 6.3 & 11.3; audit-ready reports per scan cycle
ISO/IEC 27001:2022	A.8.8 vulnerability mgmt; A.8.25 secure dev lifecycle	Continuous CVE monitoring; CI/CD integration; tamper-evident audit logs
OWASP Top 10	Web application and API security risk coverage	All scan rulesets maintained against latest OWASP release
GDPR / Data Protection	Art. 32 — security of processing; Art. 25 — privacy by design	No PII ingested by default; data residency controls enforce tenant jurisdiction
ForHumanity Audit Criteria	Human Oversight & Interaction Policy, ARC duties, KRI thresholds	Full Human Interactions Policy documented; ARC compliant
Ghana AI Strategy	Pillars 4 (Data Sovereignty) & 6 (Ethical Governance)	Ghana-based hosting; ARISE framework applied; local data residency enforced

4. Review and Accountability

AUDIT CYCLE: Quarterly internal ARC review + annual independent external audit

INCIDENT PROCESS: Any AI-related incident triggers root-cause analysis; findings published to ARC within 30 days

VERSION CONTROL: All model versions semantically versioned; changes require governance sign-off and changelog publication

PUBLIC TRANSPARENCY: Annual Human Oversight Transparency Statement published publicly

LAST REVIEWED: April 2026 | Next review: July 2026