Data Ethics Checklist

APPLIED ETHICS | SD3 SUBMISSION

Internal verification for ethical data sourcing, handling, and model governance — CyberPlug DevSecOps Security AI

1. Data Collection & Sourcing

- ✓ Only data necessary for stated security functions is collected
- ✓ No personally identifiable information (PII) is ingested by default
- ✓ All training datasets documented with provenance, source, and licence
- ✓ Anonymised remediation data stripped of tenant identifiers before any model use
- ✓ No tenant security data used to train models serving other tenants
- ✓ Aggregated, anonymised statistics used for product improvement cannot be linked back to any organisation

2. Training Datasets

Dataset	Source	Purpose	PII / Sensitive Data	Licence
NVD CVE Historical (2002–present)	NIST	Vuln. classification & severity prediction	None	Public Domain
OWASP Benchmark Suite	OWASP Foundation	False positive/negative calibration	None — synthetic data	Apache 2.0
CWE Enumeration Corpus	MITRE Corporation	Weakness classification & remediation mapping	None	Public Domain
Anonymised Remediation Outcomes	CyberPlug (internal)	Model fine-tuning on remediation effectiveness	Stripped — tenant identifiers removed before training	Proprietary

3. Model Governance

- ✓ All AI models are semantically versioned and changes require governance sign-off
- ✓ Confidence scores (High / Medium / Low) exposed to operators on every AI output
- ✓ Bias monitoring conducted quarterly across asset types, technology stacks, and industry sectors
- ✓ Quarterly bias reports reviewed by the AI Governance Lead and reported to the ARC
- ✓ Tenants may opt out of AI recommendations and operate in rules-only mode at any time
- ✓ Right to explanation: any finding can be challenged; detailed explanation within 5 business days

4. Data Residency & Security

- ✓ All tenant data processed and stored exclusively within the tenant's selected regional stack (West Africa / Europe / North America)
- ✓ AES-256 encryption at rest; TLS 1.3 minimum in transit
- ✓ No cross-regional data transfer without explicit written tenant consent
- ✓ Tenant-managed BYOK (Bring Your Own Key) encryption available for regulated institutions
- ✓ Tamper-resistant audit logs maintained independently per region with dual-authorisation required for deletion

5. Checklist Certification

All items above verified by the Algorithmic Risk Committee (ARC) as of April 2026.
Next quarterly review: July 2026. Annual independent audit: Q4 2026.
Signed: AI Governance Lead | CyberPlug Governance & Compliance Team