Version : 1.0

Prepared by FRIDRICK CYBER TECH Pvt. Ltd

Objective: Ensure that all AI tools and platforms integrated into your infrastructure meet security, compliance, and governance requirements without introducing risk or violating standards (ISO/IEC 27001, ISO/IEC 42001, GDPR, etc.).

Status Legend	
Status	**Meaning**
Pass	Requirement fully met with evidence
Partial	Partially implemented or evidence incomplete
Fail	Not implemented or inadequate controls
N/A	Not applicable for this product/scope

#	Control Item	Description	Status	Proof/Evidence Required
1.1	Model Provenance	Verified origin (e.g., Hugging Face, Azure OpenAI, internal)		Source URL, license, hash
1.2	Model Type	Is it pre-trained, fine-tuned, or custom-trained?		Documentation of training process
1.3	Model Integrity	Verified with checksums or signatures		Hash check, SBOM
1.4	Adversarial Resistance	Defenses against adversarial attacks		Threat model report
1.5	Explainability	Tools to support explainability (e.g., SHAP, LIME)		Output examples, model cards
1.6	Drift Detection	Detection and retraining strategy		ML Ops policy or pipeline doc
1.7	Model Access Controls	RBAC to restrict access		IAM policy screenshot
1.8	Output Sanitization	Output checked for PII, hallucinations		Prompt/output filtering logs
1.9	API Abuse Protection	Rate limiting and monitoring for inference endpoints		API gateway config/logs

#	Control Item	Description	Status	Proof/Evidence Required
2.1	API Security	TLS 1.2+, OAuth2.0, API key rotation		OpenAPI spec, API logs
2.2	Gateway Controls	Secure proxy or API gateway integration		Architecture diagram
2.3	Secret Management	Vault used for secrets (not in code)		Vault config, secrets policy
2.4	Input/Output Validation	Validates against schema, DLP checks		Validation code snippet
2.5	Error Handling	Sensitive info not leaked via errors		Sample error logs
2.6	Logging Enabled	API usage logged and sent to SIEM		Log file or SIEM screenshot

#	Control Item	Description	Status	Proof/Evidence Required
3.1	Identity Federation	SSO integrated (e.g., Okta, Azure AD)		SSO metadata / screenshot
3.2	Role-Based Access	RBAC implemented for all services		IAM roles, permissions audit
3.3	Admin Access	Admin use monitored and restricted		Audit logs
3.4	Credential Hygiene	No hardcoded creds or long-lived tokens		Secrets scan report
3.5	Least Privilege	Each user/service has minimal access		IAM policy samples
3.6	MFA for Access	Required for dashboard, API, CLI, Privileged account		MFA config proof

#	Control Item	Description	Status	Proof/Evidence Required
4.1	Hosting Type	On-prem, cloud, hybrid—security aligned		Hosting architecture
4.2	OS & Container Hardening	Hardened base image, CIS benchmarked		Dockerfile, scan reports
4.3	Runtime Security	Agent-based monitoring (Falco, Aqua, etc.)		Tool report
4.4	Network Segmentation	VPC/Subnet separation and firewall rules		Network diagram
4.5	Egress Filtering	Restricted outbound access		Firewall config
4.6	Patch Management	All software up-to-date with patch SLAs		Patch report or schedule
4.7	IaC & Scanning	Terraform/K8s scanned before deployment		IaC repo + scanning report

#	Control Item	Description	Status	Proof/Evidence Required
5.1	Data Classification	PII/PHI tagged and mapped		Classification report
5.2	Encryption in Transit/Rest	TLS 1.2+ and AES-256 or FIPS validated,Databases and model artifacts		Config screenshot, cert details, database data encryption
5.3	DPIA Conducted	Privacy assessment for data use		DPIA document
5.4	Anonymization	Sensitive data redacted or masked		Data transformation script
5.5	Privacy Policy Review	Reviewed by legal/compliance		Redlined version
5.6	Consent Handling	Explicit user consent where required		UX screenshots / audit logs
5.7	DLP Enabled	DLP tooling for cloud and endpoints		DLP policy config
5.8	GDPR/CCPA Alignment	Meets applicable data privacy laws		Legal opinion or checklist

#	Control Item	Description	Status	Proof/Evidence Required
6.1	Risk Register Updated	AI tool added with documented risks		Risk log
6.2	Compliance Standards	ISO 27001 / ISO 42001 / SOC2 alignment		Audit report or SoA
6.3	Vendor Due Diligence	Third-party review completed		SIG Lite or TPRM form
6.4	Ethical AI Review	Bias/fairness/legal impacts reviewed		Governance committee notes
6.5	Audit Trail	All access/actions are logged for audit		Log samples or audit tool config
6.6	Policy Acceptance	AI users have accepted policies (AUP, Privacy, etc.)		Signed acknowledgements

#	Control Item	Description	Status	Proof/Evidence Required
7.1	Data Licensing	All training data is properly licensed		Dataset license
7.2	Retraining Workflow	Scheduled retraining and approval process		MLOps pipeline screenshot
7.3	Fairness/Bias Testing	Bias detection tools run regularly		Bias test report
7.4	Versioning	Models and datasets version-controlled		Git/MLFlow snapshot
7.5	Shadow Mode	AI tool tested in non-prod with real data		Evaluation report
7.6	Rollback Capability	Can roll back to prior version if needed		Recovery procedure doc

#	Control Item	Description	Status	Proof/Evidence Required
8.1	Retention Schedule	Defined for logs, models, data		Retention policy
8.2	Secure Deletion	Data removed with NIST 800-88 standards		Deletion logs or tool config
8.3	Backup Policy	Models and data regularly backed up		Backup job logs
8.4	DR Testing	Periodic testing of disaster recovery plan		DR test results
8.5	BCP Integration	Included in the org's BCP document		BCP/BRP docs

#	Control Item	Description	Status	Proof/Evidence Required
9.1	Real-Time Monitoring	Logs/metrics piped to central SIEM		SIEM config screen
9.2	Alerting	Alerts configured for anomalies & abuse		Alert rules
9.3	Incident Response Plan	AI-specific IR scenarios documented		IR playbook
9.4	Responsible Disclosure	Security contact and policy visible		Disclosure page/screenshot
9.5	Red Teaming	AI product tested for attacks & misuse		Red team report
9.6	Detection of Abuse	Monitoring for prompt injection, jailbreaks,Model theft,threat intelligence intergration		Abuse detection logs

#	Control Item	Description	Status	Proof/Evidence Required
10.1	Security Architecture	Approved and reviewed diagrams		Arch diagram (signed)
10.2	Threat Modeling	STRIDE or similar documented		Threat model worksheet
10.3	Code/Model Review	Reviewed by internal security or AppSec		Review findings
10.4	Penetration Testing	Completed on the AI tool or APIs		Pentest report
10.5	Compliance Certification	SOC 2, ISO, HIPAA, etc. (if SaaS)		Certification attestation

Role	Review Completed	Status
Security Architect	/	
CISO / Deputy CISO	/	
Data Privacy Officer	/	
AI Governance Lead	/	
Legal & Compliance	/	