DISC

DATA SHEET

Virtual CISO Services (vCISO)

DeuraInfoSec.com

AI Risk Management Policy (ISO 42001 Aligned)

Document Version: 1.0

Effective Date: [Insert Date]

Owner: [Chief Risk Officer / AI Governance Lead]

Approved by: [Executive Committee]

1. Purpose

This policy establishes the framework for managing risks associated with the development, deployment, and use of artificial intelligence (AI) systems in compliance with ISO 42001. It ensures AI systems are reliable, explainable, ethical, and compliant with applicable laws and regulations.

2. Scope

- Applies to all AI systems developed, deployed, or utilized by [Organization Name].
- Covers AI systems in production, research, testing, or third-party services.
- Includes all data used for training, validation, or operation of AI systems.

3. Roles & Responsibilities

Roles:

- AI Risk Owner: Oversee risk identification, assessment, and mitigation.
- AI Governance Committee: Review AI risk reports, approve mitigation plans, ensure ISO 42001 compliance.
- AI Developers / Data Scientists: Follow secure coding practices, document model design, perform bias audits.
- Compliance Team: Ensure alignment with GDPR, EU AI Act, HIPAA, and other relevant regulations.
- Internal Audit: Conduct periodic AI risk reviews and monitor policy adherence.

4. Risk Management Process

4.1 Risk Identification:
- Identify risks across AI lifecycle: data collection, model training, deployment, monitoring.
- Include risks such as bias, security vulnerabilities, regulatory non-compliance, performance failure, and ethical concerns.

4.2 Risk Assessment:
- Evaluate likelihood, impact, and regulatory implications of identified risks.
- Use quantitative and qualitative measures to prioritize AI risks.

4.3 Risk Mitigation:
- Implement controls such as model validation, explainability tools, bias mitigation techniques, access controls, and human oversight.
- Maintain documented mitigation plans with assigned ownership and timelines.

4.4 Risk Monitoring & Review:
- Continuously monitor AI systems for deviations, performance issues, or new risks.
- Conduct periodic audits and update risk assessments accordingly.

5. Regulatory & Ethical Compliance

- Ensure compliance with ISO 42001 clauses for AI risk management.
- Comply with EU AI Act (high-risk AI systems) and GDPR / HIPAA as applicable.
- Incorporate ethical principles: fairness, transparency, accountability, and human oversight.

6. Documentation & Reporting

- Maintain records of risk assessments, mitigation actions, audit results, and incidents.
- Report significant AI risks and incidents to the AI Governance Committee and senior management.

7. Training & Awareness

- Provide regular training to AI developers, data scientists, and business stakeholders on AI risks, compliance, and ethical use.
- Update training material as regulations and AI practices evolve.

8. Continuous Improvement

- Review and update the AI Risk Management Policy annually or as needed based on emerging AI risks, regulatory changes, and lessons learned from audits and incidents.

Approval

Approval: ____________________
Date: ____________________