Cisco AI Technical Practitioner v1.0

Exam Description: Cisco AI Technical Practitioner v1.0 (AITECH 810-110) is a 60-minute exam associated with the AI Technical Practitioner certification. This exam tests a candidate's knowledge and skills related to generative AI models, prompt engineering, AI ethics and security, data research and analysis, AI for Code and Workflow Optimization, and Agentic AI. The course, Cisco AI Technical Practitioner (AITECH), helps candidates prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

20% 1.0 Generative AI Models

- 1.1 Describe major generative AI model families (e.g., LLMs, diffusion models) and common use cases (text summarization, content creation, code generation)
- 1.2 Compare model hosting options (cloud-hosted vs locally hosted) and their trade-offs (cost, latency, privacy, scalability)
- 1.3 Explain role of context windows, token limits and response management
- 1.4 Understand model selection in AI model hubs and repositories for appropriate use-cases (e.g., reasoning, multimodality)
- 1.5 Describe Retrieval Augmented Generation (RAG) and role of embeddings and vector databases

15% 2.0 Prompt Engineering

- 2.1 Understand prompt engineering principles and patterns (roles, instructions, constraints)
- 2.2 Explain prompting techniques (iterative/sequential, chained, few-shot) and structures for text, image and audio generation
- 2.3 Describe prompt injection attack types
- 2.4 Explain defensive prompting and mitigation strategies for AI-generated errors (e.g., hallucinations)

15% 3.0 Ethics and Security

- 3.1 Explain responsible AI principles (fairness, transparency, accountability, bias mitigation, safety)
- 3.2 Describe approaches to protect corporate data privacy and security in AI systems
- 3.3 Explain AI-specific security threats and risks, including misinformation
- 3.4 Explain AI governance considerations (policy, risk management, compliance)

10% **4.0** **Data Research and Analysis**

- 4.1 Explain AI's role in exploratory data analysis (EDA)
- 4.2 Describe automated data preparation tasks (quality checks, formatting, transformation, cleaning)
- 4.3 Explain the ethical and privacy considerations in AI-assisted data analysis, including controls to prevent data exposure
- 4.4 Describe techniques for AI-assisted research, ideation, and content drafting

20% **5.0** **Development and Workflow Automation**

- 5.1 Describe AI's role across the software development lifecycle (requirements, prototyping, implementation, testing, deployment)
- 5.2 Describe the AI capabilities for code generation and rapid prototyping
- 5.3 Explain AI workflow design and monitoring principles
- 5.4 Describe how token usage and context-window management affect prototyping cost, latency, and output quality
- 5.5 Explain how AI improves code quality (debugging assistance, error handling, documentation)

20% **6.0** **Agentic AI**

- 6.1 Differentiate Agentic AI from Generative AI use cases
- 6.2 Explain AI agent design principles, autonomous capabilities, and orchestration
- 6.3 Describe Model Context Protocol (MCP) framework primitives in context of agentic AI
- 6.4 Explain human-in-the-loop (HITL) strategies
- 6.5 Describe data transformation and mapping within AI Agents