APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

AI at Work: Safe, Secure & Compliant

Applied Technology Academy

A practical one-day introduction to using artificial intelligence safely, responsibly and in compliance with organizational policy and regulation. Participants learn how generative AI works and where its limits lie, how AI has changed the threat landscape through phishing, deepfakes, voice fraud and AI-assisted malware, what must never be entered into a public AI tool, and how privacy, copyright and compliance obligations apply. Labs cover prompting practices, prompt guardrails and building a custom assistant.

LEVEL	DURATION	COURSE CODE	DELIVERY
Introductory	**1 Day**	**SEN-101**	**Instructor-led**

Course Overview

- One day, instructor-led, with short practical labs throughout.
- Written for every role, not just technical staff - no programming experience is needed.
- Covers public, enterprise and custom AI assistants, and the difference that matters for your data.
- Addresses Shadow AI, automation bias and the habit of critically evaluating AI-generated output.

Course Outline

- **Module 1. Introduction**
  - What AI is, and why it is a tool rather than magic.
  - How generative AI works and how it differs from traditional software.
  - Why AI has no true understanding: pattern recognition, hallucinations and misinformation.
  - Lab: prompting best practices.
- **Module 2. AI and Cybercrime: What Has Changed**
  - AI-enhanced phishing and spear phishing built from public social media.
  - Deepfake video and voice fraud, including deepfake injection during live calls.
  - AI-assisted malware, polymorphic code and the lowered barrier for unskilled attackers.
  - Lab: prompt guardrails.
- **Module 3. Using AI Safely at Work**
  - Information that must never be entered into public AI tools, and why.
  - Data retention, model training and vendor dependency.
  - Shadow AI: the risks, and how managers recognize it.
  - Public versus enterprise AI solutions; a high-level view of GDPR, HIPAA and similar obligations.
- **Module 4. AI, Privacy and Legal Risks**
  - Personal and sensitive data in an AI context, and privacy risk at the point of entry.

  - Privacy and AI impact assessments, including DPIAs.
  - The EU AI Act's risk-based approach, and why U.S. requirements vary by federal, state and sector.
  - Copyright, intellectual property, liability and contract exposure; bias and discrimination.
- **Module 5. The Human Factor: The Greatest Vulnerability**
  - Automation bias and authority bias, and recognizing overreliance on AI output.
  - Checking sources and verifying AI output logically.
  - Prompt injection and the disclosure of confidential information.
  - How AI errors spread quickly and at scale - the flywheel effect of automated mistakes.
- **Module 6. From Risk to Practice: Working Safely with Custom AI Assistants (time permitting)**
  - What a custom AI assistant is and when it adds value.
  - Platform differences across ChatGPT, Gemini, Claude and Copilot.
  - What information can safely be used, and when assistants create privacy and security risk.
  - Labs: create a Custom GPT; create a Gemini Gem.

Prerequisites

- No technical background is required.
- General familiarity with everyday business tools and a browser is enough.
- No prior experience with ChatGPT, Gemini, Claude or Copilot is assumed.

Who Should Attend

- Employees who already use AI tools, or are about to.
- Managers and team leads responsible for how their teams use AI.
- Security, privacy, HR and compliance staff who need a shared baseline to point people at.
- Organizations rolling out an AI policy that needs the people side to land.

What You'll Learn

By the end of this course, participants will be able to:

- explain in plain language how generative AI produces answers, and why it can be confidently wrong
- recognize AI-enhanced phishing, spear phishing, deepfake video and voice fraud
- describe how AI lowers the barrier for less skilled attackers and how malware evades detection
- identify which categories of company information must never be entered into a public AI tool
- explain the risks of data retention and model training, and the risks of Shadow AI
- distinguish public from enterprise AI services and apply the safe-use rules for their own role
- recognize privacy and legal exposure: personal data, GDPR, DPIAs, the EU AI Act and copyright
- spot automation bias, authority bias and overreliance in their own use of AI
- recognize prompt injection and the disclosure risk it creates

- configure a simple custom assistant, and judge when one adds value or adds risk

Hands-On Work

Labs run throughout the day:

- prompting best practices
- prompt guardrails
- a voice-assistant walkthrough
- building a Custom GPT and a Gemini Gem (time permitting)

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.