QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1205

AI Security & Privacy Training Course

AI GOVERNANCE, ETHICS & RISK
ARTIFICIAL INTELLIGENCE & APPLICATIONS

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The AI Security & Privacy Training Course is a comprehensive professional development program designed to equip executives, managers, AI leaders, cybersecurity professionals, data protection officers, governance specialists, compliance managers, risk professionals, legal advisors, data scientists, machine learning engineers, and technology teams with the knowledge and practical skills required to secure Artificial Intelligence systems and protect sensitive data throughout the AI lifecycle. As Artificial Intelligence becomes a critical component of digital transformation and enterprise operations, organizations must implement robust security and privacy controls to safeguard AI models, data assets, infrastructure, and business processes from evolving cyber threats while ensuring compliance with regulatory and privacy requirements.

Government entities, ministries, public sector organizations, banks and financial institutions, oil and gas companies, healthcare providers, manufacturing organizations, telecommunications companies, transportation authorities, educational institutions, and multinational corporations increasingly depend on AI-powered solutions to automate operations, optimize decision-making, improve customer experiences, strengthen predictive analytics, and enhance operational efficiency. However, AI systems introduce unique security and privacy risks, including data poisoning, model theft, adversarial attacks, unauthorized access, prompt injection, sensitive information leakage, privacy violations, model manipulation, and regulatory non-compliance. Organizations that proactively secure their AI environments can reduce cyber risks, protect valuable data, strengthen resilience, and maintain stakeholder trust.

This course provides a practical framework for securing enterprise AI environments by covering AI security architecture, AI threat modeling, model security, data protection, privacy engineering, identity and access management, secure AI development, AI governance, Responsible AI, cybersecurity risk management, incident response, vulnerability management, regulatory compliance, continuous monitoring, and AI lifecycle security. Participants will explore internationally recognized cybersecurity principles, privacy frameworks, and AI governance best practices while learning how to integrate security and privacy requirements into enterprise AI strategies and operational processes.

The AI Security & Privacy Training Course combines strategic knowledge with practical implementation through interactive workshops, enterprise case studies, risk assessments, security exercises, and implementation planning sessions. By the end of the course, participants will be capable of designing enterprise AI security strategies, protecting AI models and data assets,

strengthening privacy controls, improving regulatory compliance, managing AI-related cyber risks, and establishing resilient AI environments that support secure, trustworthy, and sustainable Artificial Intelligence adoption.

Objectives

- Analyze cybersecurity and privacy risks associated with Artificial Intelligence systems.
- Develop enterprise AI security and privacy strategies aligned with organizational objectives.
- Evaluate AI-specific threats, vulnerabilities, and attack vectors affecting AI environments.
- Apply cybersecurity and privacy controls throughout the AI lifecycle.
- Design secure AI architectures, governance models, and data protection frameworks.
- Improve organizational resilience through effective AI security monitoring and incident response planning.
- Strengthen AI governance, privacy protection, cybersecurity, and regulatory compliance capabilities.
- Implement security monitoring, vulnerability management, and continuous improvement processes.
- Assess organizational AI security maturity and identify opportunities for enhancement.
- Align AI security and privacy initiatives with enterprise cybersecurity, risk management, governance, and digital transformation strategies.

Who Should Attend

This course is designed for executives, chief information security officers, chief information officers, chief data officers, chief digital officers, AI leaders, cybersecurity managers, information security professionals, governance specialists, compliance officers, privacy officers, legal advisors, risk managers, internal auditors, enterprise architects, technology managers, data scientists, machine learning engineers, software developers, consultants, and decision-makers responsible for securing Artificial Intelligence systems.

The program is particularly valuable for professionals working in government entities, ministries, public sector organizations, banks and financial institutions, oil and gas companies, healthcare organizations, manufacturing companies, telecommunications providers, transportation authorities, educational institutions, consulting firms, regulatory agencies, and multinational corporations

implementing enterprise Artificial Intelligence solutions.

Professionals responsible for cybersecurity, governance, enterprise risk management, privacy, regulatory compliance, legal affairs, digital transformation, AI governance, data protection, operational resilience, infrastructure security, cloud security, and technology strategy will benefit from practical methodologies that strengthen organizational AI security capabilities.

Learning Outcomes

- By the end of this course, participants will be able to:
- Explain the principles and organizational importance of AI security and privacy.
- Identify AI-specific cybersecurity threats, vulnerabilities, and privacy risks.
- Develop enterprise AI security and privacy frameworks.
- Design security controls that protect AI models, data assets, infrastructure, and users.
- Apply cybersecurity, privacy protection, data governance, and Responsible AI principles throughout AI implementation.
- Implement identity and access management, encryption, monitoring, vulnerability management, and incident response practices.
- Monitor AI environments using security metrics, governance reporting, and continuous risk assessments.
- Integrate AI security and privacy into enterprise governance, cybersecurity, and risk management frameworks.
- Develop AI security incident response and recovery plans.
- Build enterprise implementation roadmaps supporting secure, resilient, compliant, and trustworthy Artificial Intelligence adoption.

Course Outline

DAY 01

Foundations of AI Security and Privacy

- Introduction to AI security and privacy
- AI threat landscape and cybersecurity fundamentals

DAY 01 — CONTINUED

- AI lifecycle security principles
- Privacy protection and data governance

PRACTICAL

Practical workshop on identifying AI security and privacy risks

DAY 02

Securing AI Models and Data

- AI model security and adversarial attacks
- Data protection and secure data management
- Identity and access management
- Encryption and secure AI infrastructure

PRACTICAL EXERCISE ON AI SECURITY RISK ASSESSMENT

DAY 03

Governance, Compliance, and Risk Management

- AI governance and security frameworks
- Regulatory compliance and privacy requirements
- Responsible AI and secure AI development
- Enterprise AI risk management

WORKSHOP ON DESIGNING AI SECURITY GOVERNANCE FRAMEWORKS

DAY 04

Monitoring, Incident Response, and Resilience

- AI security monitoring and threat detection
- Vulnerability management and security testing

DAY 04 — CONTINUED

- Incident response and recovery planning
- Continuous security improvement and operational resilience

PRACTICAL

Practical workshop on implementing enterprise AI security controls

DAY 05

Building an Enterprise AI Security & Privacy Strategy

- Future trends in AI cybersecurity and privacy
- International best practices for AI security and data protection
- Integrating AI security into enterprise cybersecurity and digital transformation strategies
- Organizational change management for secure AI adoption

FINAL WORKSHOP

Final workshop involving the development of a comprehensive Enterprise AI Security & Privacy Strategy integrating AI governance, cybersecurity, privacy protection, data governance, AI model security, identity and access management, encryption, vulnerability management, threat detection, incident response, regulatory compliance, Responsible AI, continuous monitoring, operational resilience, auditing, performance measurement, and implementation planning to establish secure, resilient, compliant, and trustworthy Artificial Intelligence across the enterprise.

Register or Request More Information

Course page: https://quest-training.com/courses/ai-security-privacy-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440