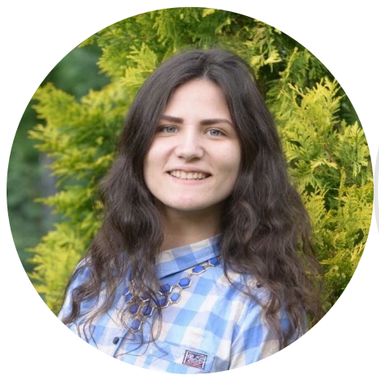
Safeguarding Your Business:

AI Security Awareness for Employees

Awareness programs must first demystify AI, explaining its capabilities and limitations. Beyond just how AI functions, employees need to understand how it can be applied to solve real-world business problems while mitigating potential pitfalls like bias, security, and privacy concerns.

Adhering to the practices outlined next not only helps develop secure AI solutions but also **establishes your organization as a trusted partner for clients** who prioritize the security and reliability of their applications.



Iryna Shevchuk

Information Security Officer

An effective awareness program empowers the employees of the company developing AI solutions to:

Better understand AI-related risks and select the best strategy to mitigate them

Ensure that all employees are knowledgeable about AI solutions (e.g., understanding what an AI tool is, how it operates, its limitations, possible threats, vulnerabilities, and risks).

Maintain adherence to various security and privacy standards and regulations

Train personnel on key safety and confidentiality protocols and guidelines – such as ISO 27001, GDPR, and HIPAA – that impact the development of AI-powered applications, outlining the potential consequences of non-compliance.

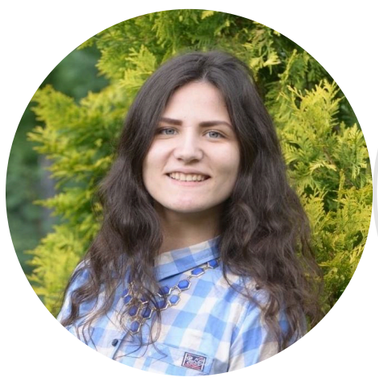
Build AI solutions with robust security mechanisms

Educate the workers that satefy is an integral part of the development process. The security team should be involved from the outset of the project, and requirements must be considered throughout the application lifecycle. Instruct the employees that all security hazards are to be processed and managed.

The awareness program for employees of the company incorporating such an AI solution into the business environment should cover the following aspects:

AI solution integration and its limitations	Educate employees on how the AI tool integrates with and enhances their daily operations. Highlight existing constraints, particularly in areas of security and privacy, to prevent misuse and establish precise boundaries.
Data security when adopting AI	Demonstrate clear guidelines on what data is safe to share, emphasizing security best practices *(e.g., anonymization where possible, avoiding the sharing of personal and confidential details)*.
Choosing a secure and trustworthy AI tool	Provide a checklist of essential security and privacy criteria for selecting a model. This should include adherence to industry-specific standards and regulations and its data protection capabilities.
Using AI output	Emphasize the importance of critically analyzing AI-generated information and practicing sound judgment. Discuss potential shortcomings in the AI's accuracy and reliability, especially in decision-making scenarios.

AI solutions are powerful, yet their success largely depends on a crucial factor - people. Whether you're developing cutting-edge AI technologies or integrating them into your business, **a staff awareness program is paramount**. Well-trained employees can maximize the benefits of AI while effectively managing related security risks. This ensures the secure development of solutions and promotes ethical and safe AI usage.



Iryna Shevchuk

Information Security Officer

What are your biggest LLM security concerns?

Let's discuss how MOCG can help you navigate LLM security challenges in your next project.

HOW MASTER OF CODE GLOBAL CAN EMPOWER YOUR SECURITY JOURNEY

At Master of Code Global, we're experts at developing custom world-class digital experiences for web, mobile, as well as conversational chat and voice solutions empowered by AI.

But we also know that building cutting-edge AI is only half the battle – securing it from day one is paramount. Here's how we do it.

Protect your Future with **our Expert-Driven Cybersecurity Services**

- Tailored Cybersecurity Consulting
- In-Depth Audits
- Robust Application Security
- Proactive Penetration Testing
- ISO 27001 & HIPAA Compliance Consulting
- Specialized Chatbot Security Testing
- Advanced AI Security Testing
- Comprehensive LLM Security Assessments

How We Protect Your LLM-Based Solutions

Our approach to LLM projects includes rigorous testing based on the latest practices and methodologies, like the OWASP Top 10 for LLMs, combined with regular internal training to ensure the highest standards of security and reliability.

We also incorporate these essential best practices:

- → Input validation and sanitization
- → Output filtering and content validation
- → Access controls and user authentication
- → Regular security assessments and penetration testing
- → Data encryption and sensitive information protection
- → Model fine-tuning and observation
- → Continuous monitoring and improvement
- → Incident response and recovery plan

ABOUT MOCG

At **Master of Code Global** we are a team of experts developing custom world-class digital experiences for web, mobile, as well as conversational chat and voice solutions empowered by AI.

1+ Billion Users Engaged

Founded in **2004**

500+ Projects Delivered

Clutch ★★★★★ 4,8/5 rating

ISO **ISO 27001** Information Security Management

250+ Masters

56 NPS, 9.2 CSA Client Feedback

Industries We Serve

eCommerce · Finance · Education · Airports · Travel & Hospitality · HR & Recruiting · Retail · Healthcare · Insurance · Telecom · Automotive · Banking

Work in partnership with

VERINT · sinch · boost·ai · HumanFirst · glia · cohere · infobip · Google Cloud · Quiq · nylas · VONAGE · LIVEPERSON · ada · chatfuel · botpress · Voiceflow

Trusted by leaders

The New York Times · BURBERRY · Esso · T-Mobile · ESTĒE LAUDER · eBags · TOM FORD BEAUTY · verizon · Dr. Oetker

Our Points of Contact

Wondering how to bring your ideas to life?

Contact us today for a free consultation and let's discuss your specific needs.

John Colón
VP of Global Enterprise Sales
john.colon@masterofcode.com

Ted Franz
VP of Sales & Partnerships
ted.franz@masterofcode.com

Olga Hrom
Delivery Manager
olga.hrom@masterofcode.com

Anhelina Biliak
Application Security Leader
anhelina.biliak@masterofcode.com

master.of.code GLOBAL

We’re helping businesses redefine and elevate customer experiences with AI

Contact our team

Get in touch via email:
sales@masterofcode.com

Learn more:
masterofcode.com