WORKSHOP

AI Security Standards:
a Step Forward in the Evaluation and AI Governance

8th May 2025 | Warsaw

NASK headquarters | 12th Kolska Street, Warsaw, Poland

Agenda

10:00 – 10:15	**Welcome** Dariusz Standerski, Secretary of State at the Ministry of Digital Affairs Paweł Kostkiewicz, Director of the Standardisation and Certification Centre at NASK
10:15 – 10:30	**AI security standardisation from the AI Act perspective** Kilian Gross, Deputy Director of the AI Office, Head of Unit Artificial Intelligence- Regulation and Compliance
	Block 1: Setting and harmonising AI security standards on the EU and global level
10:30 – 10:45	• **A view from ETSI TC Securing Artificial Intelligence** Scott Cadzow, Standardisation Expert at ETSI
10:45 – 11:00	• **Harmonised standards for the AI Act in the European and OECD context** Dr. Sebastian Hallensleben, Chief Trust Officer at Resaro, the Chair of CEN-CENELEC JTC 21
11:00 – 11:30	Coffee break
	Block 2: AI security standardisation in practice – lessons learnt, the challenges and opportunities
11:30 – 11:45	• **AI Security- a view from industry** Nicholas Butts, Director of Cybersecurity and AI Security Policy at Microsoft
11:45 – 12:00	• **ISO/IEC 42001 Certification and AI Security: SGS's Expertise and Lessons Learned** Michal Cichocki, Global Product Manager AI Assurance Services, SGS
12:00 – 12:15	• **Localizing AI Safety: Developing Guard Models and Evaluation Frameworks for Polish LLMs** Karolina Seweryn, Data Scientist at NASK
12:15 – 12:35	**Code of Practice and Technical Standard on AI Cybersecurity** Oliver B, International Technical Standards Lead at the UK National Cyber Security
12:35 – 13:00	**Fireside chat and open discussion** **Summary and closing** Filip Konopczyński, Expert at the Ministry of Digital Affairs
13:00 – 14:00	Lunch

POLAND25.EU

Ministry of Digital Affairs
Republic of Poland

NASK

Certification
NASK