ČESKÁ TECHNICKÁ NORMA

ICS 35.030 **Červen 2026**

Zabezpečení umělé inteligence (SAI) – Základní požadavky na kybernetickou bezpečnost modelů a systémů AI

ČSN
ETSI EN 304 223
V2.1.1
87 0033

Securing Artificial Intelligence (SAI) – Baseline Cyber Security Requirements for AI Models and Systems

Tato norma přejímá anglickou verzi evropské normy ETSI EN 304 223 V2.1.1:2025. Má stejný status jako oficiální verze.

This standard implements the English version of the European Standard ETSI EN 304 223 V2.1.1:2025. It has the same status as the official version.

Anotace obsahu

Tento dokument definuje základní bezpečnostní požadavky na modely a systémy AI. Tento dokument v rámci svého rozsahu platnosti zahrnuje i systémy, které vytvářejí hluboké neuronové sítě, jako je generativní AI. Z důvodu konzistence se v celém tomto dokumentu termín „systémy AI“ používá při vymezování rozsahu platnosti ustanovení a termín „bezpečnost AI“, který je považován za podmnožinu kybernetické bezpečnosti, se v rozsahu platnosti ustanovení používá v případě jakýchkoli záležitostí kybernetické bezpečnosti. Tento dokument není určen pro akademické pracovníky, kteří vytvářejí a zkoušejí systémy AI pouze pro výzkumné účely (systémy AI, které nejsou určeny k nasazení).

Národní předmluva

Informace o citovaných dokumentech

ETSI TR 104 128 dosud nezavedena

ISO/IEC 22989:2022 zavedena v ČSN EN ISO/IEC 22989:2023 (36 9019) Informační technologie – Umělá inteligence – Pojmy a terminologie umělé inteligence

ETSI TS 104 216 dosud nezavedena

ISO/IEC 27001:2022 zavedena v ČSN EN ISO/IEC 27001:2023 (36 9797) Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Systémy managementu informační bezpečnosti – Požadavky

CISA Software Bill of Materials (SBOM)

NIST AI Risk Management Framework: Second Draft:2022

NIST AI 100-1 AI Risk Management Framework (AI RMF 1.0):2023

Australian Signals Directorate An introduction to Artificial Intelligence:2023

World Economic Forum, IBM Presidio AI Framework: Towards Safe Generative AI Models:2024

OWASP OWASP AI Exchange

MITRE ATLAS™ Mitigations

Google® Secure AI Approach Framework: A quick guide to implementing the Secure AI Framework (SAIF):2023

ELSA ELSA – European Lighthouse on Secure and Safe AI:2023

Cisco The Cisco Responsible AI Framework:2024

Amazon AWS Cloud Adoption Framework for Artificial Intelligence, Machine Learning, and Generative AI", Amazon White Paper:2024

NIST AI 100-2 E2023 Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations

ENISA Multilayer Framework for Good Cybersecurity Practices for AI:2023

NCSC Guidelines for secure AI system development:2023

Federal Office for Information Security AI Security Concerns in a Nutshell:2023

G7 Hiroshima Summit Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems:2023

United States Department of Health and Human Services Trustworthy AI (TAI) Playbook: Executive Summary:2021

OpenAI Preparedness Framework (Beta):2023

Information Commissioner's Office (ICO) Guidance on the AI Auditing Framework:2020

Nvidia NeMo-Guardrails:2023

Citované předpisy

Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci).

Upozornění na národní přílohu

Do této normy byla doplněna informativní národní příloha NA, která obsahuje překlad kapitoly 3 této

evropské normy.

Vypracování normy

Zpracovatel Národní přílohy: MAREŠKA Praha, IČO 86983555

Technická normalizační komise: TNK 96 Telekomunikace

Vydala: Česká agentura pro standardizaci, státní příspěvková organizace

Citované dokumenty a souvisící ČSN lze získat v e-shopu.

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.