SHIN&KIM
법무법인(유) 세종

Korea Issues Zero Trust Guidance for AI Agents

2026.11.26

On November 6, 2026, the Ministry of Science and ICT ("MSIT") and the Korea Internet & Security Agency ("KISA") published the *Guidelines on Zero Trust for Agentic AI* (the "Guidelines"), providing practical guidance on applying zero trust principles in environments where AI agents are deployed and operated.

The Guidelines signal the government's expectations for how businesses should manage the security risks posed by AI agents and serve as a reference point for both regulators and businesses.

The key elements of the Guidelines and their practical implications are outlined below.

1. Background

The growing autonomy of AI agents has expanded the scope of security controls beyond traditional users, devices, and servers to include interactions with external services and commands issued to physical devices.

Zero trust operates on the principle of "Never Trust, Always Verify," requiring continuous verification of access requests on the assumption that the network has already been compromised. The Guidelines apply this approach to address security risks associated with the autonomy and broad access privileges of AI agents, including threats such as prompt injection and actions that exceed delegated authority.

2. Key Elements of the Guidelines

Extending the Zero Trust Maturity Model: The Guidelines adapt the four-level maturity model as defined under the *Zero Trust Guidelines 2.0*, published in December 2024, to the agentic AI environment and set specific application criteria for each level. Businesses can use the model to benchmark their current security posture, set targets, and prioritize improvements.

Verification and Human Approval: The Guidelines recommend verifying AI agent actions and enforcing security policies at key points of autonomous operation, including input processing, tool invocation, task delegation, and external communications. Depending on the level of risk, these activities may be subject to human approval or pre-approved security policies.

Implementation Roadmap: The Guidelines also set out key considerations for adoption, a step-by-step process for implementation and ongoing operation, and use cases that businesses can apply on their own.

The full Guidelines are available on the KISA website (www.kisa.or.kr).

3. Implications

Review Internal Controls for Agentic AI: The Guidelines provide the first set of specific criteria for applying zero trust principles to agentic AI environments. Businesses using or considering agentic AI should assess their current security posture against the maturity model, with particular attention to: (i) the scope of permissions granted to AI agents, (ii) controls over external service integrations and tool use, and (iii) procedures for human approval of higher-risk actions.

Take a Holistic Approach and Monitor Further Developments: The Guidelines follow the *AI Security Threat Mitigation Manual* and *AI Security Red Teaming Guide* issued by the MSIT and KISA in July 2026. Businesses should consider these resources alongside the new Guidelines when reviewing their broader AI security frameworks. As the government plans to issue further guidance on zero trust implementation, organizations should also monitor related policy developments.

About Shin & Kim's ICT Group

Shin & Kim's ICT Group has established a strong reputation for its expertise and extensive professional network in the ICT sector and has consistently received high praise from clients in recent years. Drawing on its experience in broadcasting, telecommunications, data privacy, and internet-related technologies, the Group provides comprehensive legal advice on ICT regulatory developments, government relations, legislative and regulatory reform, regulatory impact assessments, and corporate strategy. The Group also has extensive experience advising on AI compliance, the implementation of information security management systems, and security incident response.

For more information on these developments or their implications for your business, please contact any of the professionals listed above.

[Korean version] 과기정통부, 에이전틱 AI 이용 환경에서 제로트러스트를 적용할 수 있는 「자율형 인공지능 철통 인증 안내서」 발간

Key Contacts

Sinook Kang
Senior Partner

+82-2-316-4059
sokang@shinkim.com

Kwang-Hee Choi
Senior Advisor

+82-2-316-4651
khchoi@shinkim.com

Jin Hong Noh
Partner

+82-2-316-1639
jhnoh@shinkim.com

Jihyun Kang
Partner

+82-2-316-1518
jhykang@shinkim.com

Gayeong Kim
Associate

+82-2-316-7910
gyekim@shinkim.com

Hyein Lee
Senior Foreign Attorney

+82-2-316-1641
hilee@shinkim.com

Soonyoung Heo
Foreign Attorney

+82-2-316-1837
syheo@shinkim.com

Copyright SHIN & KIM LLC. All rights reserved.