Oregon
Tina Kotek, Governor

Enterprise Information Services
Cyber Security Services
550 Airport Road SE, Suite C
Salem, OR 97301
503-378-2282

MEMORANDUM

To: All Agency Directors

CC: All Agency Chief Information Officers

From: Ben Gherezgiher, Chief Information Security Officer

Date: February 12, 2025

Subject: Blocking Access to DeepSeek AI on State Resources

Security Classification: TLP Amber – Level 2 – Restricted Security Information

---

Effective immediately, all executive branch agencies must block access to DeepSeek AI across state network resources and infrastructure due to significant security and data privacy risks.

Enforcement Actions
To implement this directive, Enterprise Information Services (EIS) will:

- Block the download of the DeepSeek AI application on all state-owned mobile devices.
- Restrict access to DeepSeek AI through multiple security points on the state network.
- This effort from the enterprise is complete.

About DeepSeek AI
DeepSeek AI is a generative artificial intelligence platform, developed in China, designed for advanced natural language processing and content generation.

This decision is based on several critical security risks associated with DeepSeek AI, including extensive data collection, government access to stored data, and significant vulnerabilities that expose users to potential exploitation.

1. Extensive Data Collection
DeepSeek AI collects a significant amount of user data, including:

- Profile information
- User input
- Technical data from user devices, including keystroke patterns and rhythms
- Usage information

2. Data Storage and Government Access
All data collected by DeepSeek AI is stored on servers hosted in the People's Republic of China. Under Chinese law, government authorities can access this data if deemed necessary. As a result, it is reasonable to assume that any data processed by DeepSeek AI is accessible to the Chinese government.

3. Security Leaks
Within its first week of public release, DeepSeek AI was found to have unsecured databases containing highly sensitive information, posing a significant risk of exploitation by threat actors.

4. Independent Security Assessments
Multiple independent security researchers have evaluated DeepSeek AI and found severe security weaknesses, including:

- Lack of basic security defenses
- Vulnerability to prompt injection attacks, data poisoning, and output manipulation

Given these risks, agencies must comply with this directive immediately to protect state data and infrastructure. If agencies have questions regarding this requested action, please reach to the state Security Operations Center (SOC) and work with them to complete the block as needed. This will be added to the covered vendors list and enforcement will start immediately.