A **GOVERNMENT TECHNOLOGY** THOUGHT LEADERSHIP PAPER

Managing the Risks of **Shadow AI**

SPONSORED BY netskope

As artificial intelligence becomes more embedded into state and local government operations, IT leaders face growing challenges around data leakage.

Research by Netskope Threat Labs shows source code accounts for nearly half (48%) of all data policy violations via generative AI (GenAI), while regulated data makes up 23% and intellectual property accounts for 17%.[1] These numbers raise concerns about the information that employees feed into these platforms and whether proper guardrails are in place.

"The rise of shadow AI is a big challenge," says Melody Nouri, senior product marketing manager for Netskope.[2] "Even though organizations have corporate, standardized versions of these tools, a lot of people are still using their personal credentials."

Some 60% of people who access GenAI tools still use personal accounts for work activities, she notes.

Shadow AI risk isn't just about employees putting sensitive data into public AI models. Government organizations also need to consider how data is transmitted by their SaaS applications and how their software platforms teams use GenAI to build applications and agents.

"This really shows the need to understand what's happening in your organization, both on premises and in the cloud," Nouri says.

Shadow AI is likely already prevalent in your agency, agrees Dan Lohrmann, a senior fellow at the Center for Digital Government and the former CISO for the state of Michigan.

"There are AI projects in your organization happening now," Lohrmann says. "Make sure your security teams are involved in those and be part of the solution."

Balancing innovation and control

In developing AI governance to combat data leakage, i t's a good idea to avoid all-or-nothing extremes.

"Take the stance of, I'm going to fall somewhere in the middle," Nouri advises. "Maybe not enabling everything, but I'm going to enable what I deem as appropriate for my organization's risk appetite and set proper guardrails based on industry regulations and the capacity of my team."

The best way to combat unmanaged AI use is not just by enforcing those controls, but also by delivering a secure experience that's as fast and intuitive as an unmanaged one.

Designing for adaptive security

Along with establishing new governance and protocols for AI, agencies should also embrace an adaptative security architecture based on Zero-Trust principles. Rather than granting static access to an AI tool, adaptive systems evaluate each interaction based on the user's role, device, location and data sensitivity.

This approach lets organizations make granular control decisions, not just whether to allow or block access. Risks are continuously reevaluated as activity occurs. Security controls adjust dynamically, alerting the security team, adding safeguards or limiting actions.

Imagine an employee who's inadvertently switching back and forth between their personal and corporate AI accounts. If the employee starts to upload sensitive company information to their personal account, the organization could choose to block access and display a pop-up message alerting the employee of the error.

5 Steps to Strengthen AI Security

1. Assess Your Current Exposure

Inventory all AI activity across your agency, from employee use of GenAI tools to how SaaS applications may be leveraging AI.

- ☑ Who is using AI, and for what purposes?
- ☑ Are personal accounts being used for work-related tasks?
- ☑ Is any sensitive or regulated data being shared with public AI models?

2. Define Appropriate Use Cases

AI governance should start with business needs, not blanket restrictions. Work with department leaders to understand:

- ☑ What are they trying to solve or improve with AI?
- ☑ Can you enable those outcomes securely?

3. Select the Right Tools and Architecture

Rather than taking an all-or-nothing stance, adopt a tiered approach. Prioritize solutions that offer centralized visibility, policy enforcement and dynamic risk response.

- ☑ Will your agency standardize around a secure GenAI platform?
- ☑ Can approved tools be integrated with existing identity and access controls?
- ☑ Is a cloud-native or isolated on-premises solution better suited for your risk profile?

4. Establish and Enforce Smart Policies

Train staff on what's permitted and why. Create clear, accessible guidelines for safe AI usage, including:

- ☑ When and how to share sensitive data
- ☑ Which tools are approved and how to access them
- ☑ How to report suspicious activity

5. Monitor, Test and Adapt Continuously

AI usage and threats evolve quickly. So must your oversight.

- ☑ Monitor AI activity across users, platforms and devices
- ☑ Regularly test internal AI tools and workflows for security and reliability
- ☑ Adjust access, controls and alerts based on real-time risk

Governing the invisible

From personal accounts to AI-powered SaaS integrations, GenAI tools are being used across state and local agencies, often without IT's knowledge or oversight. But locking everything down isn't the answer.

Effective AI governance starts with visibility. It's grounded in real-world use cases and adapts over time. By embracing autonomous security architectures and rethinking policies to support safe, productive use of AI, government leaders can strike the balance between control and innovation.

Agencies that act now to manage the risks of shadow AI will be better positioned to unlock its full potential: faster service delivery, empowered workers and smarter, more responsive government.

1. https://www.netskope.com/resources/cloud-and-threat-reports/cloud-and-threat-report-generative-ai-2025
2. https://webinars.govtech.com/The-Public-Sector-AI-Security-Playbook%3A-Securing-AI-End-to-End-144230

This piece was written and produced by the Government Technology Content Studio, with information and input from Netskope.

Produced by Government Technology

Government Technology is about solving problems in state and local government through the smart use of technology. Government Technology is a division of e.Republic, the nation's only media and research company focused exclusively on state and local government and education.

www.govtech.com

Sponsored by Neskope

State and local agencies trust Netskope to modernize security and protect sensitive citizen data in the cloud and AI era. The Netskope One platform simplifies Zero Trust adoption, helping IT teams ensure compliance with evolving regulations while maximizing community impact. Powered by the NewEdge network—the world's largest, highest-performing security private cloud—Netskope provides real-time visibility and control over SaaS, web, and private applications. By eliminating trade-offs between resilience and speed, Netskope empowers SLED leaders to secure a distributed workforce, safely adopt GenAI, and protect vital community services without compromising performance.

www.netskope.com

ADOBESTOCK/AI GENERATED