Time Restrictions and Location Boundaries

GenAI typically restricts itself to company-provided devices and secure networks so that protected data can be secured. This method's intent is to help protect intellectual property and sensitive data from breaches that can occur easily on personal devices. An example is this; limiting access to AI tools during business hours can help minimize the risk of data exfiltration during unsupervised periods and help ensure compliance with labor regulations. (Reuters, 2024)

Usage is often confined to:

Company networks

Secure VPS

The purpose of this ensures that data transmissions are encrypted entirely. Using VPS ensures that GenAI tools are shielded from unauthorized access. Policies might also limit GenAI to work during work hours. This in turn, allows for:

Better monitoring

Reduced the risks of unauthorized access outside of supervised times.

Making sure that usage is purposeful.

Many organizations recommend that using GenAI tools only on company-provided so that they can stay in control of their environment.

1. *Ai and Wage and Hour Laws: What Employers Need to Know | Reuters*, www.reuters.com/legal/legalindustry/ai-wage-hour-laws-what-employers-need-know-2024-03-15/. Accessed 15 Apr. 2025.
2. *Securing Generative AI: Data, Compliance, and Privacy Considerations | AWS Security Blog*, aws.amazon.com/blogs/security/securing-generative-ai-data-compliance-and-privacy-considerations/. Accessed 15 Apr. 2025.
3. Grensing-Pophal, Lin. “Crafting Policies to Address the Proliferation of Generative AI.” *Welcome to SHRM*, 28 Dec. 2023, www.shrm.org/topics-tools/news/technology/crafting-policies-to-address-proliferation-generative-ai.