

Guidance for Use of Generative AI Models or Services Developed or Hosted in Countries of Concern

Introduction

AI models offer opportunities as well as risks that must be evaluated, particularly regarding data privacy, regulatory compliance, and censorship or bias. As AI adoption grows, assessing the potential implications of different models and services is critical.

Working with generative AI models developed outside the United States, particularly those developed or operated by federally designated 'Countries of Concern' with differing privacy laws or geopolitical influences, introduces elevated considerations related to data security, bias, censorship, and long-term operational impacts.

The purpose of this guidance is not to restrict use for instructional or administrative operations, research, or publication, but to provide awareness so that faculty, staff, and researchers can make informed, risk-aware decisions when selecting and using AI tools.

Scope

This guidance applies when AI systems are used with any University of Illinois System [Data Classification](#), except for Public Data. It does not supersede any regulations and/or university policies but rather provides considerations and guidance.

AI Model vs. AI Service

Understanding the distinction between an AI model and a service is critical for evaluating risk.

- **Model:** An AI that is available as an open-source model, allowing it to be downloaded, modified, and run locally on the University's own infrastructure. Operating a model in this manner enables the data to be processed internally, thereby mitigating risks associated with data transmission to external servers.
 - Example: Models from [Hugging Face](#) run locally.
- **Service:** The AI is made available online where users can interact with the model via a website, mobile application, or application programming interface (API). Utilizing a service not run locally by the university involves sending data to external (non-university controlled) servers, potentially exposing data to external access and subjecting it to foreign data regulations.
 - Examples:

- [Illinois Chat](#) (internal)
- [DeepSeek](#) (external).

Important: Even internal services may utilize models developed in Countries of Concern.

Countries of Concern

Multiple federal definitions exist. This guidance primarily references the [DOJ Countries of Concern \(28 C.F.R. Part 202.601\)](#), supplemented by CHIPS Act and export control considerations.

Common countries include China (including Hong Kong and Macau), Russia, Iran, North Korea, Venezuela and Cuba.

These lists evolve over time and should be treated as dynamic.

Data Privacy Considerations

Using an external online service poses significant data privacy risks. User data, including research information, could be transmitted to and stored on servers located outside the U.S. This raises concerns about compliance with data protection standards and potential government access.

Individuals should use approved tools, avoid non-public data in external systems, and consult IT when unsure.

Censorship, Bias, and Cultural Context

All AI models exhibit bias. Models developed in different geopolitical environments may reflect cultural norms, policy constraints, or censorship behaviors.

Research Security and Reputational Risk

Caution is advised when using AI models developed, hosted, or affiliated with Countries of Concern due to potential risks to research integrity, data security, and institutional reputation.

Future Risk and Operational Impact

It is also important to consider future risk and institutional dependency:

- U.S. sanctions, suspension, and debarment lists change frequently
- An AI model that is permissible today may become restricted in the future
- If a model is deeply embedded in research, teaching, or administrative workflows, it may be difficult or disruptive to transition away quickly should the developer later be sanctioned or debarred

Research vs. Operational Use

This guidance does not restrict academic study of foreign AI systems. However, researchers should avoid non-public data exposure and apply safeguards.

Recommended Approach

1. Use AI models and services that are offered as a university approved AI application or service
 - a. Be aware of when a university approved AI application or service may provide optional access to AI models from countries of concern.
2. If an approved university AI offering is not available, then consider these options:
 - a. Use AI models developed and hosted by U.S.-based companies (or those based in other trusted jurisdictions) that are not located in Countries of Concern.
 - b. Run open-source AI models locally on university owned infrastructure and ensure the model cannot access the internet.
 - i. Seek assistance from your IT department to ensure model is isolated.
 - c. Avoid institutional reliance on AI models developed by entities that are sanctioned, debarred, suspended, or otherwise restricted by the U.S. government.
3. Avoid non-public data exposure.
4. Evaluate partner and collaborator AI usage.
5. Consider the long-term sustainability and risk of future restrictions when evaluating AI tools, not solely their current availability or performance.

This guidance is intended to support responsible innovation while protecting our research integrity, compliance posture, and reputation.

Controls for University AI Services

When possible these recommendations should be utilized to allow the user to be aware of which model they are using.

- Default to safe models
- Display active model
- Warn when models are from Countries of Concern
- Require acknowledgment for higher-risk models



Role of IT and Support Resources

Individuals should engage IT, research security, and compliance offices early when evaluating or deploying AI solutions.

Questions or Consultation

If you have questions about the use of a particular AI model, or would like to discuss security, compliance, or reputational risk considerations related to generative AI, we encourage you to contact the appropriate University offices for guidance.

University of Illinois Chicago	University of Illinois Springfield	University of Illinois Urbana-Champaign
Research Security	Research Security	Research Security
Security & Privacy	Security & Privacy	Security & Privacy

Last Updated: June 29, 2026