AI API Key Requirements

Last Modified on 04/24/2025 2:00 pm EDT

For more details about the Information Security Office, **please visit our website**!

The Wharton School leverages AI APIs (e.g. ChatGPT Edu and Microsoft Co-Pilot) to enable advanced capabilities while adhering to information security and privacy standards. The following requirements outline the acceptable use and management of API keys by Wharton users:

Identity and Access Management (IAM)

- **Restricted Access:** ChatGPT Edu and Microsoft Co-Pilot AI API keys may only be utilized by users with active PennKeys to ensure proper authentication and authorization. Access to the API is limited to individuals who require it for their academic or professional responsibilities.

Data Management

- If a Data Use Agreement (DUA) or contract is in place, any provisions within that agreement must be followed in addition to these guidelines. DUAs, contracts, IRBs, etc. should be shared with Wharton Computing and ISO for visibility. ISO will review these DUAs/contracts to ensure that data protection contractual obligations are met.

- **Approved Storage Platforms:** All data generated or managed through the API must be stored and shared exclusively using University-approved cloud storage platforms, such as Penn Box, Dropbox, or OneDrive. Use of unauthorized storage solutions is strictly prohibited.

Data Classification Compliance

- Users must ensure that High data is not processed or stored through AI services.

- Low (public data only) and Moderate data (not involving PII or FERPA) are approved for use at Wharton. Please send these requests to infrastructure-support@wharton.upenn.edu (and cc' security@wharton.upenn.edu). ISO is available to consult on initiatives to ensure they align with Penn security and privacy policies and standards

- The use of Moderate data involving PII or FERPA must engage with Wharton Information Security Office (ISO) for a risk review of the overall initiative's data architecture and flow outside of the AI solution. While the API key can be granted prior to the completion of the risk review, the overall initiative should complete the risk review before going to production.

- Initiatives with interconnections to/from Wharton-managed systems (particularly Moderate or High systems) or leveraging data from Wharton-managed systems also require a risk review by ISO.

Incident Reporting

- **Security Concerns:** Any concerns related to information security, privacy issues, or potential misuse of AI API keys must be promptly reported to the Wharton Information Security Office at security@wharton.upenn.edu.

Additional Requirements

- **Key Management:** AI API keys must be securely stored and not embedded in public code repositories, such as GitHub.
- **Audit and Monitoring:** Users should regularly review AI API usage to identify any anomalies or unauthorized activities.
- **Decommissioning:** When an AI API key is no longer required or a user with an AI API key is no longer authorized, the key must be deactivated.

This AI API guidance does not supersede the Wharton Security and Privacy Risk Standard or any other established Penn/Wharton policies or standards). Please consult with the Information Security Office for any questions by emailing security@wharton.upenn.edu.