JOINT INFORMATION SECURITY AND PRIVACY ADVISORY

Introduction

This advisory contains guidelines that the Information Security Office and campus privacy office recommends while using the chat program ChatGPT and similar Large Language Models (LLMs). This advisory is not exhaustive but serves as the starting point if you are contemplating using ChatGPT as part of your work at UC Merced.

Background

ChatGPT is an artificial intelligence (AI) chatbot developed by OpenAI and launched in November 2022. Chat bots such as ChatGPT do help reduce the amount of typing that may be required for some jobs that have to do the same thing all the time. The problem is not how the person is using ChatGPT, but what data is being typed in and shared with the AI model vendor. There are many ethical, security and privacy concerns related to the use of ChatGPT that should be considered.

Information to include in ChatGPT

If you are not sure if you should share certain information with ChatGPT, then trust your gut and do not. **We specifically advise that you do not share sensitive institutional information classified as Protection Level 4 per UC Data Classification Standard with ChatGPT.** This information includes: Sensitive Personally Identifiable Information (PII), Social security numbers, Protected health information (PHI), notification triggering information, payment card information. Detailed information is available here.

If you have questions about the use of ChatGPT or are thinking of incorporating ChatGPT and similar AI models in your business operations, please contact the Chief information Security Officer and Campus Privacy Officer for a consultation.

Jackson Muhirwe, PHD, CISSP
Chief Information Security Officer
jackson@ucmerced.edu

Eric Kalmin
Campus Privacy Officer
ekalmin@ucmerced.edu