Dear Colleagues,

With the recent rise in popularity and increasing news coverage of **ChatGPT**, a novel Artificial Intelligence-based Chatbot tool released by OpenAI, the IT Security Team would like to share our position on using ChatGPT and the associated risks and considerations for usage. AI Chatbot technologies are still new, and free access is limited. Overwhelming demand has spawned a number of ChatGPT fakes, copycats, and even malicious web sites, plugins, and mobile apps. Please be aware that these apps claim to give free and easy access to ChatGPT while stealing your data or installing malware in the process.

Work/Personal Usage

All information submitted to a chatbot is used by OpenAI for learning and advancing the ChatGPT technology.

- **For Work:** The IT Security Team has reviewed the privacy and security practices and policies in use by ChatGPT/OpenAI and found these lacking. ***Therefore, their use is not approved for work purposes***. This means that for now, given the risks, ChatGPT is not on the approved company tools for work list.

- **For Personal Use (Company Laptop):** The use of ChatGPT or any other unsanctioned software or personal cloud storage on your Company laptop is allowed, but as per the IT Acceptable Use Policy, must be restricted to personal use. Personal usage on Company computers or networks is subject to the terms in our Company IT Software Policy and the corresponding policy for Protecting Personal Data.

- **For Personal Use (Private Laptop):** On your personal laptop/computer, we recommend using only official vendor sites, such as OpenAI, Microsoft Bing, or Google Bard web sites, to access these tools. The use of both the publicly available free version of ChatGPT 3, as well as the paid version of ChatGPT 4 via the OpenAI web site, carries a number of risks outlined below.

Risks and Considerations

Please find below a number of risks that should be taken into consideration when using ChatGPT.

- **Privacy and Confidentiality Risks:** When using such technologies, it is easy to inadvertently share confidential, sensitive, or personal information when having “conversations” with ChatGPT. Be cautious about the information you input and avoid sharing any details like names, location information, email addresses, and any personal health, financial, or other personally identifiable

information. Avoid uploading data sets or files containing any such personal or sensitive details. Always review and sanitize any files of such data before uploading to ChatGPT.

- **Accuracy and Bias Risks:** AI can get things wrong and "hallucinate" incorrect facts or generate toxic content. It has been known to confuse or make up sources and mix up or create entirely fictional personas. *Misinformation is a real risk*, since ChatGPT relies on the internet as a primary source. AI is also known to exhibit gender, ethnic, or cultural bias. Any content AI generates should be carefully fact-checked and screened before it can be used further.
- **Copyright and Legal Risks:** Since ChatGPT was trained on wide swaths of online information, users might receive and use information from the tool that is trademarked or copyrighted, or is the intellectual property of another person or entity. All information received from ChatGPT should be carefully vetted for any such information before it is used.
- **Data Privacy Regulation Risks:** It is also unclear if ChatGPT is compliant with European Union data privacy regulations (such as the GDPR) and can or should be used in those regions, resulting in recent block in Italy. Users in the European Union may need to further restrict their interactions with ChatGPT accordingly.

Microsoft 365 Copilot Program for Tools for Work

Many of the risks above go hand in hand with the initial release of any cutting-edge technology that is commonly made available to the public as part of early adoption or testing. These tools are intended for consumers to adopt for day-to-day use, but typically do not have the necessary safeguards, controls, and protections that businesses require of enterprise software. The market is, however, moving quickly to make the AI chatbot tools available to businesses. Microsoft announced on March 15 that it is rapidly working on adding ChatGPT into the Office 365 suite of tools and making sure that the business tools will meet a higher standard for privacy and data protection.

As soon as these business-grade tools are released, IT will pilot and adopt them for our work use. If you are interested in joining an early pilot of this program, please submit a "Tools for Work" Request for "Microsoft 365 Copilot" by emailing REDACTED. Following the pilot, IT Security will review its current position on business usage and provide an update to staff. If you have any questions, please feel free to contact me. Thank you for helping to keep our organization safe and secure as we assess emerging technologies.