IT Security – Use of ChatGPT

All associates are responsible for maintaining awareness of all company policies, procedures, and standards.

OpenAI recently released a new software called ChatGPT which has become a popular tool for many users, however, it poses a significant security threat. Many companies such as Amazon, Walmart, and others are banning the use of this software, for good reason. ChatGPT uses input from users to learn and continuously improve. The software does this by storing and learning from user input. If a user inputs confidential, company information, ChatGPT could use this data and output it to others using the software. This could lead to consequences such as competitors acquiring and using company information, attackers gaining a new insight to use as an attack surface, or users violating privacy laws. A privacy breach, even unintentional, could have serious implications for a user and the company.

- Employees should never put any sensitive or confidential company data into unauthorized software, including ChatGPT when using a personal or work computer.
- Confidential company information can include many things such as roadmaps, plans, user information, or company specific code. If you are unsure if the data is sensitive, ask before inputting it.
- Any unauthorized software, including free, open-source software such as ChatGPT, is currently prohibited from use on all company computers and networks.
- If you are unsure of whether a software is acceptable, please contact IT

Associates should always be conscious data they input into any software but need to be especially mindful when it comes to new software using AI or machine learning.

For more information please see https://www.cyberhaven.com/blog/4-2-of-workers-have-pasted-company-data-into-chatgpt/.

Thank you for your assistance in this matter.