SECURITY UPDATE

We want to bring to your attention an important issue regarding the use of third-party AI assistants, such as Otter.AI and Read.ai, with Zoom. While these tools can enhance productivity and convenience, they also present significant privacy and security risks that have not been vetted by our IT division.

Recommendation: We strongly advise against purchasing or using third-party AI assistants at this time. **We recommend using only the integrated Zoom AI Companion**. Please carefully consider the following concerns:

Privacy Concerns:

- **Data Exposure:** Third-party AI assistants may access and store sensitive information shared during Zoom sessions, including personal details, academic discussions, and proprietary research data. This could lead to unintended exposure of confidential information.
- **Unauthorized Data Sharing:** These AI tools may share your data with external entities without your explicit consent, potentially violating college policies and privacy regulations.
- **Lack of Control:** Users have limited control over how third-party services manage and protect their data, increasing the risk of breaches or misuse.

Security Risks:

- **Vulnerability to Attacks**: Third-party AI assistants could introduce vulnerabilities to your devices and networks, making them targets for cyber-attacks, including phishing and malware.
- **Compliance Issues:** Using unapproved AI tools may conflict with college compliance requirements, potentially resulting in penalties or legal complications.
- **Data Integrity:** There is a risk that third-party services may not maintain the integrity and security of the data they process, leading to potential data corruption or loss.

Best Practices:

- **Use Approved Tools**: Only use AI assistants (Zoom AI Companion) and other digital tools that have been approved by the college's IT division. These tools have been vetted or undergoing vetting for compliance with privacy and security standards
- **Review Privacy Policies:** Before using any third-party AI assistant, thoroughly review their privacy policy and terms of service to understand how your data will be handled.
- **Limit Sensitive Information Sharing:** Avoid sharing sensitive or confidential information through third-party AI assistants, especially during Zoom sessions.
- **Obtain Consent:** Before using any third-party tools, ensure all attendees unanimously agree to their use. If you attend an external meeting and notice a bot is being used, voice your concerns to the host.

By following these guidelines, we can work together to ensure a safer and more secure academic environment. If you have any questions or need further assistance, please contact the IT help desk.