Slack Guidelines

Last Modified on 04/24/2025 2:01 pm EDT

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

Slack is a powerful tool for workplace communication and collaboration. However, proper usage is essential to ensure professional, secure, and efficient interactions. Follow these guidelines to make the most of Slack while maintaining compliance with information security policies and workplace expectations.

Consider Slack for	Avoid Using Slack for
Quick questions and brief discussions	Long-term file storage or documentation (use Wharton-approved applications such as OneDrive, Box, Dropbox, Confluence, or approved project management tools)
Sharing links, resources, and updates	Recording formal business (record these through official systems outside of Slack)
Group brainstorming and stand-up meetings	
Informal interactions to support workplace culture	

Please remember:

Slack is not a system of record. However, Slack may extend and aggregate external systems of record to facilitate and enhance work processes and outcomes. Leverage an approved Wharton-managed application with logging and auditing capabilities for decision-making (e.g., Ticketing, Project Management, etc.).

Low (public) data is permissible in Slack. **No High data or Moderate PII/FERPA data is permissible in Slack**. The data should remain in the secure Wharton environment where the data is stored. Please provide a link (with appropriate access controls) to the system/data.

As always, please adhere to Wharton (and Penn) Information Security policies, standards, and guidelines.