Is Your Workspace Secure?

As an employee of USF or a Direct Support Organization, you may handle sensitive or confidential information while carrying out your daily tasks. Whether your workspace is on-campus or remote, it is essential to secure your workspace to prevent fraudulent access and use of sensitive or confidential information.

The Q&As below contain tips to help you maintain a secure workspace.

- Are physical documents in your workspace adequately secured?

  - Sensitive or confidential documents should be stored out of sight and secured in locked drawers or cabinets.

- Do you secure your devices when leaving your workspace unattended?

  - When you leave your workspace, always lock your devices to restrict access to information and applications.

- Is your device screen visible to others?

  - Privacy filters protect information by making it difficult for individuals nearby to see the content on your computer, laptop, tablet, or mobile device screen.

- Do you consider who can overhear your conversations?

  - If a private conversation might be overheard, move to a secure area, use headphones, and/or be mindful of speaking volume.

- Do you monitor the background of video calls?

  - Your background should not reveal sensitive or confidential information. Consider using a neutral or virtual background.

- Do you take precautions when screen sharing during video calls?

  - Close applications or documents that should not be seen by meeting participants. Share only the specific file or window rather than your entire screen.

Where can I find more information?

- [USF Regulation 5.001](): Fraud Prevention and Financial Detection
- USF Office of Internal Audit website: https://www.usf.edu/audit/

How can I report potential fraud or abuse?

- Notify your supervisor
- Contact the USF Office of Internal Audit at (813) 974-2705
- Report activities anonymously through the [EthicsPoint]() hotline at (866) 974-8411