The University of Texas at Austin
Financial and Administrative Services

Remote work & IT Security

- Use of personal computers to host university data is highly discouraged. Any employee using a personal computer to host university data is making their personally owned device subject to subpoena and open records requests. Refer to UT Austin policy on telecommuting (HOP 5-2130).

- Supervisors must ensure that all sensitive and confidential information is protected and secured when accessing information from the remote location. Refer to Information Security Office policies for most current guidance: https://security.utexas.edu/policies/irusp.

- University business conducted using university tools is in compliance with regulations and policy and is protected by contractual and other security measures not available in consumer tools. Employees are responsible for safeguarding information regardless of where, when and how they work. The UT Austin IT Security site offers a wealth of information about the security protocols that must be followed when using either personal or UT Austin computers outside of the office setting.

- Employees considering telework or remote work must consult UT Austin policies for detailed guidance on how information must be protected. See the information security standards that apply to everyone. For more information on High Risk Confidential Information, please refer to the IT Security policy.

- Threats to information security are always changing. As technology advances, approved tools will change as well. UT Austin IT security site also provides information on regular IT security enhancements. All UT Austin employees are encouraged to visit that site regularly.