circuit. A VPN can allow for secure communications in situations where the connecting device is on a shared or untrusted network (such as a hotel, airport or coffee shop WiFi network).

SECTION IV. PERSONAL DEVICES

A. U P a D i

Unless your supervisor, the Office of Human Resources or the Office of General Counsel provides different direction, personal devices may be used to conduct St. Thomas work under the following conditions:

- All personal devices used for St. Thomas work must comply with the university's Minimum Security Standards.
- Category III – Orange data and Category IV – Red Data must not be stored locally on personal devices. All Category III – Orange data and Category IV – Red data must be stored on St. Thomas devices or systems in accordance with the Data Security Classification Policy and Minimum Security Standards.
- St. Thomas may implement technical controls to limit or secure the connections of personal devices to St. Thomas systems with Category III – Orange data and Category IV – Red data in order to limit the possibility of local data storage, data breaches and other security incidents.
- Any St. Thomas data stored on personal devices must be permanently deleted from the device before the device is transferred to another person, sold or otherwise disposed of.

B. S P a D i

To ensure appropriate management of institutional resources, St. Thomas can only provide a limited level of support for personal devices, primarily to support the connection to St. Thomas systems and applications. In order to receive support for a personal device used for remote work, the device must meet the St. Thomas minimum technology standards. In addition:

- Users are responsible for the support, repair and replacement of personal devices should they become unusable, damaged, lost or stolen.
- Users should back up their personal data to a reliable, secure location. St. Thomas is not responsible for the loss of any personal data on personal devices.

SECTION V. REMOTE WORK

A. R W T R i

Authorization for remote work is subject to other applicable St. Thomas policies. If you are authorized for remote work, you must comply with the following requirements when conducting remote work, regardless of whether the remote work is short-term or long-term:

- All St. Thomas policies governing data management, data security and information technology apply on the same basis as if the work was not remote. This includes requirements to properly secure all data, including both digital and paper records.
- Users are expected to use a secure, private Internet network. If a secure, private network is not available, users must use the St. Thomas VPN.

- Users are responsible for procuring reliable Internet service. St. Thomas is not responsible for providing a network used in the process of conducting remote work, other than the St. Thomas VPN.
- Users should follow recommended best practices for remote work from specific work location types.
- The cost and approval to procure remote work technologies beyond the standard hardware and software provided to St. Thomas employees or volunteers will be the responsibility of the user or department. Any additional technologies procured beyond the defined standard must comply with the university's minimum security requirements.

B. S R W T i

Newly assigned technology or lease-replaced technology will normally be shipped to St. Thomas and not to a remote work location. However, once inventoried by St. Thomas, technology can be shipped to a remote work location verified by the Office of Human Resources at the expense of the employee's department.

Innovation and Technology Services will provide remote support for remote work technologies where practicable. However, users may be required to bring St. Thomas devices to campus for repair if remote support or repair is not efficient or possible.