Personal Device and Remote Work Technology Policy

Policy number: 121
Policy owner: Chief Information Security Officer

Date of initial publication: December 19, 2022
Date of latest revision: N/A

SECTION I. PURPOSE

The purpose of this policy is to establish the expectations around the use of personal devices to perform work for St. Thomas and the use of technologies to perform work remotely for St. Thomas.

SECTION II. SCOPE AND APPLICABILITY

This policy governs all use of personal devices for St. Thomas work, and all use of technologies to perform remote work for St. Thomas. This policy applies to all St. Thomas employees (faculty, staff and student workers), students, contractors, volunteers, visitors and licensees who use, access or have access to St. Thomas information technology resources, whether individually controlled, shared, stand-alone or networked.

SECTION III. DEFINITIONS

a. ***Category III – Orange data*** means data classified as Category III – Orange Data in the St. Thomas Data Security Classification Policy.

b. ***Category IV – Red data*** means data classified as Category IV – Red Data in the St. Thomas Data Security Classification Policy.

c. ***Data*** means all information, recorded in any format, that is collected, created, generated, held, legally filed, owned, received, shared or stored by St. Thomas, or that St. Thomas is obligated to maintain or manage in accordance with applicable law, an accreditation requirement, a membership requirement, or an agreement. Data can exist in any tangible format including but not limited to electronic and physical documents and communications, film and print graphics, and audio and video recordings. Data does not include personal papers, personal communications and private materials made or received by St. Thomas employees, volunteers or contractors outside of their St. Thomas role and responsibilities.

d. ***Off-site*** means not on St. Thomas property.

e. ***Personal device*** means a computer, laptop, tablet, smart phone or similar device that is not owned by St. Thomas, regardless of whether the device is managed or partially managed by St. Thomas.

f. ***Remote work*** means work conducted offsite for the benefit of St. Thomas, or using St. Thomas systems, by a St. Thomas employee, contractor or volunteer, including but not limited to work from home or while traveling.

g. ***St. Thomas device*** means a computer, laptop, tablet, smart phone or similar device that is owned and managed by St. Thomas.

h. ***St. Thomas work*** means work conducted for the benefit of St. Thomas, or using St. Thomas systems.

i. ***Virtual Private Network (VPN)*** – Technology that allows a device to connect with another system or network in a secure manner as if the connections were on a private, dedicated 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. Use of Personal Devices

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. Support for Personal Devices

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. Remote Work Technology Requirements

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. Support for Remote Work Technologies

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.