Workstation Administrator Access

To protect St. Thomas' computing and information assets, ITS Information Security in consultation with the University Technology Advisory Committee and the Information Security Council has implemented a University-wide Workstation Administrator Access policy. If you have questions about administrative permissions on your computer; please refer to policy below, contact your Tommie Tech Services or the TechDesk at techdesk@stthomas.edu.

SECTION I. PURPOSE

Managing and limiting administrator access on enterprise workstations is identified as one of the most effective ways to reduce the risk of cyber security incidents and data loss from endpoint and workstations.

This policy defines the terms and situations in which university employees can be granted administrator privileges to workstations in order to complete their work, including but not limited to academic research.

Running a system as an administrator allows a person to install software and modify system files, intentionally or unintentionally. Unmanaged, this situation can easily lead to an increase in frequency and severity of virus or malware infections, unlicensed software being installed on university systems, and increased support time by ITS staff in fixing or reimaging modified workstations.

This policy aims to address the security concerns of administrator level access while providing mechanisms to assure that members of the St. Thomas community are able to complete their work efficiently and effectively.

SECTION II. SCOPE AND APPLICABILITY

This policy is applicable to:

- Employees (faculty, staff, student employees)
- Contractors
- Licensees
- Volunteers

This policy applies to university-owned Workstations (as defined below) and does not apply to personally owned computers and devices.

SECTION III. DEFINITIONS

Administrator Access or Administrator Account – Elevated privileges on a system such as “Workstation Admin” or “Root” which allows a user to install software, change system files, and otherwise make significant system changes on a workstation that could compromise the security of the system.

Least Privilege Required – Security concept that users should only be granted the minimum level of access required to complete their job duties.

University Workstation – University-owned desktop and laptop computers and university-managed systems and devices, including both hardware and software.

Users – Faculty, staff, students and other individuals authorized to maintain university accounts or otherwise access University Workstations.

SECTION IV. Administrator Access

1. Users will be set up and run as a standard user and will not be granted an Administrator Account or Administrator Access to University Workstation(s), unless the user has a legitimate business need for Administrative Access related to the performance of the user’s job responsibilities. The grant of Administrative Access requires approval by the Information Security Officer or designee.
2. Administrator Access may be granted on a temporary or continued basis, depending on business needs. In all cases, Administrator Access will be granted on a Least Privilege Required basis.
3. Administrator Accounts will be subject to the following conditions:
    1. The user agrees to terms and conditions of use designated by the university.
    2. The user’s immediate supervisor and the President’s Cabinet member with the most direct responsibility for the user agree to the business or academic need for the Administrator Account and to the terms and conditions of its use.

SECTION V. Auditing and Logging

1. The use of Administrator Accounts is subject to audit by authorized university personnel.

APPENDIX

Use Case for Administrator Access	ITS Remote or Onsite Service	Temporary Administrator Access	Secondary Administrator Account
Standard UST Faculty or Staff	●		
Historical or Legacy Administrator Access	●		
Travel with UST Laptop - Occasional	●	●	
Business Need to Install or Update Non-Standard UST Software Occasionally	●	●	
Install Personal Home Printer on UST Laptop	●	●	
Travel with UST Laptop - Frequent	●	●	●
Business Need to Install or Update Non-Standard UST Software Frequently	●	●	●
Business Critical Application Requires Admin Access to Run		●	●

REQUESTING WORKSTATION ADMINISTRATOR ACCESS

If you have a business or academic need for recurring workstation administrator access to your computer please fill out this form to request a secondary account with elevated privileges.

- Under *Request Type* choose Information Security > Security Policy and Compliance
- In the *Question, Comment, or Request* box please be sure to include a description of the business need

Note: All requests are subject to review and approval by the University's Chief Information Security Officer and the requestor's Dean or Vice President.