University Computer Administrator Access Standard

Purpose

This standard sets forth the conditions, acceptance, and remediation steps, if necessary, for granting administrator access and other access with elevated privileges on university-owned systems, both endpoints and servers, or on any system that is handling high- or moderate-risk university data.

Administrative privileges on modern operating systems grant users complete control over most functions and features of the operating system and applications. Inappropriate use of elevated privileges by an authorized user or unauthorized third party can cause detrimental effects ranging from the widespread exposure of sensitive information stored on a system to compromising the performance and security of much or all the university's network and computing environment.

Following this standard and the instructions outlined below will reduce the security risks associated with administrative privileges and will also help the user conform to Virginia Tech's information technology policies and information technology standards. This process ensures that those with elevated privileges are actively complying with training and security protocols for the management and use of these resources.

Scope

This standard applies to anyone using a computer/laptop (Windows, Mac or Linux) machine or server supplied or owned by the university. For the purposes of this document, the word "*machine*" refers to any university-owned system, including endpoints (computers, laptops, etc.), servers, or any system that is handling high- or moderate-risk university data.

Access to any end-user or server operating system account which provides an elevated capability to impact the performance, proper operation, or security of an operating system, or which allows the creation, modification, or deletion of user accounts or medium-risk or high-risk university data in bulk beyond the capabilities of the default access level for most users of that system.

To avoid duplication of effort, other processes that provide assurances for vetting, approval, and training requirements for elevated access may satisfy and substitute for this standard at the discretion of the IT Security Officer. Elevated access strictly for the purpose of requests, approvals, or other managed workflows are NOT in scope.

Standard

Anyone wishing to have administrator privileges on university-owned machine(s) must request such access and be approved by the appropriate departmental authority in advance of utilizing such privileges.

Procedure to obtain local administrator access:

1. Fill out the appropriate ServiceNow Request Item and list each machine for which you are requesting administrator access or other elevated privileges.

2. Complete the appropriate checklist (low, medium, or high-risk endpoint or server) in the Request Item based on the Minimum Security Standards indicating the appropriate training has been completed.
3. Administrator computer account/access requests must be reviewed by departmental IT staff and approved by the appropriate department head or dean.

Appropriate use of administrator accounts and access:

- Administrator computer access accounts will be assigned to, and may only be used by, one specific user who will be designated as the owner of the account. Per the Acceptable Use Policy, the user is solely responsible for all activities performed as an Administrator, and any consequences of those actions.
- Administrator computer accounts should only be used for the duration of time necessary to perform administrative duties. **At all other times, standard user accounts must be used.**
- All software installed on university-owned computers must be properly licensed, including any open-source software.
- All users, including those with administrative privileges, must adhere to all federal and state laws and regulations and to all university policies and standards, paying particular attention to copyright.
- The user must not create any unauthorized administrator accounts on the machine.
- The user must not delete or modify any user accounts created by their unit's IT support organization on the machine or permanently uninstall, disable, or modify any software designed to protect the system that has been installed by their unit’s IT support organization without prior permission.
- The user agrees that all actions performed on university systems are subject to all IT policies and standards.

Enforcement in cases of misuse or abuse of administrator access:

Misuse or abuse of administrator access will result in the revocation of administrator credentials. The university may take disciplinary action as prescribed in the Honor Codes, the Student Code of Conduct, and Human Resources policies and procedures.

Definitions

Computer administrator/ administrative access: An administrator is someone whose account credentials allows them to make changes on a computer/ server that will affect other users of the resource. Administrators can change security settings, install software and hardware, access all files on the computer, and make changes to other user accounts.

References

Policy 7000: https://policies.vt.edu/7000.pdf
Policy 7010: http://www.policies.vt.edu/7010.pdf
Policy 7035: https://policies.vt.edu/assets/7035.pdf
Policy 3015: https://policies.vt.edu/assets/3015.pdf
20 Critical Security Controls: https://security.vt.edu/policies/critical_security_controls.html

Minimum Security Standards: https://it.vt.edu/content/dam/it_vt_edu/policies/Minimum-Security-Standards.pdf
Standard for Information Technology Logging:
https://it.vt.edu/content/dam/it_vt_edu/policies/Standard_for_Information_Technology_Logging.pdf
Division of IT policies and standards:
https://it.vt.edu/content/it_vt_edu/en/resources/policies.html

Maintenance of Standard

The IT Security Office is responsible for this IT standard. Questions may be directed to security@vt.edu.

Revisions

Version 2 of draft published January 12, 2022 clarified the wording in the first bullet on page 2 with regard to ownership and use of administrator accounts.