RESOLUTION
Franklin College Faculty Senate, The University of Georgia (UGA)

To voice our objection to the draft computer administrative access policy written by the Office of Information Technology

The Senate rejects the administrative access policy as outlined by current documents submitted and calls for new policy development started as a collaborative process with the Franklin Senate faculty. The implementation of the current proposed policy should be suspended and administrative access returned to faculty.

THE UNIVERSITY OF GEORGIA
Franklin College
of Arts and Sciences

Administrative Access Policy

Definition

Administrative accounts are special accounts that exist for the exclusive purpose of computer administration tasks such as installation, configuration, and maintenance. Depending on the operating system, this special account may be referred to as “administrator” or “root.” The ability to conduct computer administration activities is restricted because these activities can adversely affect the performance, security, and usability of computer resources. Conducting day-to-day activities such as interacting with software or maintaining files with user-level access is considered best practice. Administrative accounts should only be used to conduct computer administration activities, not day-to-day activities. Most faculty, staff, and students can conduct all required activities with user-level access.

Purpose

In an effort to reduce the risk of infection by computer viruses or other malware, and to increase both the reliability and availability of hardware and software throughout the college, the Franklin College Office of Information Technology adopted the practice of setting up and running all IT devices with user-level access rights.

Retaining administrative access rights helps ensure compliance with software licensing agreements and relevant university and state policies. This practice also enables IT professionals to engage in preventive support activities, manage their time effectively, and provide more predictable response and resolution times to our faculty and staff members.

Policy

By default, all IT devices with a UGA control number in the Franklin College will be setup with user-level access rights; IT professionals will perform installations and upgrades on these devices. User-level access enables most faculty, staff, and students to conduct all required activities. This policy empowers faculty and staff members to focus on their core activities and helps prevent unplanned downtime and data loss.

DRAFT

Scope

This policy applies to all faculty, staff, and students in the Franklin College of Arts and Sciences. All IT devices with a UGA control number are in scope.

Accountability

Campus-wide IT policies, standards, and guidelines apply to all faculty, staff and students; visit http://eits.uga.edu/access_and_security/infosec/pols_regs to review these documents.

Responsibility for information technology infrastructure and services lies with IT professionals. Franklin IT professionals are responsible for incident management in the college. Incidents range from malware infections to exposure of sensitive or protected data such as grades, social security numbers, or credit card numbers. Nearly all faculty and staff computers have access to sensitive data, and the administrative access policy helps prevent security issues and incidents.

Exception Process

Some faculty members engage in tasks that may require administrator access, and we developed an exception process to accommodate their unique needs.

Faculty with unique needs may request an exception to the administrative access policy by submitting the exception request form. {We will insert a link to the form as soon as available.}

Additional Information

Questions about this policy may be directed to fcoit-feedback@franklin.uga.edu.

DRAFT

THE UNIVERSITY OF GEORGIA
Franklin OIT

Administrative Access Policy – Exception Process

Administrative Access Policy Overview

According to the Franklin College Administrative Access Policy <hyperlink>, all IT devices with a UGA control number will be setup with user-level access rights. However, some faculty and staff have unique circumstances that warrant an exception to this policy. To accommodate these limited cases, we developed the following exception process.

Purpose

Responsibility for IT infrastructure, services, and security rests with the IT professionals in the college. IT professionals receive training on the prevention and resolution of security incidents. Delegating this responsibility to non-IT personnel necessitates a formal exception process. The purpose of the process is to 1) grant exceptions equitably across all units, 2) document who received an exception, and 3) establish clear accountability for security incidents.

Scope

Exceptions can be requested by faculty and staff. Exceptions for graduate students will only be considered if the student is employed by the department. Undergraduate students will not be eligible for exceptions.

Process for Requesting an Exception

1. Consult with your local IT Professional about your particular needs or concerns. In many cases, your local IT Professional can recommend a strategy that will address your needs without necessitating an exception.
2. If your IT Professional cannot accommodate your needs without granting an exception, confirm that you have the support of your unit head and accept responsibility for any potential security incidents on devices that you administer.
3. Fill out the exception request form, obtain signatures, and submit to the Franklin College Office of Information Technology.

Exception requests will be considered during the academic year, August through April. Complete requests will be reviewed within 30 days of receipt; incomplete requests will be returned.

DRAFT

Administrative Access Policy – Exception Request Form

Expectations

Please read each of the following statements and initial to indicate your agreement.

- ___ I agree to abide by apply all campus-wide IT policies and standards published at http://eits.uga.edu/access_and_security/infosec/pols_regs.
- ___ I understand that the occurrence of security issues or incidents will result in the loss of administrative access for up to one year.
- ___ I acknowledge that receiving an exception will result in a lower service level from Franklin OIT since I will be handling updates and installations on computers that I administer. Franklin OIT will assign a medium priority to my requests including requests for incident mitigation, and OIT will respond during regular business hours as resources allow.

Exception Information

Requester

Name: [text field] Unit: [text field]

Email: [text field] Title: [text field]

[check box] I attached a detailed description of the ongoing activities that merit an exception to the administrative access policy. Please limit your response to one page maximum.

How long do you anticipate needing this access? [text field]

By signing this, I certify that I have read, initialed, and understand everything contained in the expectations section.

Signature: Date: [text field]

Unit Head

My signature indicates that the activities of the requester merit an exception to this policy.

Name: [text field] Signature: Date: [text field]

Submission

Please deliver completed forms to 224 Old College or email to fcoit-feedback@franklin.uga.edu.

DRAFT