Senate Reference No. 22-26

MEMORANDUM

TO: Fort Wayne Senate

FROM: Erika Mann, Chair
Academic Computing and Information Technology Advisory Subcommittee

DATE: March 23, 2023

SUBJ: PFW Information Technology Services Policy on Local Administrative Rights

The Academic Computing and Information Technology Advisory Subcommittee (ACITAS) received the attached statement from PFW Information Technology Services (ITS) regarding a change to the assignment of local administrative rights. ACITAS has approved dissemination of this document because of the importance of communicating to all faculty this change of policy. ACITAS will continue discussing this document and will advise PFW ITS on developing a monitored and efficient system by which to meet effectively faculty requirements related to local administrative rights, software installation, access to necessary resources, and other needs affected by this change in policy.

The committee does not require any action from Senate regarding this document at this time.

Approved	**Opposed**	**Abstention**	**Absent**	**Non-Voting**
John Buteyn		(Xiaokai) Katie Jia	Ryan McCombs	
Rama Cousik		Scott Vitz		
Jaiyanth Daniel				
Shannon Johnson				
Sarah LeBlanc				
Erika Mann				
Dawn Moore				
Heather Tierney				
Gouping Wang				

Change to Assignment of Local Administrative Rights at Purdue University Fort Wayne

BACKGROUND

In the past, PFW assigned local administrative rights to all faculty and staff who used university-owned computers. These rights provide users with the ability to freely install or uninstall any software, modify or disable settings, etc. on their computers, in essence, granting them total control over their computers. This total control makes it convenient for the users; however, at the same time, it makes the computer and the organization more vulnerable to malicious cyberattacks. If a user's account with local administrative rights is compromised, the damage a hacker can do is significant, considerably more than if a standard account (without local administrative rights) is compromised. Potential damages may include the following:

- Severe financial loss
- Blemished brand reputation
- Loss of intellectual property
- Credential theft
- Widespread interruption to university operations (downtime to critical systems, etc.)
- Etc.

In the wake of exponential growth in cyberattacks year after year within organizations of higher education, and considering the potentially devastating costs attached to successful breaches, PFW has made changes to how local administrative rights are assigned.

MANDATE FROM PURDUE SYSTEMS SECURITY

The decision to change how PFW assigns local administrative rights was handed down from the centralized security level, the Purdue Systems Security group (PSS), to reduce risk of system compromise.

DETAILS OF THE CHANGE

Most university faculty and staff do not need local administrative rights on their devices, so, per security best practices, it is assumed that all end users do not need local administrative rights. Under this assumption, all new computers are built without local administrative rights and when existing computers are re-built, it is done without local administrative rights. In the past, the default was that everyone received local administrative rights; now, the default is that no one receives local administrative rights.

Of course, some faculty and staff do need local administrative rights on their devices to effectively function within their jobs, so exceptions to the practice detailed above can be made. To request a local administrative rights exception, an end user will need to contact the IT Services Help Desk to open up a ticket. After a ticket is opened, representatives from IT Services will review the request and work with the requester to gather information and to ensure access to necessary resources is granted (see Mitch Davidson's Statement below for specifics). If facilitating access to necessary resources can be conveniently accomplished in other ways (packaging and deploying via Software

Center, remotely connecting to end users' computers to install software, etc.), local administrative rights will not be granted.

PERCEPTION OF THE CHANGE

This change should not be seen as a denial of access to resources that PFW faculty and staff need. Instead, it should be seen as an alternate route to travel for PFW faculty and staff to gain access to the resources they need, for the sake of security. PFW faculty and staff will continue to have access to all of the resources they need to perform their duties. Most will be fine with a standard account; some will need elevated access. Yes, this change does carry with it some inconvenience, as do other implemented security measures such as Multi-Factor Authentication, but the benefits to the individual and to the university far outweigh the inconvenience.

STATEMENT FROM MITCH DAVIDSON, ASSOCIATE VICE CHANCELLOR AND CIO

Mitch Davidson wrote the following as a detailed response to a local administrative rights question during a formal security audit:

Purdue University Fort Wayne Information Technology Services is committed to limiting the number of end users we allow to have administrative rights on their respective computers.

All end users, per security best practices, are assumed to not need administrative rights on computers, either permanent or temporary. If an end user requests administrative rights, a technical representative of PFW IT Services is assigned to work with that user to chaperone whatever process the end user believes requires administrative rights, by elevation, and when the task is completed, those rights are rescinded.

In the case where it is determined that an end user requires administrative rights for an extended period of time, unsupervised, we have implemented a procedure that requires an end user who requests extended administrative rights to be vetted by me. I then consult with appropriate ITS staff to determine necessity and what our options are.

If it's determined the end user requires extended administrative rights, a record of that approval is created. A separate Active Directory account is then created and assigned to that user, usually taking the form of username-LA, where username is the end users' regular Active Directory account. This has been the case, for example, with Engineering Technology and Computer Science faculty who are frequently (i.e. daily) performing tasks that require local admin access to specific systems. To not provide it would impact their ability to perform their position duties, or it would require so much assistance from ITS as to make it overly burdensome for all parties.

On computers running the Windows operating system, the -LA account is then associated via Active Directory Group Policy Object (GPO) to the Active Directory computer name that admin rights have been requested for. The end user is then educated on the use of the -LA account, including elevating privileges when prompted. A similar process, again using the assigned -LA account, is employed via PFW's Jamf Cloud device management software for Apple Macintosh computers.

Systems have been and are being encrypted as time and resources allow and is standard on all new hardware implementations.