Requesting Elevated Privileges on Comanaged Systems in Physics and Astronomy

Physics Elevated Privileges

1. Key Contacts

Spencer Wikert, Kris Thompson and Brad Carson

2. Applicability

Physics faculty members, postdocs, grad students and research scientists or anyone else needing elevated privileges for Windows and/or Mac PCs.

3. Policy Purpose and Description

Provide a mechanism to grant elevated access privileges for managed Windows and Mac systems.

4. Definitions

Elevated privileges – an account capable of performing administrative tasks.

Comanaged – a Windows or Mac system manage by ITS on which a user or group has elevated privileges. ITS patches and manages the system via Group Policy, but the user or group may install custom software with their elevated account.

5. Procedure

The user will complete the workflow acknowledging they understand the elevated privileges expectations. The local IT support person will request a service ID from Identity and Access Management group. The local IT support person will then enable the requested service ID on the computer(s).

6. Forms

Include a hyperlink to any forms related to the policy.
No link yet – this policy is in draft. This form contains a signature line below and can be used until the online workflow form is ready.

7. Frequently Asked Questions

None at this time

8. Related Information

Elevated Privileges Expectations:

There can only be one entity responsible for system security. By requesting elevated privileges, the user understands they are now responsible for the security of the host and for responding to any security incidents on the host.

Do not remove any of the core management applications (Windows SCCM, JAMF, FireEye, service accounts, etc). Removing any of these applications or reloading your system with your own version of the operating system will put your system in a fully self managed state in which you become responsible for the following:

- Compliance with the Core Security Standards — be sure to read the “Applications and Server” tabs on this page.
- Compliance with U of I Institutional Data Policy which covers backups and data classification among other items.
- Compliance with U of I Acceptable Use Policy.

Only use the elevated access account/privileges on an as needed basis.

Software installation must follow the Security Policy which states: All technology must be reviewed via the campus Technology Review Process prior to acquisition. Ask your local IT provider if you’re not familiar with this process.

Don’t save data onto the local storage as it is not backed up and will be lost when the host is reimaged or due to hardware failures or implement backups of the data in compliance with UI Backup and Recovery policy.

On-going break/fix support:

Support staff will work with the user to determine the best path forward. Generally, 60 minutes of effort will be made to fix issues. Failure to resolve the issue in a timely matter will result in the host being re-loaded. Any user installed
software/customizations will be restored by the user that requested elevated privileges.

Critical updates/patches shall be applied within 5 days, normal patches within 30 days.

Only use actively supported operating systems. Systems with unsupported or outdated OS may not be directly connected to the campus network.

If you suspect you have a security issue with the host, contact the Information Security and Policy Office (5-6332) and the local IT support person immediately, before doing anything else on the host.

User has read and agrees to Elevated Privileges Expectations

Signature __________________________ date __________

Printed Name ______________________________________

(use signature until workflow form is ready)

**Responsible Party**

(Office owner of policy/procedure)

CLAS Technology Services

**Revision History**

Draft 3, 12/16/19

Final / Draft 4 1/15/2020

**Keywords**

Admin administrator elevated privileges