I. Title: UMKC Computer Administrative Privileges Policy

In keeping with the university's mission, Information Services (IS) is committed to providing a secure and stable computing environment to facilitate teaching, research and learning. As such, IS has adopted of practice of granting User privileges as a standard on University computers. This practice, supported by the UM Security Policy has helped to increase employee productivity and kept University data safe.

II. Policy Statement

By default, all members of the university community using campus-owned computers are granted the "User" access level on their individual workstations. Information Services' staff will provide local computer "Administrator" privileges when it has been determined that there is a valid business case for the same. Administrative privilege requests must be submitted to IS via a formal request process (See section **IV** below). These requests will be reviewed on a case-by-case basis.

The Principle of Least Privilege. All University employees should use the least set of privileges necessary to operate their computers. By adhering to this principle, we limit the damage that can result from a poorly written application, viruses, malware, an accident or error.

III. Reason for Policy:

- To follow recommended security practices from leading cyber security advisors.
- To reduce software/freeware downloads infected with malware/spyware and protect university data.
- To reduce the risk of widespread computer infection.
- To reduce the risk of compromised data, which, if breached, has the potential to have serious negative implications for the institution.
- To increase general employee productivity through use of computers not affected by spyware/malware.
- To increase technical staff productivity by staying in a proactive mode of operation rather than reactive.
- To limit the software installation on university-owned machines to appropriately reviewed and licensed software.

IV. Exceptions process:

IS recognizes that there will be some exceptions to this policy. For instance, research machines may require elevated permissions.

To request Administrative Privileges please follow this process:

1. Employee should fill out the Administrative Privilege request form, including the following information:
    a. Contact Information (Name, User ID, Phone, Email)
    b. Contact Information of Supervisor/Chair (Name, User ID, Phone, Email)
    c. Computer Name (Example: KC-DEPT-ABC1234)
    d. Business case for increased rights (Example: Discipline specific research software will only work using an Administrator Account)
2. All UM Security training must be completed prior to IS providing elevated privileges.

3. The request will be sent to the Campus Information Security (CISO) officer for review. The CISO will be in contact with the employee and supervisor if any issues arise. The CISO will route a document to the employee and supervisor for signature.
4. If the Administrator Privileges request is approved, IS will make the necessary changes to the computer.

V. Related Documents, Forms, Policies

https://www.umkc.edu/IS/policies/Computer%20Usage.asp

http://www.umsystem.edu/ums/rules/collected_rules/facilities/ch110/110.005_acceptable_use_policy

https://www.more.net/service-policies

VI. Authority for Policy is the UMKC CIO. Policy Last Updated: May 2019.