College of Agricultural Sciences --- Least Privileged User Account Mode Policy: ITP-010

1.0 Purpose

The purpose of this policy is to set the standard level of privileges that will be granted to all User Accounts in the College of Ag Sciences. It also defines the Exception process to be followed when this policy cannot be implemented to support a users specialized needs.

2.0 Scope

This policy applies to all university-owned computers (operating in the college's domain and accessing the Colleges Resources) University-owned computers are defined as any computer acquired using university general funds or grant funds administered through the university, regardless of the physical location of the computer.

3.0 Policy

Standard account creation for users in the College of Ag Sciences will be created in the least privileged user account (LUA) mode. These accounts will be used to authenticate and access services and resources in the domains that are supported by the College of Ag Sciences. These accounts by default will NOT have administrative level privileges to the computers that are used by their respective users. Simply stated, these accounts will not be placed into the "Local Administrative Group" on their computers.

4.0 Policy Exceptions

- Exceptions to this standard will be considered for the following circumstances, but is not limited to, faculty or staff who:
  - connect to certain equipment or devices that cannot, within reason, be upgraded or replaced to the modern versions not requiring administrative access to operate;
  - frequently test or use new software;
  - frequent travel needs that require specific setting changes.
- The exception process will include:
  - Completion of the *Request for Elevated Privileges form* which will document:
    - the justification / specialized user need for the exception
    - the endorsement / approval of the user's Department Head
    - the responsibly assumed by the user being granted the elevated privilege
  - Thorough analysis of the request for elevated privileges is required. Ag IT will investigate and determine if the need can be accomplished in a more secure manner without granting elevated privileges. Alternatives may include temporary elevation of privileges, reconfiguration of the software to function without administrative rights or other workarounds that allow the user to accomplish their work with permanent elevated privileges. This process may take up to 5 business days to accomplish and may require the user's time/support to determine the correct course of action.

- The approving authority for user account elevated privileges will be the IT Director for the College of Ag Sciences. A designated proxy may be assigned in a prolonged absence or emergency situation.

- If a user is granted elevated privileges, they assume the following responsibilities when accepting the Administrative level access. They must agree to:

  - only use the account that has elevated privileges when absolutely necessary to accomplish a certain task and should NOT use it to login to the domain for normal daily operations. In almost all cases, this account can be used in a "Run As" manner.

  - change the password for this account annually

  - random audits of the account usage

  - only install business related software that has been legally purchased and licensed. You must be accountable to provide the licensing information upon request as Ag IT has software licensing audits.

5.0 Enforcement

Anyone found violating this policy will be subject to disciplinary action by his or her Administrative unit, the College, or the University. The administrative level access can be revoked and associated cost deferred to a Department or user if:

- The user's computer is compromised as a result of user error/misuse of administrator privileges.
- The user's computer was running server services (file sharing, web services, any P2P software) without Ag IT approval.
- Ag IT Support has been called repeatedly to perform repairs on the machine that was damaged due to user error compounded by administrative access.

6.0 Supporting Documents

College policy ITP-001 Acceptable Computer Use
University policy AD11 University Policy on Confidentiality of Student Records
University policy AD19 Use of Penn State Identification Number and Social Security Number
University policy AD20 Computer and Network Security
University policy AD22 Health Insurance Portability and Accountability Act (HIPAA)
University policy AD35 University Archives and Records Management
University policy ADG02 Computer Facility Security
Operating in Least Privilege Mode White Paper - Information Technology Services (May 22, 2009)

7.0 Revision History

Last updated: 1/5/2012