Computer Administrative Rights Standard

Objective

Austin Peay State University defines the access rights granted to university office and lab computers as standard user rights and establishes within this document a process to grant and manage administrator user rights in special cases that require it.

Scope

All Austin Peay State University office and lab computers will have standard user rights granted to university employees and students using those computers. Administrator rights are reserved for employees who demonstrate the need and obtain approval to acquire elevated rights to perform system maintenance and user support on specific office and lab computers. A process to obtain administrative rights is described within this document and will be maintained and documented by the Information Technology department.

Compliance

Austin Peay State University faculty and staff who have requested and granted administrator rights on one or more office and/or lab computers must comply with this document. Questions, concerns, or suspicion of non-compliance are to be reported to the Director of Information Technology Security.

Definitions

Administrator User rights – Upon request and approval, faculty and staff may be given administrative rights to a computer or computers. This privilege level grants complete administrative access to the computer, including the ability to install hardware or software, manage local user accounts, edit the registry, and alter any system-level files or settings. This is the least secure and stable level of access for a computer.

Least User Privilege – A widely recognized principle and industry Information Technology best-practice that enhances the protection of data and functionality from faults and malicious behavior by giving a user account only those privileges which are essential to that user's work. The concept also requires that users, even those who have been granted administrator privileges, login normally with only standard user privileges to make it more difficult for malicious entities to take control of or impact computing resources and data.

Privileged Account – A second domain account provided to APSU employees who have requested and been approved for Administrative User Rights on one or more computers as part of their job requirements. This account will be the requester's username appended with sa (ex: SmithJ-sa) and will be used only when elevated privileges are needed to install software or perform other management tasks on the computer(s). This account is not to be used for logging into the user’s computer or to perform normal, daily functions where administrative access is not required.

Standard User rights - All university office and lab computers are installed with Standard User rights by default. This level of access provides sufficient access to perform normal, daily functions; it allows university employees and students the ability to use standard applications, print, access file shares, and access the Internet. This level of access does not allow altering of software or configurations which require changes to system-level files and settings. This is the most secure and stable level of access.

Standard and Process

A. Rationale

1. Access rights are assigned based on the Least User Privilege standard. For most university faculty and staff, Standard User Rights are adequate to allow use of applications and tools needed to complete work tasks in a timely fashion. Standard User Rights prevent most malicious malware and other software compromises from being installed on or damaging computers and data.

2. There are cases where faculty and staff computers will require Administrative User Rights to install, update, or configure necessary applications in one or more computers. In most of these cases, a request to the Information Technology Help Desk for assistance will adequately resolve this need. In cases where a permanent need for Administrative User Rights is needed, the faculty or staff member will be required to make a formal request for this access.

3. Students are not eligible to be granted Administrative User Rights access.

B. Process to Request Administrative User Rights

1. Administrative User Rights may be granted to faculty and staff for one or more university computers if sufficient justification can be provided related to daily job duties. The form in the Information Technology department’s Service Catalog, “Request Administrator Access” must be completed, approved by the appropriate department level officer and forwarded to the Information Technology department. The Director of ITS or delegate will review and respond.

2. If the request is approved, fulfillment of the request will be provided as described in the “Operational Process” below.

3. If the request is declined, the requesting employee may appeal the decision to his or her department level officer who will discuss the request with the Director of ITS or delegate. The employee may submit additional justification to support the appeal prior to the meeting between the department level officer and the Director of ITS or

delegate. The department level officer will notify the employee of the outcome of that discussion.

C. Responsibilities of Employees Approved for Administrative User Rights

1. Obtaining Administrative User Rights carries certain inherent responsibilities that must be understood by the approved employee. Due diligence must be taken to prevent loss of data, ensure compliance with copyright law, and mitigate potential threat of compromise. Responsibilities include:
   a. Full and sole responsibility for any data stored locally on the computer. Care must be taken against loss of any and all data.
   b. Compliance with copyright and licensing restrictions.
   c. Compliance with federal, state and local laws and regulations.
   d. Ensure that application updates for any employee installed software occurs in a timely fashion.
   e. Remain cognizant of activities that have the potential to infect and compromise the computer.

D. Operational Process

1. If approval for Administrative User Rights is granted, access will be provided with the following steps:
   a. APSU IT will create a second domain account (Privileged account) for the requestor. The account will be the requester's username appended with –sa (ex: SmithJ-sa).
   b. APSU IT will add the Privileged account as an administrator on the requested computer(s) listed on the request.
   c. APSU IT will monitor the Privileged account to ensure privileges are not abused. APSU IT will conduct periodic reviews of Privileged accounts and may revoke these rights as described in the "Revocation Process" below.
   d. The Privileged account is not to be used for everyday use. For example, the requestor is not allowed to log into the computer with the Privileged account; the account is only to be used when prompted during installs or other tasks requiring admin access. Use of the Privileged account is for specific computer management purposes before reverting back to the requestor's standard APSU account. IT staff are the exception to this specific rule; for purposes of supporting the university IT needs, IT staff granted with Admin User Rights may use the account to log into university computers to install, troubleshoot, and other IT functions as required.

E. Revocation Criteria and Process

1. Any software issues experienced on a computer managed by an APSU employee granted Administrative User Rights on that computer will be assumed to be the result of changes made by the APSU employee. Depending on the severity of any compromise or abuse, accidental or intentional, APSU IT retains the right to remove

network connectivity to the compromised computer and/or revoke the employee’s Privileged Account. Abuse, intentional or not, is defined as, but not limited to:

a. Downloading malicious software
b. Downloading unlicensed/illegal software
c. Downloading copyrighted material without permission.
d. Public exposure of Restricted and/or Private data as defined in the Information Security and Data Classification Policy (draft) policy.
e. Not adhering to APSU Information Technology policies and procedures.

2. Administrator User Rights granted to an employee may be revoked at any time by APSU IT if any of the following criteria are met:
   a. A single instance of malware is detected on any computer managed by the employee on more than one occasion.
   b. Multiple instances of malware are detected on any computer managed by the employee on any occasion.
   c. Any noncompliant (illegal, unauthorized, copyrighted) software or files are detected on any computer managed by the employee.
   d. Public exposure of Restricted or Private data is discovered on any computer managed by the employee.
   e. Employment status or position changes for the employee.
   f. Not adhering to APSU Information Technology policies and procedures.

3. The following steps will be taken for revoking an employee’s Administrator User Rights:
   a. Any created Privileged Account for the employee will be terminated, including any local data on any computer(s) associated with the Privileged Account(s).
   b. APSU IT will notify the employee, and the employee’s department level officer of the revocation.
   c. The computer(s) associated with the Privileged Account(s) may require remediation, not limited to, re-imaging the computer(s) to the configuration level prior to the employee being granted Administrator User Rights.

4. Employees who’s Administrator User Rights have been revoked, may re-apply for reacquisition of the rights after waiting a minimum of 90 days and after meeting with APSU IT to review operating system procedures and safe computing guidelines. APSU IT will recommend or deny re-application for Administrator User Rights after this review.

F. Annual Review Process

1. APSU IT will perform an annual reauthorization of Privileged Accounts. Each employee granted a Privileged Account will be requested to provide justification of continued use of the account. The appropriate department level officer must also indicate approval.

Document Maintenance

A. **Document Owner –** the Director of Information Technology Security is responsible for document content and questions, as well as document revisions.

B. **Document Approver –** the Associate Vice President and Chief Information Officer for Information Technology has document approval.

C. **Effective Date –** January 1, 2018

D. **Last Reviewed Date –**