PennState
College of Arts and Architecture

Standard User Account Mode

Version 1.2

March 6, 2016

Revisions and Controls

This section provides document control in alignment with best practices and standards.

Revision	
Document number: Consistent with standards	AAIT_POL_005
Document title: Consistent with standards	Standard User Account Mode
Document owner role: Position responsible for document/Not a group or multiple positions	Concept of Operations Manager
Document owner name: Last known assignment to position with email and telephone number	Daniel Ritter DFR11@psu.edu 863-5722
Document location: Link to file accessible to all IT personnel through document repository	https://psu.app.box.com/files/0/f/4709798646/Policies

Control				
Document revision: Cover page must match last date and revision. Start with 0.1 for drafts. Use 1.0 for first approved revision. Use 1.1, 1.2, 1.3, etc. for each subsequent minor revision. Use 2.0, 3.0, 4.0, etc. for each subsequent major revision. Contributors and approvers cannot be the same. Approval of controlled quality documentation will be completed using the change management process by submitting a change request.				
Date	**Revision**	**Description**	**Contributors**	**Approvers**
8/27/2015	1.0	Standard user account in CAA	AAIT Staff	Daniel Ritter Scott Lindsay Steve Sobotta
9/23/2015	1.1	Reviewed by AAIT Managers and Staff	AAIT Staff	Daniel Ritter Scott Lindsay Steve Sobotta
3/6/2016	1.2	Reviewed by the CAA Committee on Educational Resources, Information Systems, and Technology.	AAIT Staff	Committee on Educational Resources, Information Systems, and Technology

Contents

1 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 Arts and Architecture (hereafter, "CAA") as documented by the College of Arts and Architecture Information Technology department (hereafter, "AAIT").

2 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 Policy

Standard account creation for users in the CAA will be created in the standard user account mode. These accounts will be used to authenticate and access services and resources in the domains that are supported by the CAA. These accounts by default will never 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 (for PCs), nor have the "Administrative" control active (for Macs).

4 Policy Exceptions

Exceptions to this standard will be considered for the following circumstances, but is not limited to, faculty or staff who:

A. Connect to certain equipment or devices that cannot, within reason, be upgraded or replaced to the modern versions not requiring administrative access to operate;
B. Frequently test or use new software that is not part of the standard college image;
C. Frequent travel needs that require specific setting changes.

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

Further explanation regarding the exception process can be found in AAIT_POL_008- Request for Administrative Access.

5 Enforcement

Anyone found violating this policy may be subject to disciplinary action by his or her Administrative unit, the College, or the University.

6 Supported Documents

6.1 University Policies

University policies referenced in this document, and others related to University computing policies are available for review at http://guru.psu.edu.

6.1.1 *Administrative Policies*

- AD08 - Purchase of Advertising
- AD11 - University Policy on Confidentiality of Student Records
- AD20 - Computer and Network Security
- AD23 - Use of Institutional Data
- AD27 - Commercial Sales Activities at University Locations
- AD35 - University Archives and Records Management
- AD53 - Privacy Statement
- AD56 - Use of Group E-Mail to Communicate University Business to Employees and Students
- AD71 - Data Categorization
- ADG01 - Glossary of Computerized Data and System Terminology
- ADG02 - Computer Facility Security Guideline

6.1.2 *Other Policies*

- FN14 - Use of Tangible Assets, Equipment, Supplies, and Services
- HR60 - Access to Personnel Files
- Penn State Access Account Password Policy - http://its.psu.edu/be-safe/password-policy.html
- Penn State Minimum Security Baseline - https://wikispaces.psu.edu/pages/viewpage.action?spaceKey=minimumsecuritybaseline&title=Minimum+Security+Baseline+Home

6.2 College Policies

- AAIT_POL_001- Computer Audits
- AAIT_POL_002- Acceptable Computer Use (Standard Mode)
- AAIT_POL_003- Security and Privacy
- AAIT_POL_004- Server Configuration
- AAIT_POL_005- Standard User Account Mode
- AAIT_POL_006- User Password
- AAIT_POL_008- Request for Administrative Access
- AAIT_POL_009- Research Request for Administrative Access

6.3 Other References

1. NIST 800-118 Guide to Enterprise Password Management - http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

Appendix A: Revisions History

This table shows the changes that were made in the document revisions. The most recent document is presented at the top.

History	Effective Date
Version 1.2 Release 1. Removed the exception process and responsibilities of elevated privileges in section 4: Policy Exceptions as the information can be found in AAIT_POL_008- Request for Administrative Access. 2. Removed content from section 1: Purpose to reflect that the document no longer explains the exception process. 3. Removed content from section 5: Enforcement.	March 6, 2016
Version 1.1 Release 1. Update Penn State Shield logo on the title page. 2. Formatted document to meet ISO-9001: 2008 standards. 3. Added to section 1: "The College of Arts and Architecture (hereafter, "CAA") as documented by the College of Arts and Architecture Information Technology department (hereafter, "AAIT")." 4. Changed "College of Arts and Architecture" to "CAA" throughout the entire document. 5. Changed "Arts and Architecture Information Technology" to "AAIT" throughout the entire document. 6. Restructured and added parts to section 1. 7. Changed "NOT" to "never" in section 3. 8. Changed section 4 indent bullets to indent letters. 9. Replace the old administrative access form with the two new administrative access request forms throughout the entire document. 10. Capitalized and added periods to sections 4A1, 4A2, and 4A3. 11. Changed section 4B recommending password change from every 30 days to every 90 days. 12. Added section 4F. 13. Changed section 6 title from "Supporting Documents" to Supported Documents". 14. Added sections 6.1, 6.1.1, 6.1.2, 6.2, and 6.3. 15. Added references: AD08, AD11, AD20, AD23, AD27, AD35, AD53, AD56, AD71, ADG01, ADG02, FN14, HR60, PSU Access Account Password Policy, PSU Minimum Security Baseline, AAIT_POL_001, AAIT_POL_002, AAIT_POL_003, AAIT_POL_004, AAIT_POL_005, AAIT_POL_006, AAIT_POL_007, AAIT_POL_008, AAIT_POL_009, and NIST 800-	September 23, 2015

118 Guide to Enterprise Password Management. 16. In 4, D, changed “You must accountable” to “You must be accountable”.	
Version 1.0 Original Release	August 27, 2015

This publication is available in alternative media on request.