PennState
College of Arts and Architecture

Request for Administrative Access

Version 1.7

April 20, 2016

aait
arts and architecture information technology

Revisions and Controls

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

Revision	
Document number: Consistent with standards	AAIT_POL_008
Document title: Consistent with standards	Request for Administrative Access
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**
9/24/2015	1.0	Created by Steve Sobotta.	Steve Sobotta	Daniel Ritter Scott Lindsay Andy Schulz
10/1/2015	1.1	Reviewed by AAIT Managers based off comments added by Andy Schulz.	Daniel Ritter Scott Lindsay	Andy Schulz
3/1/2016	1.2	Reviewed by AAIT Managers based off Penn State Audit.	AAIT Staff	Daniel Ritter Scott Lindsay
3/2/2016	1.3	Reviewed by the CAA Committee on Educational Resources, Information Systems, and Technology.	AAIT Staff	Committee on Educational Resources, Information Systems, and Technology
3/14/2016	1.4	Reviewed the dean's notes with Andy Schulz.	Barbara Korner Andy Schulz Scott Lindsay Daniel Ritter	Andy Schulz
3/17/2016	1.5	Reviewed the notes provided from Keith Barry after audit.	Keith Barry	Daniel Ritter Scott Lindsay

3/23/2016	1.6	Reviewed the notes provided by Andy Schulz.	AAIT Staff	Daniel Ritter Scott Lindsay Andy Schulz
4/20/2016	1.7	Reviewed changes provided by Andy Schulz.	AAIT Staff	Daniel Ritter Scott Lindsay Andy Schulz

Contents

1 Purpose

The purpose of this document is to explain the specifics surrounding the expectations of a customer's use of an approved Administrator level login account on a computing device 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 full time and part time employees of the CAA who are in use of any university owned computing device that is configurable for user accounts that can carry administrative level privileges or permissions.

3 Policy

Pennsylvania State University policy, as well as Minimum Security Baseline Standards, state that as general practice administrative accounts are to be disallowed. This security measure is designed to prevent malicious software from altering files that only an administrator has rights to alter.

CAA complies with these policies by providing users with non-administrative-level access, and by having AAIT update systems across the network with the most current security patches.

To most effectively support users, AAIT provides support services such as remote assistance and processing updates to machines across the network. The AAIT help desk is capable of providing remote assistance to perform necessary installation, configuration, and update tasks, even over wireless networks that are not associated with Penn State.

In addition, specialized software can be provided to allow administrative access for specific pieces of software, thereby eliminating the need for account-level administrative access. AAIT can also install special software to provide necessary local administrative access for software that is not part of the standard software image.

While these services and actions meet the needs of the vast majority of users, there are circumstances in which is it appropriate and necessary to grant administrative access. Penn State policies make provision for an administrative account provided that its use is limited to those functions that actually require administrative privileges. Such administrative accounts are established for a specific length of time, and then disabled when no longer necessary.

Therefore, if after consulting with the AAIT Director or his/her designate, it is deemed that network updates, software specific administrative access for installation and other assistance from the AAIT Help Desk are not sufficient to perform assigned duties, users may request temporary local administrative access using the form below. After gaining department head approval, the request will be reviewed and a temporary administrative account will be configured for a set time frame.

AAIT will review all local administrative accounts on an annual basis, and disable any such accounts that, after consultation with the user, are deemed no longer necessary.

4 Agreement

I am requesting to have a special account created on my AAIT supported computer to allow for local administrative access. By signing this agreement, I acknowledge the following:

I agree that violating the points outlined in sections 1, 2, and 3 outlined below will result in removal of local administrative access immediately and temporarily until reviewed by the Director of IT:

1. If the computer to which I have local administrative access is repeatedly discovered in an insecure state by AAIT or ITS/TNS in accordance with published University and College policies, the machine will be taken off of the network and reimaged.
2. Installing software that is not work related or has negative effects to the College network, such as peer to peer networking packages. You may be expected to provide alternative solutions that can be done by contacting AAIT to formulate a plan.
3. Allowing any other user to access my local administrator account.

In addition, I agree that by signing, I acknowledge and agree to the following:

A. Having AAIT install and configure all of my software does not fully satisfy my work-related needs.
B. Having AAIT install and configure a special software program that will provide local administrative access for individual programs does not fully satisfy my work-related needs.
C. I will use normal support channels (AAIT Help Desk) for installing and configuring software when possible.
D. I understand that a complete PII (personally identifiable information) scan of all hard drives must be complete and remediated prior to receiving local administrative access.
E. I will NOT use the administrative access account to log in to the network for normal daily operations.
F. I will not install software that will potentially cause a security breach.
G. I will not modify any of the security settings established by AAIT.
H. I will not alter or change the user name or computer name established by AAIT.
I. I will not remove any network administrator accounts or software established by AAIT.
J. I will not use this computer to serve out information or configure it to act as a server in any fashion.
K. I agree to install only free software or software that is fully and properly licensed to the College of Arts and Architecture or Pennsylvania State University.
L. If the computer becomes unusable, or is infected by viruses due to software issues, AAIT will attempt to backup my locally stored data, and reformat and reinstall their standard software image. I will be responsible for installing any other custom programs.
M. I understand that the ability to perform software installations and configurations poses some risks that the installed software and any data stored on the machine could be compromised by malware.
N. I will ensure that if it is necessary to install an application under the local administrative login, I will configure the application to run as a normal (non-administrative) user.

O. I understand it is not acceptable to install software that can only be run with administrator privileges.
P. I agree and will abide with Pennsylvania State University Policy AD20, "Computer and Network Security" which can be found at https://guru.psu.edu/policies/AD20.html.
Q. I understand that when I am logged in as an administrator, I may not have access to my usual home directory files or preferences.
R. I may be expected to maintain a log of modifications and changes that I make to the machines while using local administrative access, and to submit the log once a month via a trouble ticket to the AAIT Help Desk.
S. I will not create accounts for other individuals to access this computer.
T. I am required to change the password for this account each semester and may be expected to do so more frequently.
U. I agree and will abide with Pennsylvania State University Policy AD71, "Data Categorization" which can be found at https://guru.psu.edu/policies/AD71.html.
V. I will maintain adherence with Pennsylvania State University Minimum Security Baseline (MSB). Exceptions which conflict with MSB may be requested must be approved through both the Pennsylvania State Office of Information Security and AAIT.
W. I agree and will abide with Pennsylvania State University Guideline FNG02, "Limited Delegation of Contract Approvals" which can be found at https://guru.psu.edu/policies/FNG02.html. I will use the guidelines provided Software Agreement Decision Tool to determine if it is permissible to accept all electronic terms and conditions of the software license without a full review by the Risk Management Office.

4.1 Agreement Form

By signing this form, I agree to these terms and hereby request local administrative access to the following workstation:

Request From Date:_____

Request To Date:_____

Penn State User ID:_____

Machine Name/Inventory Tag Number:_____

Printed User Name:_____

User Signature/Date:_____

Justification Narrative:_____

_____

_____

_____

Department Head Printed Name:_____

Department Head Signature/Date:_____

Director, AAIT: Approve/Disapprove

Director, AAIT Signature/Date:_____

PII Scan Conducted By (printed name)_____

PII Scan Conducted By (signature and date)_____

Issued Date of Administrative Access:_____

Expiration Date of Administrative Access:_____

5 Supported Documents

5.1 University Policies

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

5.1.1 *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

5.1.2 *Other Policies*

- FN14 - Use of Tangible Assets, Equipment, Supplies, and Services
- FNG02- Limited Delegation of Contract Approvals
- HR60 - Access to Personnel Files
- Penn State Access Account Password Policy
- Penn State Minimum Security Baseline

5.2 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_009- Research Request for Administrative Access

5.3 Other References

- NIST 800-118 Guide to Enterprise Password Management

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 1.7 Release 1. Modified wording in section 4 indents L, M, R, T, and V.	April 20, 2016
Version 1.6 Release 1. Modified section 3: Policy based off of input provided by Andy Schulz.	March 23, 2016
Version 1.5 Release 1. Adjusted hyperlinks in section 4 and 5.	March 17, 2016
Version 1.4 Release 1. Updated document version to 1.4 in filename, title, header/footer. 2. Moved agreement paragraph from near the end to near the top of "Section 4 Agreement". 3. Altered "A, B, and C" items in agreement paragraph to "1, 2, and 3". 4. Altered agreement paragraph wording into a more succinct version. 5. Added transition wording to the start of the alph list in "Section 4 Agreement". 6. Removed harsh wording "revoke date" in favor of "expiration date" in "Section 4.1 Agreement Form".	March 14, 2016
Version 1.3 Release 1. Changed the name "Request for Temporary Administrative Access" to "Request for Administrative Access" throughout entire document. 2. Removed "If an audit finds illegal or dangerous software installed on the workstation, the offending software will be removed by re-imaging the workstation and I will be held accountable "from section 4K. 3. Changed "I will" to "I may be expected" in section 4R. 4. Modified account password change from every 30 days to each semester in section 4T. 5. Added University reference *FNG02- Limited Delegation of Contract Approvals* to section 5.1.2.	March 2, 2016
Version 1.2 Release	March 1, 2016

6. Added indents U, V, and W to section 4: Agreement. 7. Removed blank section 5: Enforcement. 8. Changed the name “Request for Temporary Administrative Access” to “Request for Administrative Access” throughout entire document. 9. Removed “If an audit finds illegal or dangerous software installed on the workstation, the offending software will be removed by re-imaging the workstation and I will be held accountable “from section 4K. 10. Changed “I will” to “I may be expected” in section 4R. 11. Modified account password change from every 30 days to each semester in section 4T. 12. Added University reference *FNG02- Limited Delegation of Contract Approvals* to section 5.1.2.	
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. Added Section 1, 2, 5, 6, 6.1, 6.1.1, 6.1.2, 6.2, and 6.3. 7. Restructured section 3 based on comments by Andy Schulz. 8. Changed indent bullets to indent letters in section 4. 9. Removed the word “granular” in section 4B. 10. Added “of all hard drives” in section 4D. 11. Added “administrative” in section 4E. 12. Changed “acts” to “act” in section 4J. 13. Changed “may” to “will” in section 4K. 14. Removed “by offering” and “, this” in section 4M. 15. Removed “that” in section 4N. 16. Made “It is not acceptable to install software that can only be run with administrator privileges” a new indent letter in section 4. 17. Removed “acting in a fashion against the above points” in paragraph below section 4T. 18. Added “Issued Date of Administrative Access” to the Agreement Form. 19. Added “Revoke Date of Administrative Access” to the Agreement Form. 20. Added “Request From Date” to the Agreement Form.	October 1, 2015

21. Added “Request To Date” to the Agreement Form. 22. 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 800-118 Guide to Enterprise Password Management.	
Version 1.0 Original Release	September 24, 2015

This publication is available in alternative media on request.