ADMINISTRATIVE POLICY

Subject: **Information Security**	Page **1**	Policy # Version: 1.0
Title: **Administrative Computer Access Accounts**	Revision of:	Effective Date: **6/2/2015** Removal Date:

I. PURPOSE:

To control and manage the assignment, delegation and use of administrative computer access accounts. This document complements existing NUIT Policies, Guidelines, and Practices as identified in the Relevant References section below.

This policy and procedure applies to all servers and end points (e.g., workstations, laptops) within FSM, regardless of operating platform.

Failure to comply with these policies will lead to sanctions, up to and including administrative suspension of activities, loss of faculty appointment, department or unit financial penalties, or dismissal from the University.

II. POLICY STATEMENT:

1. Administrative computer access accounts must be approved prior to being configured. The procedure for requesting administrative computer access accounts and the appeal process is outlined in the Procedure Statement.

2. An administrative computer access account may be used only for the duration of time necessary to perform administrative duties. At all other times, an individually assigned standard user computer access account will be used. Administrative accounts for everyday use are not permitted.

3. Administrator computer access accounts will be assigned to the user of the account and that person will be designated as the owner of the account. The owner is accountable for all actions taken under that account, including coordinating password changes and managing access permitted by these accounts. The owner will sign an attestation agreeing to the "Use of Administrative Computer Access Accounts" as defined in the Procedure Statement below.

4. The use of administrative accounts will be monitored through system log reporting. The user's supervisor (e.g., Department Chair, Laboratory Head) will have oversight responsibility over the use of the administrator computer access account. The use and assignment of administrative computer access accounts are subject to audit.

5. Administrator computer access accounts will be revoked if it is been determined use of the account is not compliant with FSM IT (including this Policy) or Northwestern University IT Policy.

III. PROCEDURE STATEMENT:

Request Process: Administrative computer access account requests must be made through FSM IT customer support procedures by emailing requests to fsmhelp@northwestern.edu. Requests should clearly state the need, be specific to a device, and be approved by the requestor's supervisor (e.g., Department Chair, Laboratory Head).

Review Process: The FSM IT Steering Committee will review, and approve or deny all requests for administrative computer access accounts, based upon the information submitted. The FSM CISO may also act on behalf of the FSM IT Steering Committee. The following will be considered during the review process:

1. IT support provided directly by the department versus IT support provided by Central FSM IT.
2. Specialized research lab computing equipment is integrated with instruments where software levels and instrumentation are highly co-dependent for ongoing operations.
3. Specialized training and experience is required to knowledgeably support complex research technology systems.

Notification Process: An approval or denial decision will be conveyed to the requestor by the FSM CISO and the Director, IT Customer Support. Specific reason(s) for a denial will be provided. The escalation path for further consideration is to the Dean's office.

Approval will be documented with a copy of full email indicating approval and the signed user attestation. IT Customer Support will record this documentation in the customer support ticket.

Use of Administrative Computer Access Accounts:

1. Security features including configuration settings and software will not be disabled, removed or changed (e.g., disabling of encryption, removal of anti-malware software) from what is included in a standard device (desktop, laptop) image as defined and provided by Central FSM IT.

2. Device management configuration settings and software will not disabled, removed or changed (e.g., KACE).

3. All factory supplied administrative accounts must be changed immediately upon product installation and/or a maintenance cycle.

4. Passwords will be composed per the requirements of Northwestern University IT Policy.

5. Administrative computer accounts will be de-commissioned upon the owner leaving or transferring FSM employment.

6. Changes to passwords on administrative accounts will occur immediately upon personnel or responsibility changes.

7. The use and assignment of administrative computer access accounts are subject to audit. The FSM IT Steering Committee and the Dean's office will be notified if it is determined that an administrative computer access accounts is misused or its use has resulted in an incident or broad service interruption.

IV. PERSONS AFFECTED:

All FSM faculty, staff, students and trainees.

V. DEFINITIONS:

Administrative Computer Access Accounts: An administrator account is a user ID with administrative access capabilities that lets the user change security and configuration settings, add, change or delete other user accounts, install, remove and disable software and hardware, and access all files on the computer. Administrative accounts provide full control over a computer and their use can impact other network attached computers.

Standard User Computer Access Accounts: A standard user account is a user ID which allows access to personal or group files and folders, allows changes to personalize the use of your computer, and the programs and applications you are authorized to run without having the capability of inadvertently altering security or configuration settings which might affect data protection and others on the same network. Standard accounts are used for everyday computing.

VI. POLICY UPDATE SCHEDULE:

No less than every five (5) years, but more frequent updates may be conducted as required.

VII. RELEVANT REFERENCES:

Feinberg Information Technology Standards & Policies:
http://www.feinberg.northwestern.edu/it/standards-policies/index.html
NUIT Policies, Guidelines, and Practices: http://www.it.northwestern.edu/policies/
NUIT Data Access: http://www.it.northwestern.edu/policies/dataaccess.html
NUIT Use of Computers, Systems, and Networks:
http://www.it.northwestern.edu/policies/csn-use.html
NUIT Guidelines for Security and Confidentiality of Data Files:
http://www.it.northwestern.edu/policies/uccpolicy.html
NUIT Desktop Security Recommendations:
http://www.it.northwestern.edu/policies/desktop_security.html
NUIT System Administration Guides: http://www.it.northwestern.edu/policies/sysguide.html
NUIT NetID Password Overview - Password/Passphrase:
http://www.it.northwestern.edu/netid/password.html
NUIT Server Security Requirements and References:
http://www.it.northwestern.edu/policies/serversecurity.html

Subject: **Information Security**	Page **4 of 4**	Policy # Version: 1.0
Title: **Administrative Computer Access Accounts -** **User Agreement for the Use of Administrative Computer Access Accounts**	Revision of:	Effective Date: **6/2/2015** Removal Date:

The owner of an approved Administrative Computer Access Accounts agrees to the appropriate "Use of Administrative Computer Access Accounts" as defined in the Procedure Statement of the Administrative Computer Access Account Policy. The requirements for appropriate use are repeated here:

<u>Use of Administrative Computer Access Accounts</u>:
1. Security features including configuration settings and software will not be disabled, removed or changed (e.g., disabling of encryption, removal of anti-malware software) from what is included in a standard device (desktop, laptop) image as defined and provided by Central FSM IT.

2. Device management configuration settings and software will not disabled, removed or changed (e.g., KACE).

3. All factory supplied administrative accounts must be changed immediately upon product installation and/or a maintenance cycle.

4. Passwords will be composed per the requirements of Northwestern University IT Policy.

5. Administrative computer accounts will be de-commissioned upon the owner leaving or transferring FSM employment.

6. Changes to passwords on administrative accounts will occur immediately upon personnel or responsibility changes.

7. The use and assignment of administrative computer access accounts are subject to audit.
The FSM IT Steering Committee and the Dean's office will be notified if it is determined that an administrative computer access accounts is misused or its use has resulted in an incident or broad service interruption.

Signed: ______________________________________

Print Name: __________________________________

Department: __________________________________

Device Name: ________________________________

Date: ____________________________