RUTGERS
School of Arts and Sciences

Office of the Executive Dean
School of Arts and Sciences
Rutgers, The State University of New Jersey
77 Hamilton Street
New Brunswick, NJ 08901-1248

sas.rutgers.edu

p. 848-932-7896
f. 732-932-5150

RUTGERS SCHOOL OF ARTS & SCIENCES (SAS) STANDARD BUSINESS PRACTICE

Practice Name	Workstation Management & Administrative Rights Practice
Responsible Executive	SAS Executive Director of IT
Approval Authority	SAS Executive Dean
Responsible Office	SAS Information Technology Office

1. University Policies Governing the Practice

- Rutgers Acceptable Use Policy (70.1.1)
- Information Classification (70.1.2)
- Incident Management (70.1.3)
- Information Security Awareness, Training, and Education (70.1.4)
- Provisioning/Deprovisioning Policy (70.1.7)
- Audit and Monitoring (70.1.8)

2. Reason for the Business Practice

To establish the process with which systems management, monitoring, and workstation administrative rights will be handled.

3. Who should read this practice

- SAS Deans
- SAS Departmental Chairpersons
- SAS Faculty
- SAS Staff

4. Definitions

Research Staff – Staff that primarily perform research under the direction of a faculty member. This includes postdocs, fellows, GAs, Research NTTs, and other staff with the words “research” or “lab” in their title.

System – Computer system, whether it be a desktop, laptop, or other device that accesses the university network. Refers only to systems owned by the university unless otherwise noted.

5. Practice

A. System Management

Systems require appropriate and ongoing management. The SAS IT office is tasked with managing university owned systems to ensure that they operate efficiently while maintaining appropriate

security and handling security incidents. Management of systems by the end user is contingent on their adherence to best practices, including the timely update of systems and response to requests from SAS IT or OIT should an issue arise.

B. System Monitoring & Inventory

The SAS IT office is required to utilize appropriate tools to check and inventory university owned systems. This includes not only the physical inventory of the system but an appropriate and updated inventory of the installed software, software versions, software patch levels, etc. This is a requirement for all university owned systems in the SAS, even if the end user is handling the management of the system.

The following is an excerpt from the University Audit and Monitoring Policy:

> *The University has the right and obligation to audit and monitor access to its electronic information, information systems, and information technology infrastructure, some of which are protected by federal and State laws and regulations. It uses the information produced from audit and monitoring activities to protect against, anticipate, and respond to threats to the confidentiality, availability, and integrity of its information assets and to ensure that policies and programs protecting its information assets continue to be effective.*

These reports include regular data collection including, but not limited to, the list of installed software, software patch levels, lists of user accounts, rights granted to user accounts, the configuration of the systems, etc.

Details on the tools that are used to check systems, the data collected, and the reasons for that data collection will be continuously updated and maintained on the SAS IT website.

C. Administrative Rights

The granting of administrative rights to anyone other than trained SAS IT staff is strongly discouraged but there are circumstances when the needs of the individual user may require these rights.

- **Non-research Staff Administrative Rights** – Administrative rights are typically not granted to staff members. Requests for a staff member to be granted administrative rights may be submitted to the SAS IT office who will review them on a case-by-case basis and make a recommendation regarding the request to appropriate divisional or vice dean.
- **Faculty Administrative Rights** – Administrative rights will be granted to faculty upon request unless there are specific reasons why these rights should not be granted to an individual. In that case, SAS IT will forward its recommendation and the request for

administrative rights to the appropriate divisional or vice dean for a final determination regarding whether these rights will be granted.

- **Research Staff Administrative Rights** – Administrative rights on the research related system will be granted at the request of the supervising faculty member/principal investigator. As with faculty administrative rights, if SAS IT believes there is a reason why these rights should not be granted, details of their concerns will be forwarded to the appropriate divisional or vice dean for a final determination.

User Requirements

- Users who receive administrative rights are required to complete security training, expected to take no more than 90 minutes per year, that must be renewed on a schedule that will be determined by the designated academic leadership.
- The differences between operating systems necessitate that different methods be used to grant administrative rights:
    - Windows Based Systems: Administrative rights will be granted on a secondary account that will be used only for administrative purposes.
    - MacOS Based Systems: The primary account will be granted administrative rights and the user will be required to enter a password to confirm admin access for each required task.
    - Linux Based Systems: Given the multiple ways administrative rights can be handled in Linux, the method by which these rights are granted will be determined by the SAS IT Director who is responsible for the user's area.
- Administrative rights must not be used to modify the rights on any user account on the system.
- Administrative rights must not be used to create new accounts on the system that have elevated access.
- Administrative rights must not be used to limit, modify, remove, or otherwise impact the ability of the SAS IT office to access, monitor, or manage the system.
- Users agree to notify SAS IT if they will be working with particularly sensitive data so that the existing security safeguards can be reviewed and adjusted if necessary. This data is broadly given the 'Critical' and 'Restricted' designation in the Information Classification Policy.
- Users agree that failure to abide by the above conditions for receiving administrative rights will be reviewed by the appropriate divisional dean or vice dean and can result in loss of administrative rights on all systems.

SAS IT Requirements

- The SAS IT office will only deploy management tools and collect data required to ensure that the system is functioning efficiently, properly maintained, and that no security issues exist. Every effort must and will be made to ensure that no user information is included in the monitoring.

- The use of monitoring and management tools is limited to only authorized SAS IT and University OIT staff and only those staff who actively require this information to do their jobs will be authorized.
- All SAS IT staff must strictly adhere to the requirement to collect the minimum amount of information and appropriately safeguard it.
- The SAS IT office will make a list available that details the information that is being collected, the reason that information is required, and how the information will be used.
- Under no circumstances will any information that is gathered be used for any purpose other than those authorized by this practice or by university policy.
- Misuse of these tools by any staff member constitutes a violation of the University's acceptable use policy.
- A staff member's failure to comply with these requirements will result in the incident being reviewed and possible action by human resources and the Vice Dean for Administration.

D. Procedures

a. Implementation – System changes mandated by this practice will be rolled out to all systems in the School of Arts and Sciences at a pace that will be governed by resource availability in SAS IT.

b. **Support Categories –** SAS IT will support systems based on their placement in one of three categories:

i. **Fully Managed** – SAS IT will handle all aspects of systems management. Users of the systems in this category will not have administrative rights so all software installs, patches, or changes that require elevated privileges will be handled by SAS IT office staff.

ii. **Partially Managed –** Partially managed systems are those where the user has administrative rights. The key difference from a fully managed system is that the user has administrative rights that allow them to install software on their own and make changes to the system's configuration. The user will be responsible for any changes they've made and take responsibility for any negative impacts that might result. This includes possible conflicts with management tasks that are performed by SAS IT.

iii. **Monitored –** The user has decided that, in addition to administrative rights, they will also handle all maintenance and configuration of the system. The SAS IT office will not make changes to the system outside of those required to maintain the ability to appropriate monitor the system as detailed above.

c. **Controlling Updates –** Fully and Partially managed systems will be configured to leverage automatic updates from the software vendor and, when the software permits it, users will be given the option to delay non-critical updates until a more convenient time. Non-critical updates that are installed by SAS IT will be advertised in advance, so users have time to consult with SAS IT if they have concerns about an updates timing or

content. Monitored systems will be configured for automatic updates but SAS IT will not push automatic updates to these systems. It is the responsibility of the user to manage the updates on these systems and ensure that required updates are installed in a timely manner.

d. **Configuration Changes –** For Fully and Partially Managed systems, SAS IT will update critical system configuration settings when required. These changes will be limited to those required to keep the system operating and connected to the network. An example of these changes could include updates to configuration settings or security certificates that allow systems to login or connect to networked storage.

e. Requests for Administrative Rights

i. Requests for administrative rights can be submitted to the IT ticket system at any time. When a new system is being purchased the SAS IT staff member will consult with the user and determine if they would like to request administrative rights. This consultation will include an explanation of the risks that come with this elevated level of access.

ii. If the user decides against having administrative rights, the system will be configured in accordance with the Fully Managed support category.

iii. If the user decides that they would like to request administrative rights the process will proceed based on the user's role:

1. Staff - Details about the request will be forwarded to the SAS IT Executive Director for review and comment which will then be forwarded to the designated academic leadership for a final decision.
2. Faculty – The request will be reviewed by SAS IT staff to determine if there is any reason to warrant withholding administrative rights from the user. If such a reason exists, the request will be forwarded to the Executive Director of IT for review and comment which will then be forwarded to the appropriate divisional or vice dean for a final decision. If no such reason exists, administrative rights will be granted to the faculty member in accordance with this practice. The user will be further consulted regarding whether they wish the system to be Partially Managed or simply Monitored by SAS IT and the system will be placed in the category requested.

f. Administrative Rights Procedure

Once approved for administrative rights, the following procedure must be followed to grant those rights:

i. The user must complete security training unless the user has already completed the most recent version of this training.

ii. The user must sign the administrative rights agreement.

iii. The method by which rights are granted will vary based on the system and the software available at the time. As a general principle, systems will be configured so that the exercise of administrative rights requires re-authentication. When software permits granular control over administrative permissions so that individual services or software can be elevated in a controlled manner, the IT Director in the area can leverage those capabilities to allow access without additional authentication (e.g. sudo on linux).

iv. SAS IT will modify the system's grouping to ensure that it falls into the appropriate support category.

v. The system is properly inventoried in the designated system and, if the device is portable or is known to be leaving campus, appropriately signed out.

vi. The system is provided to the user.

6. Working with Confidential and Restricted Data

Appropriate handling of confidential and restricted information is critical to maintain compliance with legal and policy requirements as well as safeguarding the reputation, privacy, and confidentiality of the institution and all faculty, staff, and students.

SAS IT should be consulted about proper security practices when working with data that is classified as confidential or restricted, regardless of whether administrative rights are available.

7. Ongoing Development

The methods and practices proposed here are not standard in industry. The result is that the software that is used both for management, and on individual user systems, isn't designed to provide all the flexibility that is desired. Meeting the requirements of this practice will require SAS IT's procedures and technologies to undergo continued development as we work to maintain compliance with this practice.

Document Version History and Change Log

Date	Version	Description	Author
07/22/2023	0.1	Initial Draft	Vosseler, T.
07/26/2023	0.2	Second Draft after review and comment by SAS IT Leadership Team	Vosseler, T.
08/28/2023	0.3	Third draft after review and comment by MPS Dean and former Co-Executive Dean	Vosseler, T.
11/16/2023	1.0	Approved version distributed at Chairs Meeting	Vosseler, T.