Office of the Chief Information Officer

Self Service

KNOWLEDGE (KNOWLEDGE_SPLASH) > STAFF SUPPORT SERVICES (KB_SEARCH?SYSPARM_SEARCH=LAPS&&SYSPARM_TOPIC=STAFF SUPPORT SERVICES) > KB04087

OCIO Local Administrative Privileges Standard (LAPS)

OCIO Local Administrative Privileges Standard (LAPS)

Applies to: All Staff and Student Employees, All Consultants – Office of the Chief Information Officer
Revision Date: May 8, 2013

Version 1.1

Note: This Standard is being replaced to align with requirement "IT5.2.3 Administrative account management" of the Information Security Control Requirements (ISCR) (https://go.osu.edu/infosec-iscr), which supersedes this Standard. In the future it will be referred to as the Local Administrative Account Management Process (LAAMP), and is scheduled to be in place in May 2015.

The processes and procedures described below still generally apply and will be followed even though some portions may have changed or no longer apply. If clarification is needed, users should direct questions to itpolicy@osu.edu.

I. General Statement

The overriding goal of this Standard is to protect university resources from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and/or damage to the University's public image.

Using administrative privileges for everyday tasks such as reading e-mail or browsing the web carries an increased risk. Malicious software can take advantage of administrative privileges on a computer to jeopardize the integrity of the system, compromise data and launch attacks against other systems on the network.

For this reason it is important to refrain from using administrative access for the most risky tasks and to restrict administrative access to the tasks that truly need it.

This Standard defines how local administrative privileges will be granted and the process used for requesting, granting/denying, appealing, and revoking these privileges.

II. Scope and Applicability

This Standard is complementary to any previously implemented OSU and/or OCIO policies or standards dealing specifically with computer, network, or data access and privileges.

Local administrative privileges are granted to specific users on specific computers.

This Standard applies to all Office of the Chief Information Officer (OCIO) users, including staff and student employees and consultants that require a computer account on the OCIO network to access University resources.

The standard applies to local administrative privileges on OCIO user's general purpose computer(s) used for performing standard business tasks such as email and internet.

This standard does not apply to administrative privileges on development, test and production servers.

III. Local Administrative Privileges

No local administrative privileges are granted by default to OCIO users. LAPS Exceptions can be requested as described in Section "**IV. Exception Process**", below.

A. Eligibility

The university LAPS intentionally leaves it to the unit to determine which parts of an organization requires local administrative privileges. This allows the unit to define and apply approval criteria consistently and efficiently.

1. While it is expected that most OCIO users do not need administrative privilege when using their computers, any OCIO user may request a LAPS Exception (see Section "**IV. Exception Process**").
2. To help ensure a measure of consistency, OCIO has defined a common set of approval criteria to be applied (see Section "**IV.C Exception Criteria**").
3. To help ensure a measure of efficiency, OCIO teams can be empowered to establish default roles and then approve LAPS Exception requests for those members of their team (see Section "**IV.E Pre-Approved Default Roles**").

B. Implementation

1. Each user's name.# user account, referred to as a "standard" user account, will be excluded from the local Administrator group on all computers. Everyone in OCIO will have a standard user account; for the majority of users this will be their only account.
2. For those who need one, a LAPS Exception can be granted to have another account (e.g., name.#a) created, referred to as an "administrator" account. This administrator user account will be included in the local Administrator group on only the computer(s) required by the user to perform their job duties, and will require a strong password be maintained.

C. Use

1. All users will login with their standard user account (name.#).
2. Standard user accounts can't perform privileged operations by themselves (such as installing software and drivers, changing system-wide settings, viewing or changing other user accounts or running administrative tools). Standard user accounts must rely on an administrator to elevate their privileges. This elevation is done via the dialog box used to enter administrator credentials.
3. In OCIO, when privileged operations are needed:
    a. Staff who possess only a standard (name.#) user account can ask the OCIO Desktop Support staff to access their computer (e.g., remotely), and then provide administrator credentials to perform the task.
    b. Staff who possess an administrator (name.#a) user account can provide their administrator credentials to perform the task without assistance.
4. Any other use of administrator user account credentials (other than changing its password) will need to be reviewed in advance.

IV. Exception Process

The following LAPS Exception process will be followed if an OCIO user requires local administrative privileges.

A. Training and Awareness

Prior to requesting a LAPS Exception, all OCIO employees are required to carefully read and fully understand

1. OSU Client Computing Security Standard (http://ocio.osu.edu/KB04087)
2. OCIO Local Administrative Privileges Standard (http://ocio.osu.edu/KB04087) (this document)
3. OCIO Local Administrative Privileges Training (http://ocio.osu.edu/KB04088)

B. Exception Requests

Users may request a LAPS Exception by submitting a request through Service Now's Request Catalog, using the "Local Administrative Privileges for Desktop" item under "Client Computing Services".

C. Exception Criteria

Requests must clearly indicate why local administrative privileges are required and duration needed. A LAPS Exception will be considered based on one or more of the following specific criteria, which may be selected using the Service Now form:

1. The software required for the normal performance of the user's job does not allow non-administrative execution, or is written in such a way as it requires the user to run as an administrator on the system.
2. The user provides desktop support to other users in OCIO.
3. The user regularly operates their computer in an area not supported by OCIO Desktop Support.
4. The user regularly operates their computer at times when there is no OCIO Desktop Support available.
5. The user is not supported by OCIO Desktop Support.
6. The software required for the normal performance of the user's job cannot be managed by OCIO Desktop Support.
7. Other documented reasons for the LAPS Exception, including whether the request needs to be expedited. Urgent requests should be discussed with the user's manager in advance.

D. Approval Process

Each request will be subjected to two approvals.

1. Manager approval: Requests will be automatically routed to the user's manager for review and approval.
2. Final approval: Based on the user's role and job duties, a request approved by the user's manager will be routed to either
   a. the OCIO IT Risk Management team (typical), or
   b. another OCIO team authorized to approve these requests (see Section "**IV.E Pre-Approved Default Roles**", below)
3. The response time for the preliminary approval depends on the manager. Urgent requests should be discussed with the user's manager in advance. Following the manager's approval, final approval will be provided within five (5) business days.
4. In all cases, the user will be notified by Service Now of the reason should the LAPS Exception request be denied (see section "**H. Appeals**", below).

E. Pre-Approved Default Roles

The university LAPS allows "default" administrative privileges based on roles identified by the unit. To help ensure a measure of efficiency, OCIO's approval process accommodates default (role-based) approvals as follows:

1. OCIO's approval process grants local administrative privileges to specific users on specific computers, not to a role. This means each user, including those in a pre-approved default role, will submit a LAPS Exception request as described in this Section.
2. Pre-approved default roles, independent of the user performing the role, can be registered with OCIO Enterprise Security's Risk Management team.
3. OCIO teams can be empowered to perform Final Approvals of LAPS Exception requests for the members of their team (instead of OCIO Enterprise Security).
4. To register pre-approved default roles, contact the Associate Director of OCIO Enterprise Security IT Risk Management.

F. Enabling Local Administrative Privileges

The OCIO Desktop Support team will contact the user by phone within three business days following final approval. During the call, they will arrange a time to enable local administrative privileges which will include, but may not be limited to:

1. Remotely accessing the user's computer(s) long enough to add the privileged account (e.g., name.#a) to the local Administrator group
   a. The user will be prompted to allow remote access to the computer(s)
2. Assisting the user with setting the password for the privileged account
   a. Privileged accounts are subject to stronger password policies
   b. The user should be prepared to provide and maintain a password for the privileged account
      i. Use the same password criteria as used at my.osu.edu, except at least 15 characters in length
      ii. Significantly different from the general purpose account (e.g., name.#)
      iii. The user should take steps to guarantee the password is changed within 90 days (e.g., set up a calendar reminder)
3. Restarting the computer
4. Answering any questions the user may have regarding Standards, training, or use of the privileged account

G. Approval Duration

All requests for local administrative privileges will be granted for a maximum of one year and then reviewed on a regular (e.g., annual) basis. This review will confirm the need stated in the LAPS Exception request is still valid and the user still requires the approved access.

H. Appeals

Users whose LAPS Exception request for local administrative privileges is denied may appeal the decision to their OCIO Senior Leadership Team (SLT) director, who will review the request with the OCIO Chief Information Security Officer (CISO).

The decision from the OCIO SLT director and CISO may not be appealed.

V. Enforcement

OCIO users who knowingly do not comply with this Standard may have their account suspended, access privileges revoked, and may be subject to other penalties and disciplinary action.

A. Revocation Criteria

Local administrative privileges may be revoked for the following reasons:

1. User no longer serves in a role or has job tasks requiring local administrative privileges.
2. User no longer utilizes software requiring local administrative privileges.
3. User is involved in a data breach that is related directly to their having local administrative privileges.
4. User demonstrates unsafe practices while using local administrative privileges.
5. At the request of the user's OCIO Senior Leadership Team director.

VI. Resources

The following University IT policies, procedures and resources apply to and support this OCIO Standard:

- University Computer Security Standards (http://ocio.osu.edu/policy/standards/security/) - http://ocio.osu.edu/policy/standards/security/ (http://ocio.osu.edu/policy/standards/security/)
- University Institutional Data Policy (http://ocio.osu.edu/policy/policies/policy-on-institutional-data/) - http://ocio.osu.edu/policy/policies/policy-on-institutional-data/ (http://ocio.osu.edu/policy/policies/policy-on-institutional-data/)
- Responsible Use of University Network and Computing Resources (http://ocio.osu.edu/policy/policies/responsible-use/) - http://ocio.osu.edu/policy/policies/responsible-use/ (http://ocio.osu.edu/policy/policies/responsible-use/)
- University IT Security Training (http://ocio.osu.edu/itsecurity/training/) - http://ocio.osu.edu/itsecurity/training/ (http://ocio.osu.edu/itsecurity/training/)

Article: KB04087 **Published:** 2015-04-28 **Last modified:** 2015-04-28

Search

LAPS

Most Popular Articles

Student Advantage - Installation of Office for Windows/Mac (kb_view.do?sys_kb_id=7201ece1e86bb580d9ed797e538675e1)
my.osu.edu: Ohio State Username Password (kb_view.do?sys_kb_id=26d0638a0a0a3c260044c908cc5bbe79)
Student Advantage (kb_view.do?sys_kb_id=cfcf60d8e8e3b180d9ed797e5386755c)
OSU Wireless-Network: Configuration Utilities (kb_view.do?sys_kb_id=3fa926601cec5880b82be6a1deb96c27)
my.osu.edu: Eligibility for Ohio State Username (kb_view.do?sys_kb_id=26cf6d180a0a3c2601659b78ca55b8dc)

Share this Knowledge Base Article

ocio.osu.edu/KB04087

Email (mailto:?Subject=Link Share Tweet (https://twitter.com/intent/tweet?text=View%20Knowledge%20Base%20Article%20-%20OCIO%20Self%20Service%20Portal%20-%20https%3A%2F%2Fosuitsm.service-now.com%2Fselfservice%2Fkb_view.do%3Fsys_kb_id%3D26cf6d180a0a3c2601659b78ca55b8dc%26sysparm_search%3DKB04087) istrative Privile

Your Recent Searches

how to set up email on mobile device (kb_search.do?sysparm_search=how to set up email on mobile device), spss (kb_search.do?sysparm_search=spss), spss (kb_search.do?sysparm_search=spss), virus policy (kb_search.do?sysparm_search=virus policy), virus (kb_search.do?sysparm_search=virus)

Feedback

Was this helpful? Not rated

Yes
No
No, I need help. (get_help.do)