Carnegie Mellon

# Guidelines for Appropriate Use of Administrator Access

| Document Information | |
|---|---|
| Identifier | |
| Status | Published |
| Published | 12/01/2007 |
| Last Reviewed | 12/01/2007 |
| Last Updated | 12/01/2007 |
| Version | 1.0 |

Carnegie Mellon

## Revision History

| Version | Published | Author | Description |
|---|---|---|---|
| 1.0 | 12/01/2007 | Doug Markiewicz | Original publication |

Carnegie Mellon

## Purpose

The purpose of this Guideline is to instruct users on appropriate use of Administrator Access to Carnegie Mellon University ("University") computing and information resources and to aid in the interpretation of requirements set forth in the University Computing Policy.

## Applies To

This Guideline applies to all University system and application administrators and any other personnel who are provided with Administrator Access to University computing and information resources.

## Definitions

*Administrator Access* is defined as a level of access above that of a normal user. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. In a traditional Microsoft Windows environment, members of the Power Users, Local Administrators, Domain Administrators and Enterprise Administrators groups would all be considered to have Administrator Access. In a traditional UNIX or Linux environment, users with root level access or the ability to sudo would be considered to have Administrator Access. In an application environment, users with 'super-user' or system administrator roles and responsibilities would be considered to have Administrator Access. In theory, this guidance applies to any user account in that utilization of access rights is reserved solely for the intended business purpose.

*Non-public Information* is defined as any information that is classified as Campus-Wide Information or Restricted Information (both Moderately Sensitive and Highly Sensitive) according to the University Data and Computer Security Policy. Access to *Non-public Information* must be approved by the designated Data Owner, which is also defined in the University Data and Computer Security Policy.

## Guidelines

The University Computing Policy provides a framework for appropriate and inappropriate use of University computing and information resources. More specifically, the University Computing Policy prohibits, "Using a computer system without proper authorization granted through the University, college or department management structure." It further prohibits attempts to "...circumvent system security without the explicit permission of the owner of that system." System administrators and other University personnel with Administrator Access to computing and information resources are entrusted to use such access in an appropriate manner. The following provides high-level guidance on what constitutes appropriate and inappropriate use of Administrator Access.

*Appropriate Use of Administrator Access*

Administrator Access to University computing resources should only be used for official University business. While the University Computing Policy permits reasonable personal use of computing resources, this is restricted to non-administrative activities. Use of Administrator Access should be consistent with an individual's role or job responsibilities as prescribed by management. When an individual's role or job responsibilities change, Administrator Access should be appropriately updated or removed. In situations where it is unclear whether a particular action is appropriate, and within the scope of current job responsibilities, the situation should be discussed with management.

Carnegie Mellon

*Inappropriate Use of Administrator Access*

In addition to those activities deemed inappropriate in the University Computing Policy, the following constitute inappropriate use of Administrator Access to University computing resources unless documented and approved by management:

- Circumventing user access controls or any other formal University security controls
- Circumventing bandwidth limits or any other formal University computing controls
- Circumventing formal account activation/suspension procedures
- Circumventing formal account access change request procedures
- Circumventing any other University procedures that are in written form and/or approved by some level of management

The following constitutes inappropriate use of Administrator Access to University computing resources under any circumstances, regardless of whether there is management approval:

- Accessing Non-public Information that is outside the scope of specific job responsibilities
- Exposing or otherwise disclosing Non-public Information to unauthorized persons
- Using access to satisfy personal curiosity about an individual, system, practice, or other type of entity.

*Reporting Inappropriate Use of Administrator Access*

As stated in the University Computing Policy, any user who suspects a violation of the University Computing Policy should contact the Information Security Office at abuse@andrew.cmu.edu. This includes suspected inappropriate use of Administrator Access.

## Additional Information

If you have any questions or comments related to this Guideline, please send email to the University Information Security Office at iso@andrew.cmu.edu.

Additional information can also be found using the following resources:

- University Computing Policy
  http://www.cmu.edu/policies/documents/Computing.htm

- University Data and Computer Security Policy
  http://www.cmu.edu/policies/documents/DataSecurity.html