WAYNE STATE UNIVERSITY
COMPUTING & INFORMATION TECHNOLOGY

# Administrative Rights Access Policy

Date of Issuance: 2012-06-08

## Contents



## Purpose

The Administrative Rights Access Policy has been established to define the criteria for which Administrative Support or Local Administrative rights for a Desktop Technology Services (DeskTech) supported desktop, laptop or other end-user device may be granted, and the terms and conditions upon which rights will be granted. The granting of Administrative Rights Access to an employee/contractor of Wayne State University to a desktop, laptop, or other end-user device is a privilege only provided to individuals who require this level of access and control in order to do their jobs effectively. The goal of this policy is to describe the circumstances under which Administrative Rights Access shall be granted as these rights allow users the ability to change standard desktop configuration settings, install unlicensed software and disable other security measures, potentially creating security weaknesses in the desktop environment.

## Authority

This policy is issued pursuant to a Signed Memorandum of Understanding, which implies that the user and computer is supported by the Desktop Technology Services team in Computing and Information Technology.

### Scope

This policy applies to all individuals and organizations supported by DeskTech.

## Definitions

**Desktop Support** – Access level that allows a group of individuals unrestricted access to change the configuration of operating system level settings on a designated group of desktops, laptops, other end-user devices, or servers.

**Local Administrative Rights** – Access level that allows an individual unrestricted access to change the configuration of operating system level settings on a specific desktop, laptop, other end-user device, or server.

**Least Privilege** – The minimum resources required for a user to perform his or her official job functions.

## Policy

Computing and Information Technology (C&IT) will grant Administrative Support and Local Administrative rights, as appropriate, to those personnel who require such rights to perform their duties. C&IT will strictly adhere to the principle of "least privilege" when granting rights to computers supported by DeskTech. Rights will only be granted under the condition that they are essential for the performance of the grantee's job. Lack of adherence to all IT policies may cause revocation of these rights. C&IT will manage and track all users who require Desktop Support or Local Administrative rights. All users, other than the Administrative Support groups, requesting rights must complete the Administrative Rights Access Form (ARAF). The ARAF will be reviewed and validated for either Local Administrative access rights. Standard procedures will require a recurring review and revalidation of all access rights, at least annually, if not specified more frequently by C&IT. Personnel who have been granted administrative access rights must adhere to all IT policies.

## Responsibilities

**Desktop Support** – Desktop Support staff have total control over the operating system and files on a specific group of computers. Desktop Support staff have many of the same rights as a Domain Administrator; however, the scope of their power excludes them from being able to make domain-level changes, restricting their administrative level activities to only those specific computers on which their user account is a member of the local system's Administrators user account group. Such activities on the local computers include the ability to:

- Create, modify, and access local user accounts and local user account groups
- Create, modify, and delete any files
- Install new hardware and software
- Run applications that can modify the operating system

- Modify operating system settings (e.g. network settings, access control, file resource sharing, local firewall, services configuration, etc.)
- Access the network
- Back up the system and its files

Desktop Support staff cannot: Modify domain-level settings. Affect other users' data or desktop settings on other computers outside of their designated group.

**Local Administrative Rights** – Local Administrative Rights allow a single user total control over the operating system and files on a specific computer. The user can perform the same activities as the Desktop Support staff, but only on their assigned computer and contain the same restrictions as above.

## Requirements for Administrative Rights Granted

- Users who are granted any level of Administrative rights shall adhere to the following:
- Comply with all existing policies of Wayne State University (including the C&IT Acceptable Use Policy)
- Users will use their domain account for all routine work on their system and only use their administrative privileges when needed to install or update software
- Do not apply changes to a desktop, laptop or other end-user device that has not been assigned to the grantee
- Do not install any unauthorized, unlicensed or non-standard software
- Take all reasonable steps to ensure that the device with administrative rights is secured from malware or intrusion
- In the event of failure of the device with administrative rights, the grantee will be responsible for restoring any applications, configurations and associated data beyond what has been approved as a standard base image
- Ensure that the desktop is properly connected to the Wayne State University network so that it receives schedule software patches and upgrades
- Administrative rights can be terminated at any time

## Appendix A

### Administrative Rights Access Form

Desktop Rights Management, Administrative Rights Access Form (ARAF)

Important Information Related to Administrative Rights - PLEASE READ FIRST

WAYNE STATE UNIVERSITY
COMPUTING & INFORMATION TECHNOLOGY

This form must be completed in its entirety for each individual employee and associated individual workstation.

- Only one employee and one workstation per form.
- We recognize there are certain situations where least privilege for some employees on an individual desktop workstation requires elevated rights. These employees and the individual workstations must go thru an approval process to ensure the justification is valid. The approval process includes review from employees within their own business area as well as individuals internal to DeskTech.
- Employees who are granted administrative rights on an individual workstation, must abide by specific terms and conditions which are described in the "Administrative Rights Access Policy."

*This form is available for print or online submission at tech.wayne.edu/forms/desktech*