



## UNITED STATES PATENT AND TRADEMARK OFFICE

OFFICE OF THE CHIEF INFORMATION OFFICER

OCIO – 5001-09

### Administrative Rights Access Policy

**Date of Issuance:** May 4, 2009

**Effective Date:** May 4, 2009

**Review Date:**

#### Table of Contents

##### Section

- I. Purpose
- II. Authority
- III. Scope
- IV. Definitions
- V. Policy
- VI. Responsibilities
- VII. Effect on Other Policies
- VIII. References
- Appendix A – Administrative Rights Access Form
- Appendix B – Standard Operating Procedures (To be developed)

#### **I. Purpose**

The Administrative Rights Access policy has been established to define the criteria for which Domain Administrator, Administrative Support or Local Administrative rights for a USPTO desktop or laptop 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 the United States Patent and Trademark Office (USPTO) 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 since these rights allow users the ability to change standard desktop configuration settings, install unlicensed software and disable other security solutions, potentially creating security weaknesses in the desktop environment.

#### **II. Authority**

This policy is issued pursuant to:

- The Federal Information Security Management Act of 2002 (FISMA)
- Agency Administrative Order (AAO) 212-4, Information Technology Security
- IT Security Handbook

## ADMINISTRATIVE RIGHTS ACCESS POLICY

### III. Scope

This policy applies to individuals and organizations providing IT desktop hardware and/or software support to USPTO.

### IV. Definitions

***Domain Administrator Rights*** - access level that affords an individual elevated privileges necessary to carry out domain wide or local configuration and/or operating system level changes to any Windows based system within the domain infrastructure.

***Administrative 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 on a specific computer.

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

### V. Policy

The Office of the Chief Information Officer (OCIO) will grant Domain Administrator, Administrative Support and Local Administrative rights, as appropriate, to those personnel who require such rights to perform their duties. The OCIO will strictly adhere to the principle of “least privilege” when granting rights to desktop and laptop computers used at USPTO. 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.

The OCIO will manage and track all users who require Domain Administrator, Administrative Support or Local Administrative rights at the USPTO. 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 Domain Administrator or 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 the OCIO.

Personnel who have been granted administrative access rights must adhere to all IT policies. Penalties for failure to adhere to IT policies and procedures violation of this policy will vary depending on the nature and severity of the violation. Penalties include:

- Removal of access rights.

## ADMINISTRATIVE RIGHTS ACCESS POLICY

- Disciplinary action, including, but not limited to, reprimand, suspension and/or termination of employment.
- Civil or criminal prosecution under applicable law(s).

### VI. Responsibilities

#### A. Domain Administrators

Domain Administrators have total control over the operating system and files on all desktops, laptops, and servers across the domain. Domain Administrators are able to perform the following activities:

- Create, modify, and access domain and local user accounts and groups
- Create, modify, and delete any files
- Grant local administrative rights
- 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 a system and its files
- Claim ownership of files
- Upgrade the operating system

#### B. Administrative Support

Administrative Support staff have total control over the operating system and files on a *specific group* of computers. Administrative 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

## ADMINISTRATIVE RIGHTS ACCESS POLICY

Administrative Support staff *cannot*:

- Modify domain-level settings
- Affect other users' data or desktop settings on other computers outside of their designated group

### **C. 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 Administrative Support staff, but only on their assigned computer and contain the same restrictions as above.

### **D. 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 the USPTO.
- 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 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 USPTO network so that it receives schedule software patches and upgrades.
- Administrative rights can be terminated at any time.

### **VII. Effect on Other Policies**

This policy has no effect on other existing policies.

### **VIII. References**

- USPTO IT Security Handbook
- USPTO IT Rules of the Road
- AAO-212-4, IT Security
- Federal Information Security Management Act of 2002 (FISMA)

ADMINISTRATIVE RIGHTS ACCESS POLICY

ISSUED BY:



John B. Owens II  
Chief Information Officer  
United States Patent and Trademark Office

OFFICE OF PRIMARY INTEREST: Customer Support Services Group

ADMINISTRATIVE RIGHTS ACCESS POLICY

**Appendix A**  
**Administrative Rights Access Form**

A sample Administrative Rights Access Form is found on the following page.



## Desktop Rights Management, Administrative Rights Access Form (ARAF)

### Important Information Related to Administrative Rights - **PLEASE READ FIRST**

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

- Only one employee and one workstation per form.
- The Office of Management and Budget (OMB) Federal Mandate, Federal Desktop Core Configuration (FDCC), states that typical users must be assigned standard (or “restricted”) user rights to comply with this mandate. At the USPTO we are currently progressing towards FDCC compliance and strive for following the “Principle of Least Privilege.” In theory, this principle states the lowest set of privileges possible are to be assigned in order to accomplish any task. When this is applied to Desktop Rights Management, it positions the USPTO to have a more standardized desktop environment, increased desktop stability, increased desktop security and overall improved usability and supportability of the desktop.
- Between now and the time the USPTO is FDCC compliant, 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 OCIO.
- 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 policy can be found on the [OCIO’s IT Operations Policies](#) page.

I certify that in order to carry out my mission at the USPTO I need administrative rights on the identified computer. (Type full name here)

I certify that I have read and understand the [Administrative Rights Access Policy](#). (Type full name here)

### Employee Information

1. Government or Contract Employee
 

Government	Contractor
------------	------------
  
2. Employee Phone Number
3. Employee Requesting Administrative Rights
 

a. If employee is a Federal Government Employee, provide GS-14 or above Supervisor	b. If employee is a Contractor, provide COTR or Task Order Manager
--	--
  
4. Requesting Employee’s Business Area (Approving Authority)
 

CAO	(Colleen Sheehan)	CFO	(Greg Eslinger)
EA	(Glenn Cobb)	OCIO	(Joe Vastola)
OGC	(Mike Christensen)	Patents	(Cecelia Branch)
Trademarks	(Charlene Cameron)	Under Secretary	(Glenn Cobb)

### Required Details for Administrative Rights

5. Login ID
6. WSID
7. Asset CD#
- 8a. Location      Workspace      Madison West Development Lab      8b. Domain
9. Duration
11. Administrative Rights Justification Grouping
12. Justification Details

ADMINISTRATIVE RIGHTS ACCESS POLICY

**Appendix B**  
**Standard Operating Procedures**

[To be developed]