

## **Information Services & Technology Administrator Level Access Policy**

### **I. PURPOSE**

This document defines UMDNJ policy regarding local administrator rights to UMDNJ employees on University workstations.

University is committed to providing members of the UMDNJ community with reliable technology in a stable operating environment while appropriately addressing the University needs and maintaining University system integrity and data security.

### **II. APPLICABILITY**

This policy applies to all computer and communication devices owned or operated by UMDNJ. This policy also applies to any computer and communications device that is transmitting or receiving data traffic on the UMDNJ network. This includes, but is not limited to, devices using wireless, wired, infrared, cellular, or any other technology used to transmit and receive data within the University's Data Infrastructure. The equipment may or may not be owned by the University, and in cases of wireless technology, the device may be physically located in structures and on property not owned by UMDNJ.

### **III. ACCOUNTABILITY**

Under the President, the Senior Vice Presidents shall ensure compliance with this policy. The Vice President for Information Services and Technology (IST), the President/CEOs of the Healthcare Units, Deans and Vice Presidents shall implement this policy by means of system specific procedures, guidelines and standards.

### **IV. POLICY**

#### **A. Levels of Access**

There are two security access levels to a university owned computer:

1. User
2. Administrator.

The User access level allows most administrative controls with some restrictions. Installation of software or hardware that makes changes to the underlying operating system will require the assistance of IS&T or the local IST Technical support group. The standard User access level will generally assure the highest level of stability for your computer.

The Administrator access level allows the client to have complete and unrestricted access to the operating system. This includes the ability to install any hardware or software, edit the registry, manage the default access accounts and change file level permissions. Manipulating the configuration of these software / hardware devices may cause serious stability problems with your system and could affect the data transmission between your machine and other devices on your local network segment.

By default, all UMDNJ employees are assigned standard User access level rights on their individual workstations. Staff members that meet the following requirements can make a request to gain Administrator level access. These requests must be submitted via web registration form and accompanied by an approved authorization form signed by a Director, Dean or their designate

assignee. The head of the School or the Units local Information Technology Support staff will also be sent electronic notification of the request and will have an opportunity to submit comment about the application. Once the signed authorization form is received and acknowledged by IS&T, the Administration rights can be granted. The use of these rights and the level of access to the workstation are to be in accordance with the University Acceptable Use Policy and all applicable Security Policies. IS&T reserves the right to revoke local administrator rights if this access leads to abuse or causes problems within the Universities Data Infrastructure.

#### **B. Criteria for gaining Administrative access**

1. The device is portable, such as a laptop or PDA, and is regularly used outside the UMDNJ network.
2. The user needs privileged access to the device for the testing of software and/or hardware.

#### **C. Guidelines**

1. UMDNJ workstations are University property and are intended for University business.
2. Individuals will refrain from installing applications downloaded from the Internet or software not compatible with the workstation's operating system. Installation of the incompatible applications may damage files and expose the University's data network to virus attacks and data traffic for malicious code.
3. Individuals will refrain from installing unauthorized software as it may monopolize local processor power, resulting in noticeable system slowdown or degradation of performance.
4. Individuals will not install applications that may establish network share protocols which result in an increase in bandwidth utilization. This prevents network congestion and the degradation of performance across wide areas of the campus network.
5. Individuals should not download applications (software) that are illegal or not licensed on University owned equipment.
6. The University strongly recommends and encourages individuals to utilize IS&T, or the local support group, to install any software that is necessary on their workstation.
7. Individuals will refrain from altering or removing any standard software that was originally installed by IST or the local support group.
8. Individuals requiring administrator level access must submit a completed and signed Administrative Access Request Form and Agreement to Comply with Policies. A signed copy will be kept on file in IS&T.
9. IS&T, or the local support group, shall not troubleshoot, repair or install non-standard applications.
10. Non-standard software will be removed as part of a normal repair process if necessary to restore system functionality, as defined by the Core Services and Technology division of IS&T.
11. IS&T strongly recommends that individuals save all documents to the Network Drives. ( H, J or K ) If additional compartmentalization is required, subfolders may be created within these drives. Placing information on the H, J, K drives allows the information to be backed up by System Administrators and prevents an individual's documents from becoming lost or damaged should the local operating system become compromised and need to be reloaded.
12. All University workstations are configured with remote support software. This software allows authorized IS&T, or the local support staff to remotely control the workstation if necessary for troubleshooting.
13. IS&T, or the local support group, will not remotely access individuals' workstations for troubleshooting without the individual's approval.

V. NON-COMPLIANCE AND SANCTIONS

Any person found to have violated this policy may have their Administrators access rights revoked; be subject to denial or removal of access privileges to the University network; disciplinary action under applicable University policies and procedures up to and including termination; civil litigation; and/or civil or criminal prosecution under applicable state and federal statutes.