INFORMATION TECHNOLOGY POLICIES
Administrative Privileges for Personal Workstation(s)
COLLEGE OF ARCHITECTURE
2007-08

1. GENERAL

1.1. The nature of certain software in conjunction with the need for expeditious resolution to specific projects and problems has emphasized the need for members of the College of Architecture to be able to do certain activities on their local computers that have previously been reserved for system administrators.

1.2. While it is the preferred method to have Information Technology Services (ITS) install the software in a timely manner, ITS is fully aware that at times that may not be a viable solution.

1.3. The purpose of this document is to define responsibilities, delegation, support, and potential consequences in the granting of local administrative rights to individuals.

2. RESPONSIBILITIES

2.1. The assumption of local administrative rights on a University computer carries certain inherent responsibilities. Care must be taken due to the potential loss of data, compliance with copyright laws and potential threat of compromise.

2.2. College of Architecture members who are granted administrative rights should be aware that they would become fully and solely responsible for any data that is stored locally on the computer they are administering and as such must exercise due diligence in providing a backup mechanism to ensure against the potential loss of any data. Failure to implement a backup mechanism can result in permanent loss of any and all data.

2.3. College of Architecture members who are granted administrative rights should be aware of copyright restrictions and licenses placed on ALL software installed on their systems as well as being aware that there exists severe criminal and civil penalties for non-compliance.

2.4. College of Architecture members who are granted administrative rights should be aware that they will assume full responsibility for maintaining anti-virus software installed and current on the systems they manage. Furthermore, College of Architecture members who are granted administrative rights should be aware that something as seemingly benign as opening an email or visiting a web page has the potential to infect and compromise a computer.

3. DELEGATION

3.1. It is the understanding of the ITS that in certain circumstances, a professor or staff member may not have the sufficient amount of time to properly administer the systems themselves, for instance in the case of specialty labs.

3.2. In such circumstances where the faculty or staff member is unable to personally manage the systems, authority may be delegated to another member of the faculty's team, with the following constraints:

3.2.1. The team member must be directly involved in the project or lab they will be administering.

3.2.2. The faculty member delegating this authority is ultimately responsible for the actions of any person that has been delegated this authority.

4. SUPPORT

4.1. The unrestrictive nature of administrative accounts carries the potential to encounter unexpected and adverse consequences. Problems encountered are further complicated by the immense volume and variety of software, and it is thus impossible for an operation of any size to have a complete knowledge of it all, and therefore we may be unable to provide assistance.

4.2. Resolution to problems encountered by members who have local administrative rights will be limited to the following three solutions:

4.2.1. ITS will devote a maximum amount of time and effort NOT to exceed one hour of labor and resources.

4.2.2. Should the problem not be resolved within that allotted time, ITS will offer to re-image the system to the configuration level the system had when it was ORIGINALLY given to the faculty or staff member. The implications of this are as follows:

4.2.2.1. ITS is not responsible for any data on the system. It is the individual who assumes administrative privileges that is responsible for data as stated in section 2.2 above.

4.2.2.2. ITS will not be responsible for any software installed on the system after administrative privileges were granted.

4.2.3. Should the problem not be resolved within that allotted time, ITS will be available to recommend outside sources to assist in the resolution of the problem. Any fees associated or incurred by these outside sources will be the sole responsibility of the person possessing administrative rights to that particular machine.

5. CONSEQUENCES

5.1. The degrees of impact associated with administrative privileges are widely varied and can range from a simple error with a simple solution to catastrophic results impacting the entire College of Architecture.

5.2. Data that is not properly archived is at risk or being irretrievably lost, regardless of its significance or importance.

5.3. As mentioned in section 2.3 above, severe criminal and civil exist for improperly licensed software. Please refer to appendix B, *System Regulation 21.99.10*, and appendix C, *University Rule 21.99.10M1*, for further documentation regarding software licensing in the Texas A&M University System.

5.4. Depending on the severity of compromise, CIS has the ability to remove network connectivity to the compromised host or TO THE ENTIRE COLLEGE and has previously established precedence in this regard.

APPENDIX B

SYSTEM REGULATION

21.99.10 Use of Licensed Commercial Software

April 24, 1996
Revised September 30, 1998

1. GENERAL

1.1 Commercial computer software is protected by federal copyright laws. Only appropriately licensed software may be placed on System computing resources and/or used by System employees in the conduct of System business. The purpose of this regulation is to define the responsibilities of System employees with regard to the use of computer software protected under the Copyright Act.

1.2 Users of computer software are warned by various means against the illegal use of such software. Labels appear on packaging materials, and in some cases the warning is displayed on the computer screen when the software is used. System employees are expected to be familiar with the licenses on the software they use.

1.3 Varying degrees of copyright protection are afforded for different classes of computer software. Generally these fall into the following categories.

1.3.1 Commercial Software: This is software that is distributed under a strict licensing agreement. Typically this means that a fee is paid by the purchaser or licensee. The only legal way to obtain the right to use such software is through a purchase agreement or license with the owner of the copyright or with a licensed distributor. Site license agreements are available on some commercial software, which allow the duplication of software upon payment of a specific site license fee.

1.3.2 Shareware: Shareware typically refers to software that is available for use on a trial basis at no cost. A user who decides to continue using the software must then send a registration fee to the author or distributor of the software. There is usually a licensing agreement associated with the software and it usually appears on the screen during the login process.

1.3.3 Public Domain: This type of software is made available with no restrictions on its distribution or copying. A point of concern is that many users may assume if there is no copyright notice attached to the software, it is then in the public domain. Actually, the reverse is true: unless there is a statement to the effect that the software is in the public domain, the user should assume the author retains the copyright to the software.

2. PROHIBITED ACTS

2.1 The unauthorized use, copying, or distribution of copyrighted software is a violation of the U. S. Copyright Act. These illegal acts are commonly referred to as "software piracy." Violations include, but are not limited to, the following:

(1) making extra copies of microcomputer-based software for use on other microcomputers unless specifically allowed through a licensing agreement;

(2) putting copies on a network so that they may be copied by others;

(3) obtaining copies of software from others without paying the appropriate licensing fees; and

(4) unauthorized distribution of software by electronic mail.

2.2 It should be noted that some software is licensed so that it is allowable for the user to make a copy for home use in conjunction with the business use of the software. A user of licensed software should not assume that this provision is in place but should check with the licensing agent before making copies for other machines.

3. IMPLEMENTATION

3.1 Chief Executive Officers will implement a component rule and/or procedures to ensure that all computer software on generally accessible computing resources, on networks and on individual microcomputers belonging to their respective components and/or under their control is appropriately licensed. Such procedures should provide for regular checking of computing resources, including microcomputers, and the appropriate correction of any violations that may be discovered.

3.2 System employees are to be provided appropriately licensed copies of computer software necessary to perform their assigned tasks. Employees must not be asked nor tacitly expected to perform tasks for which appropriately licensed software has not been provided.
****

CONTACT FOR INTERPRETATION: The System Office of Information Resources

HISTORY: April 24, 1996
Section 21 Rules

APPENDIX C

UNIVERSITY RULE

21.99.10.M1 Software Licensing

Approved May 28, 2005
Revised May 30, 2006
Supplements System Regulation 21.99.10

1. GENERAL

All software installed on University owned or operated computer systems used by faculty members, staff members, agents, or students in the conduct of University business must be appropriately licensed. For software having a licensing agreement, persons installing, or authorizing the installation of software should be familiar with the terms of the agreement. Where feasible, the licensing agreement should be maintained in the department that operates the system on which the software is installed. In cases where this is not feasible, individuals or organizations should maintain sufficient documentation (e.g., End User License Agreements, purchase receipts) to validate that the software is appropriately licensed. No software may be copied or installed by any faculty member, staff member, agent, or student unless the licensing agreement specifically grants such a procedure.

For instances in which the department is the owner-custodian or custodian of the system, the department is responsible for ensuring compliance with this rule. Each department will be asked to report the status of their compliance as part of the annual Information Security Assessment, Awareness, and Compliance (ISAAC) process (refer to Rule 24.99.99.M1).

2. PENALTIES

Non-compliance with copyright laws regarding software is subject to significant civil and criminal penalties imposed by federal and state laws. These penalties are applicable to the University and/or an individual. Violation of this rule is subject to University disciplinary action as well (System Regulation 21.99.10 Use of Licensed Commercial Software; System Policy 07.01 Ethics Policy, TAMUS Employees; University Rule 33.04.99.M2 Rules for Responsible Computing).

Contact: Information Technology Issues Management of CIS

Office of Responsibility: Vice President and Associate Provost for Information Technology

Administrative Privileges for Personal Workstation(s)

Authorization to modify computer systems assigned to personal faculty or personal systems assigned to specific service unit within the College of Architecture.

1. Name (print): _____
2. Department or Unit: _____
3. Machine Asset: _____
4. Serial Number: _____
5. Computer Name: _____

In signing this authorization request, I agree to adhere to Texas A&M University computing and security regulations (TAMU SAP 21.01.99.M1.04) on the use of personal workstations. Should I choose to install software on my workstation (s), I acknowledge that I will be responsible for installing and maintaining only licensed software on these systems. Computer Services, within the College of Architecture, will be available for limited support, restricted to re-imaging for systems normally provided by the College of Architecture in the event of catastrophic loss, and updating anti-virus software installed by them. Recovery from catastrophic loss caused by software I put on my workstation (s) may require outside resources beyond the capabilities of the College's Computer Services and this may be my responsibility. Backing up critical data will be my responsibility.

I understand that I will not be given these administrative privileges if I do not sign this form. Also, I acknowledge that I may lose privileges if I abuse them or do not follow Texas A&M procedures in administering any of the computers I use or have under my control.

_____

Signature Date

APPROVAL RECOMMENDED

_____

Department Head/Manager Date

_____

Executive Associate Dean - CARC Date

*** Forward to the Dean's Office**