Preview Mode: Data entered will not be submitted.

ADMIN PRIVILEGES - RIGHTS AND RESPONSIBILITIES

GENERAL INFORMATION

Most modern computer systems operate on a principle of least privilege (https://en.wikipedia.org/wiki/Principle_of_least_privilege); this means that under normal circumstances, the computer account you use will be a *regular* or *standard* account, and not an *admin* account (or an account with escalated privileges). There are a number of reasons for this:

- **Better overall security.** When code is limited in the system-wide actions it may perform, vulnerabilities in one application cannot be used to exploit the rest of the machine. This is particularly important given the increase in malware (https://en.wikipedia.org/wiki/Malware) in our environment.
- **Better system stability.** When code is limited in the scope of changes it can make to a system, it is easier to test for its interactions with with other applications. This is important given the limited IT staff available to manage college systems.
- **Compliance with state regulations.** Texas Administrative Code, TAMU System policies, and even federal regulations govern the ways that we manage and use our computer systems here on campus. All three have rules about how admin privileges are granted and used (AC–5 (http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=AC-5); IA–2 (http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=IA-2); TAMUS–29.01.03 (http://policies.tamus.edu/29-01-03.pdf); NIST–800-53-AC-6 (https://nvd.nist.gov/800-53/Rev4/control/AC-6)).

In the College of Architecture, we use a product called CyberArk (https://www.cyberark.com) to help us manage the use of admin rights. When a task requires administrative privileges (such as installing an application, or updating a printer driver), CyberArk intercepts the action and can grant the access needed without a password from the user (this is called privilege escalation (https://en.wikipedia.org/wiki/Privilege_escalation)).

In most cases, this process happens behind the scenes and is never even noticed. In a small number of cases, CyberArk will ask for more information about the program, and submit a request that will be reviewed by Information Technology Services (ITS) staff. This happens when there is an application that is new, or if there is abnormal behavior on the computer that is suspected of being malware. **All of the common applications in use within the college are already pre-approved**, and do not require any additional approval.

In rare circumstances, there are computers that require regular access to administrative privileges. This may be due to the nature of the research or development activity on the machines. While it is best to use our normal process, it's not always practical in some situations. In these cases an individual employee may be granted administrative rights to a specific computer system.

The purpose of this policy is to define the rights and responsibilities involved in granting local administrative rights to individuals, including delegation, support, and potential consequences for misuse.

RESPONSIBILITIES

Using accounts with administrative privileges on University assets carries increased responsibility. There are additional risks associated with potential data loss, software licensing and copyright issues, and regulatory compliance:

- **Data loss.** Users with administrative rights are solely responsible for any data that is stored locally on the computer, and for providing a backup mechanism to protect against the potential data loss. Failure to implement a backup mechanism can result in permanent loss of data.

- **Computer security.** Executing code using administrative privileges is inherently risky. A seemingly benign action (such as opening an email or visiting a web page) has the potential to infect and compromise a computer because of the elevated privileges. Users with administrative rights must exercise great care in their actions while using credentials with elevated access, and agree to use the account with the minimal privileges necessary for each task (AC–5 (http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=AC-5)). To increase the security posture of accounts granted elevated privileges, the following changes are required to made to the user's normal computer account (NetID):
  - **Enable** supported two factor authentication (Duo 2FA) on the NetID account
  - **Disable** over-the-phone password resets for the NetID account
  - **Enable** self-service password resets for the NetID account

- **License compliance.** Users with administrative rights must be aware of copyright restrictions and licenses placed on all software installed on their systems (CM–11 (http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=CM-11); TAMUS–29.01.02 (http://policies.tamus.edu/29-01-02.pdf)). There are severe criminal and civil penalties for noncompliance.

- **Accessibility regulations.** State law and TAMU Rules mandate that all applications installed on university assets meet strict accessibility guidelines (TAMUS–29.01.04 (http://policies.tamus.edu/29-01-04.pdf); TAC–213.30 (https://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=). Any software you install using your administrative privileges must meet or exceed those standards.

- **Audit and compliance.** Texas A&M University System rules require that we perform annual information security risk assessments (TAMUS–29.01.03 (http://policies.tamus.edu/29-01-03.pdf)). Users with administrative rights will be required to assist college IT staff with this process in order to maintain administrative access to those systems.

DELEGATION

Sometimes in a university setting, the customer responsible for a computer system (the information resource owner (http://cio.tamu.edu/policy/glossary.php#glossary_term-58) in Texas A&M's vocabulary) is unable to personally manage the system. In these cases, authority may be delegated to another member of the resource owner's team, with the following constraints:

- The team member must be directly involved in the project or lab to which the computer system belongs.

- The resource owner delegating this authority is ultimately responsible for the actions of any person to which they delegate administrative rights.

SUPPORT

The unrestricted nature of administrative accounts creates the potential for unexpected consequences. Problems encountered can be various and complex, and since ITS will not have a complete record of administrative actions on the system, we may not be able to fully resolve issues that arise in a reasonable timeframe. Limited resources prevent the college from spending large amounts of time on a single issue.

If an issue cannot be resolved within a reasonable time, ITS will offer to restore the system to the base configuration as originally delivered to the customer. This means that:

- ITS is not responsible for any data stored locally on the system. Users with administrative rights assume responsibility for locally-stored data and ensuring that a backup mechanism exists to restore that data in accordance with TAMU data classification rules (RA–2 (http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=RA-2)).

- ITS is not responsible for restoring software installed on the system by users with administrative rights. License management and software configuration in these cases will be the responsibility of the customer.

CONSEQUENCES FOR MISUSE

Intentional misuse of computer systems is covered by University Rule 29.01.03.M2 (http://rules-saps.tamu.edu/PDFs/29.01.03.M2.pdf) and can result in disciplinary action and even criminal prosecution. Be aware that having administrative access on a system can hold you to a higher standard of conduct, because of the greater potential for harm that exists.

However, we assume that in most cases TAMU employees are trying to do the right thing. Therefore, this section addresses *un-*intentional or accidental misuse of administrative privileges. Because of the nature of administrative access, the potential exists for small actions to have dramatic effects. It is even possible that a mistake made on a single computer system can have consequences that affect the entire college:

- **Data loss.** Commands executed with administrative access may not provide the opportunity to confirm an action, and may not be reversible if a mistake is made. This makes it very easy to cause inadvertent, permanent data loss.
- **Criminal or civil penalties.** Improperly licensed software can result in criminal or civil penalties, even if the license violation was unintentional (CM–11 (http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=CM-11); TAMUS–29.01.02 (http://policies.tamus.edu/29-01-02.pdf)).
- **Loss of connectivity**. In the event of a malware-compromised computer, the Texas A&M networking group has the authority to unilaterally disconnect the compromised host from the network. In some situations, they have even isolated entire buildings from the network because of a single infected computer.
- **Loss of administrative privileges.** If the actions of user with administrative privileges creates a significant risk to the college, the administrative rights may be revoked.

ACKNOWLEDGEMENT

The college is required to maintain a list of all users with administrative or special access to computer systems, and this list must be reviewed and approved annually (AC–5 (http://cio.tamu.edu/policy/it-policy/controls-catalog/controls.php?control=AC-5)). The administrative rights granted below will expire no later than 12 months from the signature date, although they may be reviewed earlier.

By signing this form, you acknowledge that you have fully read and understand the responsibilities outlined above, and you accept the risks involved with using administrative privileges on the computer systems listed below:

Full Name

Email Address

NetID

Date

Justification

Please provide a business-case for wanting administrative privileges on your machine.

Hostname

End-User Signature

Resource Owner Signature (if delegated)

Department

Submit