5.5.4.20 LETU Office Computer Local Access Rights Policy

Policy

All LETU computers have local User rights granted to individuals using those computers. Administrator rights are reserved for departmental staff that are responsible as outlined in their job descriptions for providing administration of computing resources such as system maintenance and user support. A process to obtain an exemption to this policy will be maintained and documented by Information Technology.

Definitions

User Level
All computers are installed with User rights by default. This level of access provides a great deal of power to perform normal, daily functions; it allows faculty and staff to use standard applications, print, and access the Internet. It does not allow altering software or configurations which require changes to system-level files and settings. This is the most secure and stable level of access.

Administrator Level
Upon request and approval of exclusion from the LETU policy, faculty and staff may be given administrative rights to a computer. This privilege level grants complete administrative access to the computer, including ability to install hardware or software, manage local user accounts, edit the registry, and alter any system-level files or settings (except Group Policy configurations). This is the least secure and stable level of access for a computer. Employees who require administrative level access for job-related tasks will be asked to submit a request through their departmental Dean or Cabinet Level Officer and sign a compliance agreement stating that they will adhere to all pertinent Federal and State laws and LeTourneau University technology policies, including, but not limited to, copyright and licensing agreements.

Least User Privilege
A widely recognized principle and industry IT best-practice -- that enhances the protection of data and functionality from faults and malicious behavior -- is to give a user account only those privileges which are essential to that user’s work. The concept also requires that users, even those who have been granted Administrator privileges, login normally with only standard User privileges to make it more difficult for others to take control of computing resources. Benefits of the principle include:

- Better system security. When software is limited in the system-wide actions they may perform, vulnerabilities in one application cannot be used to exploit the rest of the computer as is the case with malware such as rootkits, spyware, and viruses.
- Better system stability. When applications are limited in the scope of changes they can make to a system, the application will not have access to perform operations that could crash a machine or adversely affect other applications running on the same computer.
- Ease of deployment and maintenance. In general, the fewer privileges an application requires the less cost to LETU to deploy and maintain.
**Rationale**

Access rights are assigned based on the standard of giving access needed to perform job-related functions. For most faculty and staff, standard **User** rights are adequate to allow use of applications and tools needed to complete work tasks in a timely fashion. **User** rights prevent many computer contaminants such as viruses, Trojan applications, and malware from being installed on computers and provide the most stable system.

Some faculty and staff use applications that require administrative rights to install, update, or configure. While giving faculty and staff local **Administrator** privileges allows them to make these system changes as necessary, it also introduces an attack vector. When computers or accounts with higher levels of administrative rights are compromised, the potential for damage to LETU is much greater. A compromise can be anything from software that harvests data from the hard drive or monitors keystrokes, to infecting the computer into a “BotNet,” which may contribute to illegal activity across State and Federal borders. Allowing individuals to install software also makes troubleshooting and diagnosing system problems difficult because there is no Change Management audit trail. For this reason, quick calls to the IT Help Desk for review/approval by a trained Technician are the best way to handle these temporary needs for elevated privileges.

This policy is based on the principle that individuals who have local **Administrator** access levels to a computer are the de facto administrators for that computer. As Administrators, users have greater control and flexibility, but also greater responsibility for their computers. Administrators are responsible for maintenance and upkeep of the changes and software installed.

**Necessary Administrator Access**

The following departmental staff require local Administrator accounts as a matter of conducting daily business:

- Information Technology
  - Business Systems Management
  - Network & Telecommunication Services
  - User Support & Engagement
    - Help Desk Team
- Instructional Design and Technology
  - Instructional Technology
Exemption

Elevated privilege, herein referred to as Exemption, may be provided as further described: Exemption from the Policy may be granted to personnel outside of Necessary Administrator Access departments if justification can be provided related to daily job duties. Approval must be given by the requesting employee’s Dean or Cabinet Level Officer, and the CIO, or a delegate of his choosing. Currently only faculty may request exemption.

Process to Request Policy Exemption
The “Office Computer Access Rights Policy Exemption” form must be completed and submitted to your Dean or Cabinet Level Officer. The Dean or Cabinet Level Officer must approve the request and forward the completed form to LETU IT. The CIO or delegate will review and respond (Approve/Decline Exemption). If Exemption is approved, fulfillment of Exemption will be provided as described in “Operational Fulfillment” section below. If Exemption is declined, and the employee disagrees with the decision by the CIO to decline the Exemption request, he/she may appeal the decision to his/her Dean or Cabinet Level Officer. The Dean or Cabinet Level Officer will discuss the issues with LETU IT and notify the requesting employee of the outcome of that discussion. The employee may, at his/her option, submit additional justification to support the appeal, prior to the meeting between the CIO and Dean/Cabinet Level Officer.

Responsibilities of Exempted Individual
Exemption carries certain inherent responsibilities. Due diligence must be taken to prevent loss of data, ensure compliance with copyright laws, and mitigate potential threat of compromise.

- Full and sole responsibility for any data that is locally stored on the computer. Take care against permanent loss of any and all data.
- Copyright and licensing restrictions.
- Ensure compliance as there are severe civil and criminal penalties for violations.
- Application updates for any software installed by the employee.
- Remain cognizant that many activities have the potential to infect and compromise the computer.

Support Ramifications
Due to the unfettered access to the computer and the changes that can be made, supportability is greatly reduced. LETU IT will devote minimum (usually an hour or less) labor/resources to troubleshooting. Should the problem not be resolved, LETU IT will offer to reimagine the computer to the configuration level the system had when it was originally given to the employee. LETU IT is not responsible for any data located solely on the computer. The Exempted individual is responsible for all data as stated in the “Responsibilities” section above.

Operational Fulfillment
If Exemption from the Policy is granted, privileged (Administrator) access will be provided in the following way:

- LETU IT will create an Administrator account on the requested computer listed on the “Office Computer Access Rights Policy Exemption” form. The account will be your LETU username appended with –x (e.g.: JoeSmith-x).
- A password will be assigned, but must be changed immediately in accordance with LETU’s Password Policy.
- Once the password has been set, the account must be maintained and managed by the Exempted individual. LETU IT will monitor local Administrator accounts to ensure privileges are not abused. LETU IT will conduct periodic review of the Exemption and may revoke such an Exemption as described in the “Review, Revocation, and Exclusions” section below.
- This Exempted account’s password must be changed every 90 days.
**Note:** Do not use the Administrator account for everyday use - for example, don’t log in with your Administrator account, only use it when prompted for installs. Use this elevated account only for specific computer management purposes before resorting back to your standard LETU account.

**Review, Revocation, and Exemptions**

Any software issues experienced on the computer will assume to be the result of changes made by the exempted individual. Degrees of impact can vary from simple errors with quick solutions to vast-reaching issues that may influence other computers or network segments. Depending on the severity of any compromise or abuse, accidental or intentional, LETU IT retains the right/ability to remove network connectivity to the compromised computer and/or revoke any previously granted exemption. Abuse, intentional or not, is defined as, but not limited to:

- Downloading malicious software
- Downloading unlicensed/illicit software
- Downloading copyrighted material without permission
- Public exposure of Confidential & Sensitive Information (CSI) as defined in the Identity Theft Policy
- Not adhering to LETU LetNet policies and procedures

**Revocation Process**

Administrator access granted through exemption may be revoked at any time by LETU IT if any of the following criteria are met:

- A single instance of malware is detected on an exempted individual’s computer on more than one occasion
- Multiple instances of malware are detected on an exempted individual’s computer on any occasion
- Any noncompliant (illegal, unauthorized, copyrighted) software or files are discovered on an exempted individual’s computer
- Public exposure of CSI on an exempted individual’s computer is discovered
- Employment status or position of an exempted individual changes

Revocation may also immediately occur at the discretion of the CIO, or delegate, if any of the LETU LetNet policies or procedures are violated, depending upon severity.

In the event of the necessity to revoke exemption, the following steps will be taken:

- Any created Administrator account(s) for the Exempted individual will be terminated, including any local data on any computer(s) associated with the account(s)
- Communication of the revocation will be sent to the Exempted individual, his Dean or Cabinet Level Officer and the CIO
- The Exempted individual’s computer may require remediation including, but not limited to, reimaging the computer to the configuration level the system had when it was originally given to the employee

If a previously exempted individual wishes to reapply for exemption after a revocation, the “Reapplying after Revocation” section below should be followed.
**Reapplying after Revocation**

Individuals with revoked exemption who would like to re-apply for exemption must wait a minimum of 90 days and coordinate a time with LETU IT to review operating system procedures and safe computing guidelines. LETU IT may recommend re-application for administrator rights after this review.

---

**Annual Review**

To ensure all current exemptions are still relevant, LETU IT will perform an annual reauthorization of local Administrator accounts. Every discovered Administrator account provided through the Policy’s Exemption will need to have the Dean or Cabinet Level Officer’s agreement that exemption is still needed.

For example, a timeline would be as follows:

- Day 0. Revocation takes place and notifications for resubmission go out to Dean/Cabinet Level Officer
  - Resubmissions are kept on file as received
- Day 15. Resubmissions yet to be received will have a second notification sent to Dean/Cabinet Level Officer
- Day 30. Resubmissions still not received will prompt a final notification to Dean/Cabinet Level Officer
- Day 45. Previous Exemption will be revoked

---

**Exclusions from Policy Exemption**

Due to the nature of data with which they work, employees in the following areas will not be granted Exemption from this Policy:

- Accounts Payable
- Business Services
- Financial Aid
- Human Resources
- Registrar’s Office
- Resident Directors
- Student Accounts