Authorization for Administrator Privileges on Managed Desktops

“We put processes into place to implement these policies (described in our procedures), and various practices emerge over time to accommodate local variation, exceptions or unforeseen irregularities that arise in carrying out these processes... Procedures should be written down and available for reference, but they change more frequently and are properly the responsibility of decision-makers responsible for the associated processes and practices.”

From the U of S policy on Development, Approval and Administration of University Policies

Purpose

- The procedure for authorizing local administrator privileges on managed desktop computers at the U of S will facilitate employees ability to do their work, while mitigating the risks of:
  - Infection from malware.
  - Installation of unlicensed or illicit software.
  - Use of programs with significant potential for abuse (e.g. peer-to-peer file sharing).
- To formally implement the Center for Internet Security Critical Security controls as the framework that the university will govern and safeguard information as committed to the Board of Governors.

Scope

- The procedure for delegating local administrator privileges on managed desktop computers at the U of S is applicable to the entire university community.
- Reasons for delegating local administrator privileges might include:
  - Key software requires administrator privileges to run/operate.
  - Configuration/installation/updates of software requires administrator privileges.

Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer/Client Without Administrator Privileges</td>
<td>– Plan ahead to ensure you have the software you need before you need to use it.</td>
</tr>
<tr>
<td></td>
<td>– Only access applications and websites relevant to your work (e.g. avoid risky websites).</td>
</tr>
<tr>
<td></td>
<td>– Review department software inventory before requesting the purchase or installation of new software. Work with your supervisor (to justify business need) and UITS/Service Desk.</td>
</tr>
<tr>
<td></td>
<td>– Request new software through UITS/Service Desk.</td>
</tr>
<tr>
<td>Customer/Client With Local Administrator Privileges or Access to a Functional Account</td>
<td>– Plan ahead to ensure you have the software you need before you need to use it.</td>
</tr>
<tr>
<td></td>
<td>– Review department software inventory before purchasing new software (work with your supervisor and UITS/Service Desk).</td>
</tr>
<tr>
<td></td>
<td>– Only install/access applications and websites relevant to your work (e.g. avoid risky websites).</td>
</tr>
<tr>
<td></td>
<td>• Ensure software is legitimate before downloading.</td>
</tr>
<tr>
<td>Unit Support Team (UITS)</td>
<td>Service Desk Team</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>• Don’t install and run pirated/illegal software.</td>
<td>• Respond promptly to requests from clients to have new software.</td>
</tr>
<tr>
<td>• Only use your local administrator account to configure/install/update the necessary application, and then revert to your non-administrator account for the rest of your work.</td>
<td>• Create centralize software inventory for different business areas defining standard software.</td>
</tr>
<tr>
<td>• Keep your functional administrator account private—you will be held accountable for all actions taken using that account.</td>
<td>• Package and update software for different business areas.</td>
</tr>
<tr>
<td>• Review Responsibilities and Vetting Software information provided in Appendix A.</td>
<td>• Maintain published list of software available for employees to install upon request.</td>
</tr>
<tr>
<td>• Don’t tamper with published security settings:</td>
<td>• Troubleshoot issues related to deployed software.</td>
</tr>
<tr>
<td>• AV/Firewall/CIS hardening/App Whitelisting/UAC/etc.</td>
<td>• Report dated software and provide recommendations to supervisors and staff.</td>
</tr>
<tr>
<td>• Don’t remove/update/reinstall core software build:</td>
<td>• Remove all personal NSIDs from computers’ local administrator groups.</td>
</tr>
<tr>
<td>• Office version</td>
<td>• Bitlock all computers hard drives.</td>
</tr>
<tr>
<td>• Java/Flash/Acrobat/Chrome/Firefox/etc.</td>
<td>• Report malware incidents to individual and his/her supervisor.</td>
</tr>
<tr>
<td></td>
<td>• Manage exception process and escalation with Security team.</td>
</tr>
<tr>
<td>Role</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Team</td>
<td>- Report malware incidents to individual and his/her supervisor.</td>
</tr>
<tr>
<td></td>
<td>- Assist with application white listing</td>
</tr>
<tr>
<td></td>
<td>- Respond promptly to all reports of malware incidents.</td>
</tr>
<tr>
<td></td>
<td>- Manage escalated exception requests</td>
</tr>
<tr>
<td>ICT Leadership Team</td>
<td>- ??</td>
</tr>
<tr>
<td>AVP ICT and CIO</td>
<td>- ??</td>
</tr>
</tbody>
</table>

**Procedure**

This procedure balances the need to have administrator privileges on managed devices with the need to protect the university from malware and other IT security risks.

1) Client contacts UITS/Service Desk asking for administrator privileges to run, configure, update or install software because:
   a. Key software they use requires administrator privileges to run/operate.
   b. Configuration/installation/updates of software they use requires administrator privileges.

2) UITS/Service Desk employee assesses reason for request. There are three possible scenarios.
   a. Key software requires administrator privileges to run/operate:
      i. Will three or more individuals require the same software package?
         • Engage ICT to create package for automated installs.
      ii. Can ICT troubleshoot to remove the requirement?
         • Check UAC Virtualization for System Folder/Registry:
      iii. Is there a suitable replacement that does not require administrator privileges?
         • Notepad/productivity tool vs. core business requirements
      iv. Follow exception process to grant NSID-based administrator privileges.
         OR
      v. Install elevation tools (Thycotic Privilege Manager/Carbon Black/ etc.) to allow short-term administrator privileges.
   b. Configuration/installation/updates of software requires administrator privileges:
      i. Can we troubleshoot to remove the requirement?
         • Relax permissions on Registry/Folders
         • Grant limited group access (HyperV - Admin), etc.
      ii. If configuration is one-time (initial setup), either:
         • Have UITS/Service Desk complete the work
         • Grant temporary NSID administrator privileges and revoke when activity is complete. Review Responsibilities and Vetting Software information (see Appendix A) with individual.
• Grant access to local administrator account and revoke when activity is complete. Review Responsibilities and Vetting Software information (see Appendix A) with individual.

   iii. If the configuration is repeated, but infrequent (monthly or less?):
   • Hand off to UITS/Service Desk to elevate on demand.

   iv. If the configuration is repeated, but frequent (monthly or more?):
   • Grant access to local administrator account and review Responsibilities and Vetting Software information (see Appendix A) with individual.

   c. For all other scenarios, require all software installation/configuration management be completed by UITS/Service Desk.

3) In order to maintain administrator privileges requires compliance with responsibilities described above. Administrator privileges will be revoked in the following situations:
   a. Installation of unlicensed/illicit software.
   b. Infection from malware.
   c. Use of programs with significant potential for abuse (e.g. P2P) without business case that has been signed by supervisor.
   d. General abuse of responsibilities.

Appendices
• Appendix A – Responsibilities and Vetting Software
• Appendix B – Decision Tree for Approval of Administrator Privileges
Appendix A – Responsibilities and Vetting Software

1) Check to see if we have a license for the software.
   - Be aware of open source, trial versions, shareware, and software for non-commercial use.

2) Check to see if it is from a reputable source.
   - Ensure software is downloaded from the original software vendor, not from an individual, a torrent site, or from a third party.
   - Peer-to-peer (P2P) software must have documented business case and sign off by supervisor.

3) Check to see if it is the most recent version of the software.
   - Only install the most current version of software to ensure it is and remains up to date with patches. (e.g., do not install SQL 2005 if 2012R2 is the current version).

4) Check to see if the university has another version of the software installed already.
   - Check other installers, Lansweeper, etc.
   - If another version is available, see if it makes sense to deploy that version.
   - If a more recent version is available, see if it makes sense to upgrade everyone else to the new version.

5) Check to see if Microsoft System Center Endpoint Protection (SCEP) / Malwarebytes complain about the installer.

6) Check to see if a Google search for "does x contain malware?" return reputable results.

7) Check to see if there is an equivalent software package already deployed or available (e.g. someone is requesting a new text editor when we have notepad++).

8) Check to see if the package requires elevated privileges.
   - If so, can we troubleshoot and/or find permissions/registration keys/etc. to avoid needing admin privileges?

   Different solution will be required i.e. special VMs for sandboxing (testing of software).

Additional Notes:
1) Ensure the security of the admin user name and password (i.e. no sharing with others)
2) Save all installers centrally
3) Save install notes for each package:
   i. Download location
   ii. License keys (if required)
   iii. End users
   iv. Security / Support mailing lists
4) Don't tamper with published security settings:
   i. AV/Firewall/CIS hardening/App Whitelisting/UAC/etc.
5) Don't remove/update/reinstall core software build:
   i. Office version
   ii. Java/Flash/Acrobat/Chrome/Firefox/etc.
6) Don't create additional admin accounts for others.
Appendix B – Decision Tree for Approval of Administrator Privileges

1. **Do you have administrator privileges?**
   - **Yes:** Proceed to Step 2.
   - **No:** Proceed to Step 3.

2. **If yes:** Proceed to Step 4. If not, proceed to Step 3.

3. **Instructional Network Login:**
   - **One Time:** Contact your local IT support or the ICT Service Desk for assistance.
   - **Ongoing:** Proceed to Step 5.

4. **Is the need to run or perform key software?**
   - **Yes:** Proceed to Step 6.
   - **No:** Proceed to Step 7.

5. **Can ICT subsection to remove the requirement?**
   - **Yes:** Proceed to Step 8.
   - **No:** Proceed to Step 9.

6. **Is there an alternative application that doesn't require administrator privileges?**
   - **Yes:** Administrator privileges granted through exception process.
   - **No:** Proceed to Step 10.

7. **Requirement removed as administrator privileges not required.**
   - **Yes:** Proceed to Step 11.
   - **No:** Proceed to Step 12.

8. **Alternate application installed by ICT.**
   - **Yes:** Proceed to Step 13.
   - **No:** Proceed to Step 14.

9. **Frequent troubleshooting or daily task.**
   - **Yes:** Proceed to Step 15.
   - **No:** Proceed to Step 16.

10. **Further assessment required by local IT support to determine business need.**
    - **Yes:** Proceed to Step 17.
    - **No:** Proceed to Step 18.

11. **Administrative privileges granted.**
    - **Yes:** Proceed to Step 19.
    - **No:** Proceed to Step 20.

12. **Local administrative privileges granted through exception process.**
    - **Yes:** Proceed to Step 21.
    - **No:** Proceed to Step 22.

13. **Can ICT subsection to remove the requirement?**
    - **Yes:** Proceed to Step 23.
    - **No:** Proceed to Step 24.

14. **No:** Proceed to Step 25.

15. **Administrator privileges granted.**
    - **Yes:** Proceed to Step 26.
    - **No:** Proceed to Step 27.

16. **Local administrative privileges granted through exception process.**
    - **Yes:** Proceed to Step 28.
    - **No:** Proceed to Step 29.

17. **Requirement removed as administrator privileges not required.**
    - **Yes:** Proceed to Step 30.
    - **No:** Proceed to Step 31.

18. **Further assessment required by local IT support to determine business need.**
    - **Yes:** Proceed to Step 32.
    - **No:** Proceed to Step 33.

19. **Administrative privileges granted.**
    - **Yes:** Proceed to Step 34.
    - **No:** Proceed to Step 35.

20. **Local administrative privileges granted through exception process.**
    - **Yes:** Proceed to Step 36.
    - **No:** Proceed to Step 37.

21. **Can ICT subsection to remove the requirement?**
    - **Yes:** Proceed to Step 38.
    - **No:** Proceed to Step 39.

22. **No:** Proceed to Step 40.

23. **Can ICT subsection to remove the requirement?**
    - **Yes:** Proceed to Step 41.
    - **No:** Proceed to Step 42.

24. **No:** Proceed to Step 43.

25. **Further assessment required by local IT support to determine business need.**
    - **Yes:** Proceed to Step 44.
    - **No:** Proceed to Step 45.

26. **Administrator privileges granted.**
    - **Yes:** Proceed to Step 46.
    - **No:** Proceed to Step 47.

27. **Local administrative privileges granted through exception process.**
    - **Yes:** Proceed to Step 48.
    - **No:** Proceed to Step 49.

28. **Can ICT subsection to remove the requirement?**
    - **Yes:** Proceed to Step 50.
    - **No:** Proceed to Step 51.

29. **No:** Proceed to Step 52.

30. **Requirement removed as administrator privileges not required.**
    - **Yes:** Proceed to Step 53.
    - **No:** Proceed to Step 54.

31. **Further assessment required by local IT support to determine business need.**
    - **Yes:** Proceed to Step 55.
    - **No:** Proceed to Step 56.

32. **Administrator privileges granted.**
    - **Yes:** Proceed to Step 57.
    - **No:** Proceed to Step 58.

33. **Local administrative privileges granted through exception process.**
    - **Yes:** Proceed to Step 59.
    - **No:** Proceed to Step 60.

34. **Can ICT subsection to remove the requirement?**
    - **Yes:** Proceed to Step 61.
    - **No:** Proceed to Step 62.

35. **No:** Proceed to Step 63.

36. **Can ICT subsection to remove the requirement?**
    - **Yes:** Proceed to Step 64.
    - **No:** Proceed to Step 65.

37. **No:** Proceed to Step 66.

38. **Can ICT subsection to remove the requirement?**
    - **Yes:** Proceed to Step 67.
    - **No:** Proceed to Step 68.

39. **No:** Proceed to Step 69.

40. **Further assessment required by local IT support to determine business need.**
    - **Yes:** Proceed to Step 70.
    - **No:** Proceed to Step 71.

41. **Administrator privileges granted.**
    - **Yes:** Proceed to Step 72.
    - **No:** Proceed to Step 73.

42. **Local administrative privileges granted through exception process.**
    - **Yes:** Proceed to Step 74.
    - **No:** Proceed to Step 75.

43. **Can ICT subsection to remove the requirement?**
    - **Yes:** Proceed to Step 76.
    - **No:** Proceed to Step 77.

44. **No:** Proceed to Step 78.