Admin Responsibility Matrix

Every university affiliated member (faculty, staff, student, grant-funded positions, visitors, etc) is required to read and abide by the University’s Acceptable Use Policies. The Office of Information Security and the Internal Audits work closely to ensure compliance is being kept. Regular departmental audits from both teams occur and results are shared with the department’s corresponding Office of Information Technology. CNS IT works to implement these required security settings and configurations across all managed/supported devices. Specific policies can be found in the Information Resources and Security Policies site.

- AUP requires a renewal via digital signature. Alerts go out when you are due to review the campus AUP. You may also check your status here: [https://forms.security.utexas.edu/acceptable_use](https://forms.security.utexas.edu/acceptable_use)
- Hardening Checklists for those looking to manage and maintain their systems can be found here: [Hardening Checklists](https://www.security.utexas.edu/policies/HardeningChecklists)
- CNS IT has no authorization to offer policy exceptions for any systems. If you feel your system should be exempt from any policy/security requirements, please submit an exception so the Information Security Office may get the request and determine exemption status. [https://forms.security.utexas.edu/misc/exception](https://forms.security.utexas.edu/misc/exception)
  - If an exception is given, please forward the notice to CNS IT via email help@cns.utexas.edu so that we may have it on record.

CNS Department of IT - User Services

(Help Desk and Desktop Support)

<table>
<thead>
<tr>
<th>SERVICES</th>
<th>OIT Managed System</th>
<th>Self Managed</th>
<th>User’s Options?</th>
</tr>
</thead>
</table>
| OS Installation| OIT Fully Supported and Maintained | Latest Windows OS (Cannot be older than 3 versions)  
Latest Mac OS (Cannot be older than 3 versions)  
Latest Linux OS (Cannot be older than 3 versions) | Local System Admin agrees to manage application, OS updates, and upgrades. |
| Hardware Repair| Full Assessment and Remediation | Dells Optiplex/Latitude line  
Apple line  
Other models or legacy systems are best effort | CNSOIT runs diagnostics on hardware:  
If hardware fails, admin/dept responsible for purchasing hardware.  
If hardware is hard drive, CNSOIT images and Admin/User configures/restores from their backup. |
| Software Support| Full Assessment and Remediation | Reinstall only | Do not provide Application support, only reinstalls. Admin/Staff responsible for supplying software and licenses. |
| Administrative Access | Fully Monitored | IT admin access  
User assigned to System | CNSOIT retains admin access to computer to assist with best effort troubleshooting. Admin/Staff retains admin access to manage computer updates/upgrades/compliance. [Password Policies](https://security.utexas.edu/policies/passwords) |
| Software Updates | User responsibility | Admin is responsible for all critical updates. Information Security Office will quarantine if critical updates are missing. Un-quarantine procedure requires local admin scan/eliminate for viruses/malware and running updates. Local admin alerts CNSOIT through quarantine ticket of remediated/cleaned/updated system. CNSOIT removes quarantine after verification. |
| Antivirus | User responsibility | Admin responsible for all antivirus updates. ISO will quarantine if the machine is infected. Un-quarantine procedure includes admin scanning for viruses and running updates. Admin alerts CNSOIT of cleaned/updated box. CNSOIT removes quarantine. |
| Data Backup | User responsibility | Admin responsible for backing up data using UTBackup or 3rd party service with encrypted external volume. Admin responsible for file restores from these backups. CNSOIT responsible for re-imaging if OS damaged and Admin responsible for data/software restore. |
| Data Retention | User responsibility | Based on data classification standards, users must identify such data and apply data retention schedules against it. |
| Data Recovery | Best Effort | CNSOIT runs diagnostic and data recovery (if possible). If unrecoverable, alternative option lies with third-party and admin/dept assumes financial responsibility for using service. |
| Encryption | User responsibility | Admin responsible for complying with ISO requirements for data encryption. All machines on the network must be encrypted. Admin responsible for supplying inventory of encrypted machines and encryption key management. [https://security.utexas.edu/policies/encryption](https://security.utexas.edu/policies/encryption) |
| **Inventory** | User responsibility | Admin responsible for maintaining an inventory of all equipment under their administration. Periodic inventory audits will require that they identify all machines noted in the audit. |
Network Quarantines due to viruses

| CNS IT handles case via a format/OS reinstall minus Absolute Manage User handles data recovery and other software installs. | Admin scans for viruses and running updates. Admin alerts CNSOIT of cleaned/updated box. CNSOIT removes quarantine. If the system is quarantined more than once during a semester, the quarantine will only be lifted after CNSOIT re-images the system and the Admin restores cleaned files/software from backup. |

NOTE: By default, users are set as standard users on their systems. A local CNSOIT management account is set as admin to allow the support tools to interact with the client machine. Once approved, the administrative account will be supplied and the customer will be responsible for using it only to escalate privileges to perform certain tasks on the device. IT IS NOT to be used to log in regularly as a regular account to perform daily activities like email or web browsing. IT IS NOT to be used to escalate any standard account to admin account or any admin account to standard account. This must be performed only by the CNS IT group once an exception for the change has been granted. IT IS NOT to be used to remove management or administrative tools installed by CNS IT. Such actions will be reported to the CNS Executive Director of IT and could be escalated to the UT Information Security Office for further disciplinary action.

Related articles

- Connecting to the UT VPN
- How To: Duo Two-Factor Authentication
- How To: Resource Email Accounts
- Employee Enter and Exit Forms
- Admin Responsibility Matrix