UTEP Standard 20: Software Licensing

20.1 All software used on University devices will be used in accordance with the applicable software license. Unauthorized or unlicensed use of software is regarded as a serious violation subject to disciplinary action and any such use is without the consent of the University.

(a) UTEP Information Security Policies: UTEP provides a sufficient number of cost-effective, licensed copies of core business software to enable faculty members, staff, and students to perform their work in an expedient and effective manner.

(b) Systems administrators have the right to remove software from University devices for cause. For example, if a user in unable to show proof of license, or if the software is not required for University business purpose, or causes problems on the University-owned device.

(c) All departments/colleges are responsible for the accurate accounting of software purchased by their respective department/ college and must ensure that the installation of the software complies with the license agreement of the software. For audit purposes, departments/colleges must maintain proof of purchase and/or original installation media for each software package. Third-party software in the possession of UTEP must not be copied unless such copying is consistent with relevant license agreements and prior management approval of such copying has been obtained, or copies are being made for contingency planning purposes.

(d) All software purchases shall go through the UTEP Purchasing Department.

(e) All commercial software used on computing systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product and shall be purchased through the Purchasing Department. Personnel must abide by all license agreements and must not illegally copy licensed software. The University reserves the right to remove any unlicensed software from any system at any time without prior notification.

20.2 Prohibited Software or Uses. This section provides examples of prohibited software; however, it is by no means all inclusive. Software that falls within the categories outlined below is also prohibited unless the Information Resource Manager (IRM) grants an exception.

- Bloatware – Other demonstration software bundled with needed software
    - McAffee Anti-Virus Software must be unchecked when installing or updating Adobe.
- Peer to Peer (P2P) or Social Networks - for illegally sharing/ uploading/ downloading/ streaming / stream-ripping copyrighted media (e.g., music, videos, movies, television series, gaming software, etc.) and Miscellaneous Other Services – See also RIAA Notorious Markets Report 2016. Note that this is not intended to be an all-inclusive list.
    - UTorrent
    - Sharest
    - BitTorrent
    - Ares
    - FrostWire
    - Transmission
    - Limeware
    - Shereaza
    - Kazaa
    - eMule Plus
    - Azureus aka Vuze
    - BearShare
    - Gnutella
    - Movie Torrent
- BitCoin Stratum miner, etc.
- Opening Shares without Setting Appropriate Restrictions
- Software which was not legally purchased (i.e., pirated, unlicensed software, etc.)
- License Key Generators
- Adware and toolbars (e.g., example cashbach, weatherbug, etc.)
- Video Games
- Malware
- Remote Access Utilities/Software
    - Telnet
    - FTP
    - IMAP
    - GoToMyPC
    - pcAnywhere
    - TeamViewer

- Network Scanning or Sniffing Utilities/Software
- Password Cracking Utilities/Software
- Keyboard Sniffers, Keylogging, or System Monitoring Utilities/Software
- Joke Software
- External DNS Software
- Use of Personal Email Accounts to Store or Transmit Confidential Information
- Unauthorized Anti-Virus Software
- Removal of Required Software
- Disabling of Security Features

20.3 Revision History

First Draft:	April 4, 2002
Revised:	January 12, 2012
Revised:	June 1, 2017
Approved:	June 16, 2017
	Gerard D. Cochrane Jr., Chief Information Security Officer