SPICE The Focus is on YOU
Security Program for the Information and Computing Environment
http://security.health.ufl.edu

SPICE EduGuide EG0017
Peer to Peer File Sharing Software Usage Risks

This SPICE EduGuide applies to HSC faculty, staff, students, and affiliates who use computers for HSC business. Peer to peer (P2P) file sharing is a fast and efficient way to share electronic files across the Internet. P2P software joins a computer on a world wide network with other computers enabling its users to upload and download files from each other's computers. Products like Warez P2P, Morpheus, eDonkey, Limewire, Cabos, BitTorrent, BearShare, and Kazaa are used by millions of Internet users throughout the world. It is extremely popular because it is typically used for acquiring free music, movies, games, and computer programs. However, P2P file sharing software poses high risks for the HSC:

Unauthorized Disclosure - Some P2P software installers default to sharing a user's entire MyDocuments folder or HomeDir folder. The MyDocuments and HomeDir folders are generally where MS Windows and Apple save all the user's files and newly created folders. Sometime during the P2P software installation process the installer prompts the user to click 'Ok' to sharing their MyDocuments folder or HomeDir folder. Users can optionally enter another folder name to share. However most users accept the default settings, unaware that they are sharing far more files than they had intended. Furthermore, some P2P software contains a 'browse' feature enabling one P2P software user to browse any other connected P2P software user's computer and download anything he finds.

Malicious Software – The threat of contracting malicious software such as spyware, viruses and worms is very high when P2P software is installed and used. Some P2P software programs themselves contain malicious software enabling the author to capitalize on thousands of unwitting users who download their software. Further, files shared on P2P networks can be unhealthy. Users who acquire files on P2P networks generally do not know the sources of the files. The anonymity with which files are shared on a P2P network is a haven for malicious software distributors.

Objectionable or Illegal Material Mule - Some savvy P2P software users use other P2P computers as 'mules' to hide and distribute adult pornography to children, child pornography to anyone, inflammatory literature, and illegal or "unpopular" material. The mule can be accomplished when the savvy user disguises file names of objectionable material with the names of popular files that are frequently searched. A novice P2P software user searching for a popular song title could end up downloading and sharing objectionable and illegal files without knowing it.

Safeguard Requirements and Guidance

- Due to the high risk of an accidental unauthorized disclosure of HSC Restricted data, P2P file sharing programs are prohibited on HSC computers and networks. HSC users who have installed P2P file sharing software on their work computer must de-install it immediately. Unit Information Security Managers (https://security.health.ufl.edu/staff/index.shtml) are available for assistance.

- Personally owned computers with P2P file sharing programs may not be used for HSC related business. Users with P2P file sharing software installed on a personally owned computer (i.e. home computer) used for work, can either de-install the software or discontinue using the computer for HSC business.

- A comprehensive list of prohibited P2P software is available here: https://security.health.ufl.edu/p2p/p2p.shtml. However, any product that connects your computer to an open world wide network of anonymous peer computers and users is prohibited. Unit IT departments are highly encouraged to establish an application blacklist policy to include the list of software at the site referenced in this paragraph, and to push the blacklist policy out to all Unit computers.

- The HSC Security Office will perform a P2P network assessment on a periodic basis. If P2P software is found on HSC computers or HSC business information is found on personally owned computers, users face loss of computer and network access and disciplinary action.

Policy & Standards References:
TS0006 Electronic Communications and Data Transmission Policy
TS0006.02 Electronic Communications and Data Transmission Standard
https://security.health.ufl.edu/policies/#ts0006