Intrusion Prevention System Information
Software not in compliance with policy and standards blocked by the IPS

The Commonwealth Office of Technology is entering the next phase of deployment of the newly installed Intrusion Prevention System, often referred to as IPS. These network based security appliances will be placed into active blocking mode to stop certain attacks from reaching our network. Additionally, these devices will block instant messaging (IM), peer to peer (P2P) file sharing software such as Bit Torrent, and other unauthorized software. The purpose behind moving these devices to active blocking mode is to further protect our infrastructure and data from malicious activity by blocking attacks from the outside and to comply with the Commonwealth's Enterprise Policies and Standards. It is not to restrict innovation or business. Below is a list of applications and software that will be affected. This list will be updated as any new application or software is added.

Software	**Category**
Yahoo Messenger	(Instant Messaging)
Meebo Instant Messaging	(Instant Messaging)
AOL Instant Messenger	(Instant Messaging)
MSN Messenger	(Instant Messaging)
Google Talk	(Instant Messaging)
ICQ	(Instant Messaging)
IRC	(Instant Messaging)
Swapper Alive	(Peer to Peer)
Bit Torrent	(Peer to Peer)
Limewire	(Peer to Peer)
Warez	(Peer to Peer)
Gnutella	(Peer to Peer)
Azureus	(Peer to Peer)
Thunder KanKan	(Peer to Peer)
Groove Virtual Office	(Peer to Peer)

Please refer to the Enterprise Architecture and Standards for a listing of software approved for use on the Commonwealth network:
http://technology.ky.gov/governance/Pages/architecture.aspx