

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	May 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.11	Peer-to-Peer Access Policy	Responsibility:	Chief Information Security Officer

PEER-TO-PEER ACCESS POLICY

Overview

This policy establishes access to and from the institutional computer network and the Internet for Peer-to-Peer (P2P). Computers that are set up in a peer-to-peer model are linked to another computer (or computers) designed to share files. Every file on each system may be subject to access by the other system (or systems) so that every piece of information on the University computer is now accessible by an outside entity.

Policy

1. Computer users are permitted to use only those network (IP) addresses as authorized by Systems and Network Operations (SNO) for Internet communications. See the *Handbook of Operating Procedures* (HOP), [Section 5.8.7](#), "Network Access Policy".
2. Computer users cannot install or use P2P applications that have not been authorized by the Dean, Chair, or Director and determined by the Information Security Office to have minimal risk.
3. The use of authorized P2P configuration for personal use is a direct violation of this policy.
4. A listing of unauthorized P2P software and applications is posted at the following Web site: <http://ims.uthscsa.edu/policies.aspx>. The Information Security Council will, at least annually, review the list of prohibited P2P applications.
5. This policy does not apply to music sites that broadcast music such as Realmusic or radio stations, such as WOAI.com, that broadcast over the Internet.
6. Departments that require P2P applications and communications to complete their assigned University missions must provide the name of the P2P application(s) and specify whether the P2P application requires access to the Internet. This information should be submitted to SNO via a Service Request Form (SRF). Authorization of P2P applications is a joint decision between the

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	May 2003
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.11	Peer-to-Peer Access Policy	Responsibility:	Chief Information Security Officer

Chief Information Security Officer, the Directors of CR and SNO, and the requesting department's Chair or Director.

7. In the event that a P2P application appears on the "unauthorized list" but a department has a business need requiring the use of that specific P2P application, that requirement will be reviewed by the Chief Information Security Officer, and the department's Chair or Director to determine either an alternate solution or compensating controls that would ensure the security of the information resource.