

INFORMATION TECHNOLOGY POLICY COMMITTEE  
**Policy on Administrative Access to LAN User's Information**

The following set of authorizations and restrictions is designed to enable LAN administrators to carry out their responsibilities while protecting the privacy of LAN users.

This statement is intended as a clarification of the Purdue University "Policy for Access and Use of Purdue's Electronic Mail System." Purdue policy supersedes in cases of conflict with this IPFW statement.

**Authorizations**

For purposes of system maintenance and management, LAN administrators are specifically authorized to acquire, store, and use the following types of information stored in computers attached to IPFW LANs:

1. LAN administrators are permitted unlimited access to a network user's computer when that user has given explicit consent for such access, as during installation, upgrade, trouble-shooting, and repair operations.
2. LAN administrators have read-only access to information about the current configuration of any user's networked computer, subject to the limitation that no user-input information is to be collected by the administrator. In practice, this authorization would allow the administrator to use software to identify the user's CPU, keyboard, and monitor types, amounts of free RAM and disk space, operating system and version, available ports, and similar useful configuration data such as that contained in generic configuration files.
3. LAN administrators have unlimited read and write access to one specified directory and its subdirectories on the networked computer and one specified individual-user-drive directory and its subdirectories on each attached server, subject to the limitations described later in this paragraph. For example the LAN administrator might select the network directory on the computer and the setups directory on the server's I: drive. However, these rights of special access shall be exercised only after users have been given one-time notice of the unusual privileges the administrator enjoys in these directories and their subdirectories.
4. LAN administrators are permitted to make back-up copies of all files stored on servers. These copies are to be used solely to protect against data loss.
5. LAN administrators are permitted to use software that identifies and directs specific file types on the network to specific network bandwidth areas. For example, .MP3 file types used for the sharing of recreational music shall have a limited operating bandwidth. This action is taken in the interest of protecting the maximum amount of network bandwidth for the academic purposes of the university.

**Restrictions**

Except as noted above, it is the policy of IPFW that electronically stored information be treated as confidential. This confidential treatment refers not only to personal files but also to the content of keystrokes, files, printing queues, and other information-bearing materials sent on the network. Examining or disclosing the files and/or contents thereof is appropriate only if authorized by the owner of the information, approved in writing by the appropriate university official (the dean for academic units, the director for other units, or the vice chancellors, or chancellor), or required by state or federal law.