

TO: University Resources Policy Committee

FROM: Academic Computing and Information Technology Advisory Subcommittee
Tiff Adkins, Chair

DATE: November 19, 2003

SUBJECT: Concerns regarding the IPFW mandatory screen saver policy

DISPOSITION: For information only

The Academic Computing and Information Technology Advisory Subcommittee met on November 5, 2003 to investigate and discuss the rationale of Information Technology Services mandating a screen saver for all faculty computers on the IPFW campus. At the request of the Executive Committee we are bringing these concerns to the attention of the Senate for information only.

The Academic Computing and Information Technology Advisory Subcommittee worked directly with the Director of Information and Technology Services to prepare this report. Specifically, the following concerns were addressed:

1. Is IPFW the only campus in the Indiana University/Purdue University system where this is required?
2. Is it appropriate for Information Technology Services to mandate screen savers on computers which reside in private faculty offices, and which are not publicly accessible?
3. Could Information Technology Services limit the universal mandate?

Is IPFW the only campus in the Indiana University/Purdue University system where this is required?

Indiana University – Purdue University Fort Wayne is taking a proactive step in requiring reasonable measures to help reduce the possibilities of unauthorized access to the IPFW student information system, servers, and network resources. Enacting this requirement puts IPFW in a leadership role in establishing enhanced security measures that can serve as a model for other campuses and institutions. Support for this measure is also garnered from an internal audit conducted by Purdue's Information Technology at Purdue (ITaP) Internal Audit Office during the spring of 2003 that recommended IPFW implement just such a security measure. The Academic Computing and Information Technology Advisory Subcommittee recognizes, as stated in a campus wide e-mail from Information Technology Services sent on August 22, 2003, that the primary impetus for this procedure is to help IPFW stay on the path of compliance with several federal acts, including the following:

The Patriot Act: Covers wide areas protecting electronic transmission of information & data,

Gramm-Leach-Bliley Act: Covers protection of customer information gathered from financial transactions,

Health Insurance Portability & Accountability Act (HIPAA): Protects a person's health information

Is it appropriate for Information Technology Services to mandate screen savers on computers which reside in private faculty offices, and which are not publicly accessible?

At a public institution the size of IPFW, private faculty offices are never free from the risk of being accessed by unauthorized personnel. It takes very little time for a person to gain entry to an office and unlawfully access the computer of a faculty or staff member. This includes exposure during night and weekend hours, which have experienced unauthorized use of computers in offices. As part of Information Technology Services main mission of operating and supporting the computing and information technology

environment at IPFW, it is appropriate within that duty to recommend guidelines and requirements for the campus constituents.

Could Information Technology Services limit the universal mandate?

Information Technology Services approaches computer related security measures with the utmost attention given to the users of the services provided. Careful consideration is given to the impact any suggested guidelines or requirements may have. Information Technology Services is willing to investigate any computing situation when evidence suggests that the universal mandate may not be a reasonable security measure, or where the restrictions may have to be further tailored to allow certain critical activities to continue within the security objectives. One example would be in the IPFW Police and Safety Department, where due to the nature of requiring quick access to information, and the fact that their computers are staffed 24 hours a day, a generic log-in was added to those machines requiring quick access.

It must also be noted that the restriction has been placed only on computers operating Windows, and which are on the IPFW network. At present, Apple computers cannot accept the screensaver tied to the network login, except those with the Mac OSX operating system. ITS is testing use of the screensaver password with these machines. Some Mac OSX users have initiated the screen saver password capability on their own.