New UC guidelines on Encryption

The best way to protect data is to not have it. However, restricted data should be retained only when it is necessary but if you must keep sensitive data, the University requires encrypting it. The purpose of encryption is to prevent unauthorized access to data while it is either in storage or being transmitted. For example, encryption can protect the privacy of restricted data that is stored on a laptop computer, even if that laptop computer is stolen. Similarly, it can protect data that is transmitted, for example, over a network, even if that network is tapped by an unauthorized third party.

In April, 2006, UCOP's Information Resources and Communications released guidelines for encryption and announced an agreement with Pointsec to provide the University with encryption tools for PCs, smartphones, PDAs, removable media such as CDs and flash drives, and management tools for those who have to look after all these various devices.

As the guideline states "Encryption is not, however, a panacea. It is not a substitute for other security measures, such as authentication, authorization, and access control, and must be used in conjunction with those other measures." The guidelines provide information on developing strategy at the local level to use encryption effectively.

Revision #3
Created Wed, May 24, 2006 12:20 PM by Chuang, Kimberly
Updated Fri, Mar 24, 2017 8:24 PM by Phillabaum, Paul