Portable Device Encryption at UMSL

Recommended software and practices for encrypting “private” student, faculty or research data on laptops or other portable devices.

Audience

All members of the UMSL Network with portable computers and their supervisors.

Statement

It is the recommendation of the Information Technology Services department at the University of Missouri St. Louis that any portable computer with “private” or “sensitive” student, faculty, or research information on it should be protected with a full disk encryption method. This would include either a hardware or software method of encryption. It is also recommend that you use only University supported methods of encryption for your protection and the protection of University information.

Background Issues

Computer, System, or Network Use

All users of the University's computing and network resources must be aware that certain types of information must be kept private even in the case of computer theft. If you carry a portable computer with private student, faculty or research data you may need to use encryption software.

- You have social security numbers, credit card data or any other personal information of students, faculty or anyone else affiliated with University business on you computer.
- You have any protected FERPA or HIPAA data on you computer.
- You have data that could damage your research or any University intellectual property if it were stolen.

If any of the above items matches what you carry on you portable computer please contact the Technology Support Center on campus and they will get you in touch with the appropriate people.

Computer, System, or Network Administration

The Information Technology Services department at UMSL has tested and can recommend an encryption solution for campus use. The recommended methods of encryption will have mechanisms built in to it that will protect your data from being stolen and you from permanently loosing access to it. Encryption keys used can get lost and access to the data could be lost if it is not setup properly. ITS can help prevent that by properly protecting encryption keys to protect you and University property. It is recommended that you only use University approved methods of encryption and have ITS help you with implementing your solution.

Original Issue Date

August 2006

Revision Date