



INTERMEDIATE INFORMATION STEWARDSHIP

PORTABLE MEDIA

**Information Security & Privacy
Advice**
(ISO/IEC 17799:2005 § 6.1.2.f)

PRIVACY

POLICY

BGSU employees are required to protect the confidentiality and privacy of data.

The BGSU [Code of Ethics and Conduct](#) also reminds us that “we must act in a way to inspire public confidence in the honesty and integrity of our actions.”

**ITS Network
& Computer
Policies #A27**

[www.bgsu.edu
/downloads/cio
/files9602.pdf](http://www.bgsu.edu/downloads/cio/files9602.pdf)

USB flash drives (AKA memory sticks) are popular productivity tools. They provide fast and efficient access to portable data. The pocket-sized devices are lightweight, contain no moving parts and continue to drop in price as their storage size continues to increase. Common storage sizes are 8Mb to 64Gb and they can be used with most computers that contain an active USB port.

As the use of these devices in the workplace increases it is important to examine how USB flash drives impact the privacy and security of BGSU information.

A recent news story chronicled an audit process of a credit union and their use of these portable devices. USB flash drives were placed strategically around the organization and contained Trojan software that would report if connected to the company network. Of the twenty USB flash drives left in the workplace fifteen

were found by employees and attached to their company PC's.

Along with introducing tracking software the uncontrolled use of flash drive can introduce other hazards such as:

- Loss of sensitive or private data
- Stolen proprietary data and plans
- Placement of viruses or other malicious software on the network

Consequently, some organizations ban their use where sensitive information is handled. Although USB flash drives can be difficult to control there are things you can do to reduce the risk when using them in the workplace.

“The personal information of thousands of students ... was lost in a foreign country ... the device is missing ... may have contained files with personally identifiable student information, including social security numbers ... It wasn't against the rules for the professor to take the student files with him. However, it's still possible the university could take action against him.”

-Excerpts from actual news story, June 2007

TIPS

MEDIA HANDLING

- ⚠ First, do not collect or process sensitive information like Social Security Numbers if not absolutely necessary. You can not lose what you do not have.

See the Information Security & Privacy brochure, [Managing Sensitive Data](#) for additional relevant tips.

- ⚠ Refer to BGSU's Records Retention Schedule before copying or destroying data.
- ⚠ **Do not store or process sensitive University information on personally owned media or computers!**
- ⚠ Establish physical barriers to prevent access to areas containing computers, media, or printouts with sensitive information.
- ⚠ Do not take an unencrypted University laptop computer out of its secure office environment if it has ever been used to store or process sensitive data.
- ⚠ **Immediately report the loss or theft of media or computers that have been used to store or process sensitive information.**
- ⚠ Sensitive information on mobile media such as diskettes, USB memory devices, PDAs, Blackberrys, digital cameras, or CDs must be encrypted or physically secured.
- ⚠ Do not transmit sensitive information through email or attachments unless encrypted.
- ⚠ Remove sensitive printouts from printers or fax machines immediately.
- ⚠ Lock offices containing sensitive information when not in use or when authorized persons are temporarily out of the area.