

BGSU SENSITIVE DATA PRIVACY*INTERIM POLICY*

Applicability	All BGSU stakeholders	Number	IT – xx - xx
Last Revised	June 26, 2007		
Policy Owner	Office of the Chief Information Officer (CIO) cio@bgsu.edu		
Governing Body	N/A		

INTRODUCTION

BGSU must protect its information resources, comply with laws and applicable statewide policies issued by the Ohio Office of Information Technology (OIT) under the authority of the Ohio Revised Code, and comply with other University policies regarding the protection and use of University data and information technology resources. As a result, the Policy on Sensitive Data Privacy has been established.

POLICY

BGSU stakeholders must have the ability to collect and process information for administrative and academic purposes. Information collected and processed may include sensitive information.

Sensitive information includes personal information and proprietary information of the University including but not limited to: Social Security numbers, Driver License numbers, credit card or other financial account numbers, BGSU ID numbers, protected health information, financial data, educational records, intellectual property or research records, donor profiles, or any information that could result in a material risk of identity theft, a violation of the Family Educational Rights and Privacy Act, or otherwise harm the legitimate financial and reputational interests of the University if unauthorized access is permitted, whether intentionally or unintentionally.

BGSU stakeholders are to use University information on University owned media or equipment. BGSU stakeholders are not to store, communicate, transport, or process University information on personally owned media, devices, or computers without prior written approval from the appropriate Vice President and approval of the personal equipment by Information Technology Services (ITS).

Information on University owned portable devices such as flash drives, disks, or laptop computers must be stored in physically secure locations and is not to be transported without encrypting the data using University approved software and techniques.

Software, policies, and procedures for encrypting sensitive information are currently being deployed as part of the ITS CELO project. Due to the scope of this project, deployment of encryption will be completed during the next several months. To schedule encryption installation for a University owned portable device, please contact the Technology Support Center (TSC) at extension 20999 or email at tsc@bgsu.edu.

The Ohio Breach Notification Act requires prompt notification to individuals whose personal information has been exposed if the incident could lead to fraud or identity theft. Any loss of sensitive data, disclosure of sensitive data to unauthorized individuals or suspected misuse of sensitive data must be immediately reported to the Office of the CIO.

ADDITIONAL INFORMATION

Once printed, this policy may be outdated. The most recent version of this policy can be found at <http://www.bgsu.edu/offices/cio/page32228.html>

See also:

- BGSU Code of Ethics and Conduct
www.bgsu.edu/offices/president/page11661.html
- BGSU Core Values
www.bgsu.edu/catalog/University/University8a.html
- BGSU Information Technology Policy
<http://www.bgsu.edu/offices/cio/page52522.html>
- BGSU records retention requirements
www.bgsu.edu/colleges/library/cac/uarchives/recman.html