BGSU
BOWLING GREEN STATE UNIVERSITY

3341-6-39 Sensitive Data Privacy.

Applicability	All University units
Responsible Unit	The Vice President for Finance and Administration
Policy Administrator	The Office of the Chief Information Officer

(A) Policy Statement and Purpose

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.

(B) 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 included 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 the 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 installed. 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.

(1) Related Policies

(a) Code of Ethics and Conduct; Core Values; Information Technology Policy; Records Retention Requirements

Registered Date: March 17, 2015