

BGSU INFORMATION TECHNOLOGY POLICY*ABBREVIATED VERSION*

Applicability	All BGSU stakeholders	Number	IT – xx - xx
Last Revised	July 21, 2008		
Policy Owner	Office of the Chief Information Officer (CIO) cio@bgsu.edu		
Governing Body	N/A		

INTRODUCTION

Bowling Green State University provides information technology resources to support the academic, administrative, educational, research and service missions of its appropriately affiliated members within the margins of institutional priorities and financial capabilities. The information technology resources provide for the University a conduit for free and open forum for the expression of ideas mindful of the University core values. In order to protect the confidentiality, integrity, and availability of information technology resources for intended purposes, the following policy has been developed. The scope of this policy is to encompass all information technology devices owned by the University, any device obtaining connectivity to the University network, and all University relevant data on these devices.

POLICY

1. All usage of information technology resources is to be consistent with all other relevant policies at BGSU.
2. Users must be aware of and comply with all Federal, State, local, and other applicable laws, contracts, regulations and licenses.
3. Use of information technology to access resources other than those supporting the academic, administrative, educational, research and service missions of the University or for more than limited social purposes is prohibited.
4. All users must only access or attempt to access information technology resources that they are authorized to use and then only in the manner and to the extent authorized.

5. Attempting to circumvent information technology security systems is prohibited.
6. Disruption of University authorized activities is prohibited.
7. Use of information technology to conduct reconnaissance, vulnerability assessments, or similar activity by unauthorized personnel is prohibited.
8. Users are required to protect the confidentiality, integrity, and availability of information technology.
9. Anonymous use, impersonation, or use of pseudonyms on an information technology resource to escape accountability is prohibited.
10. The use of any unlicensed spectrum space is prohibited on any BGSU-owned or BGSU-occupied property, unless it is part of the wireless services being deployed by the University.

RESPONSIBILITIES

University Responsibilities

- Provide and coordinate information technology resources to allow completion of duties as assigned in support of the academic, administrative, educational, research, and service missions, within the margins of institutional priorities and financial capabilities
- Communicate, review, update, and enforce policies to protect information technology resources
- Take reasonable measures to mitigate security threats

User Responsibilities

- Read, agree to, and abide by all University policies and policy updates
- Practice safe computing when using information technology resources
- Notify University officials upon discovery that an assigned information technology resource has been accessed, attempted to be accessed, or is vulnerable to access by unauthorized users
- Users are responsible for activity resulting from their assigned information technology resources

SECURITY AND PRIVACY STATEMENT

BGSU respects the privacy of all information technology users. The University does not routinely monitor the content of material but does reserve the right to access and review all aspects of its information technology infrastructure to investigate performance or system problems, search for harmful programs, or upon reasonable cause, to determine if a user is violating a policy, State or Federal law. BGSU monitors, keeps, and audits detailed records of information technology usage; traces may be recorded routinely for trouble shooting, performance monitoring, security purposes, auditing, recovery from system failure, etc.; or in response to a complaint, in order to protect the University's and others' equipment, software, and data from unauthorized use or tampering. Extraordinary record keeping, traces and special techniques may be used in response to technical problems or complaints, or for violation of law, policy or regulations, but only on approval by University administrators specifically authorized to give such approval. In addition to the privacy of individuals being respected under normal circumstances, the privacy of those involved in a complaint will be respected and the University will limit special record keeping in order to do so, where feasible. Information will be released in accordance with law. Users should be aware that while the University implements various security controls to protect information technology resources, protection of data from unauthorized individuals cannot be guaranteed.

ENFORCEMENT AND SANCTIONS

Individuals or entities in violation of the BGSU Information Technology Policy will be referred to the appropriate disciplinary authority for review. Access privileges may be suspended without prior notice if it is determined that a policy violation is causing a current or imminent threat to the confidentiality, integrity, or availability of information technology resources.

DEFINITION OF TERMS

Appropriately Affiliated Members - those associated with the University through the status of current student, faculty, staff, BGSU retiree, BGSU alumni, active BGSU account holder.

Core Values - The Core Values to which the University adheres include respect for one another, cooperation, intellectual and spiritual growth, creative imaginings, and pride in a job well done.

Information - Data, in all its forms, collected, maintained, accessed, combined, or modified by and for members of the University community.

Information Technology (Resource) – All aspects associated with management and processing of information. This includes facilities, technologies, and data used for University processing, transfer, storage, and communications. Examples of these resources, include, but are not limited to, computers, networking equipment, telecommunications equipment, electronic mail, electronic information sources, network bandwidth, wireless devices, video communications, IP telephony, University assigned accounts, voice mail, passwords, access controls, storage media, documentation, personal digital assistants.

Network - a configuration of communications equipment and communication links by any wired or wireless means, that enables resources to be geographically separated, while still connected to each other.

Reconnaissance – An inspection or exploration to gain knowledge of a network's topology, configuration or components.

Safe Computing – Using information technology in a secure manner consistent with its intended purpose. Examples of security measures to be taken, include, but are not limited to, the use of strong passwords that are not easily guessable, are changed regularly and are kept private; the application of all relevant security patches in a timely manner; maintenance of up-to-date virus definitions; backup and protection of important/critical data; security of passwords; protection of data and files.

Security Controls - Any procedure or technology that mitigates the risk of unauthorized users from accessing information technology resources, including, but not limited to, firewalls, encryption, policies, and passwords.

Technology - a method or methodology that applies technical knowledge or tools.

Unlicensed spectrum space - Unlicensed spectrum includes the FCC unlicensed 2.4 Ghz Industrial/Scientific/Medical (ISM) band and the 5.1 Ghz Unlicensed National Information Infrastructure (UNII) band.

User - A user is any person, either authorized or unauthorized, who utilizes information technology resources from any location.

Vulnerability Scanning – The process of proactively identifying vulnerabilities of computing resources in a network in order to determine if and where a resource can be exploited and/or threatened.

ADDITIONAL INFORMATION**Policy Implementation and History**

This policy replaces the Information Technology Services Network and Computer Policies and the Acceptable Use Policy for Information Technologies and is authorized by Office of the Chief Information Officer (CIO) and has been approved by the Information Technology Committee (ITC).

This policy may be supplemented with additional published guidelines by campus units that are authorized to operate/control their own information technology resources provided such guidelines are consistent with and supplemental to this policy and do not alter its intent.

Policy Review and Evaluation

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