BGSU
BOWLING GREEN STATE UNIVERSITY

3341-6-7 BGSU Information Technology.

Applicability	All University units
Responsible Unit	Division of Finance and Administration
Policy Administrator	Chief Information Officer

(A) Policy Statement and Purpose

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.

(B) Policy Scope

The scope of this policy is to encompass all information technology devices owned by the university, any device connected to the university network, and all university data on these devices.

(C) 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, regulations, contracts, and licenses, which include the following:

(a) Digital Millennium Copyright Act (DMCA)

(b) Electronic Communications Privacy Act (ECPA)

(c) Computer Fraud and Abuse Act (CFAA)

(d) Family Educational Rights and Privacy Act (FERPA)

(e) HIPAA Hybrid Entity Designation of Health Care Components and Administrative Responsibilities

(f) Gramm-Leach-Bliley Act (GLBA)

(g) House Bill 104 of the 126th General Assembly (Ohio Rev. Code 1347.12, 1349.19 through 1349.192).

(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.

(a) Information technology is provided to access resources supporting the academic, administrative, education, research and service missions of the university. Use of the provided information technology resources is to be mindful of the university core values. Use of information technology for experimental use or limited social purposes is permitted, as long as it does not violate other policies or interfere with operations of the university.

(b) The legitimate use of information technology resources does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not they are built into the operating system or network and whether or not they can be circumvented by technical means.

(c) Network applications and protocols that are not essential to carrying out the mission of the university or to conduct university business are neither specifically permitted nor specifically prohibited. Should such a subsidiary application or protocol become a risk to the security of the university's information technology infrastructure, its use will be restricted or blocked as deemed appropriate or necessary, without prior notice.

(4) All users must only access or attempt to access information technology resources that they are authorized to use and then only in a manner and to the extent authorized.

(a) Ability to access information technology resources does not, by itself, imply authorization to do so. Prior to accessing a resource, users are responsible for ascertaining and properly obtaining necessary authorization. Accounts, passwords, and other authentication mechanisms, may not, under any circumstances, be shared with, or used by, persons other than those to whom they have been assigned by the university.

(5) Attempting to circumvent information technology security systems is prohibited.

(a) BGSU employs various technologies and procedures in the interest of protecting the confidentiality, availability, and integrity of information technology. Some examples of these technologies and procedures include, but are not limited to, physical methods, firewalls, anti-virus software, encryption, and passwords. Circumvention or attempted circumvention of a security system creates a threat to the university and is not permitted.

(6) Disruption of university-authorized activities is prohibited.

(a) All members of the BGSU community share the information technology resources provided by BGSU. Those causing disruption to the use of information technology resources for other community members will be in violation of this policy. Some examples include, but are not limited to, configuration of devices that disrupt network services, launching denial of service attacks, and disturbing public access resources.

(7) Use of information technology to conduct reconnaissance, vulnerability assessments, or similar activity by unauthorized personnel is prohibited.

(a) In an effort to protect the confidentiality, availability, and integrity of information technology resources, BGSU

officials will investigate any discovered unauthorized network reconnaissance, vulnerability scanning, or service enumerations. While it is recognized that there are some valid purposes for this activity, BGSU officials are unable to determine intent and must react in a manner that will best protect information technology resources by assuming that the source of scans are malicious. Additionally, many vulnerability scanning tools utilize techniques that may be disruptive if not properly used. Please contact the ITS Information Security Office for authorization to conduct vulnerability or service assessments using BGSU information technology resources.

(8) Users are required to protect the confidentiality, integrity, and availability of information technology.

(a) This responsibility includes practicing safe computing at all times when deploying or using BGSU information technology resources. Users are to care for the integrity of technology-based information sources they are authorized to access and to ensure that information is shared only with other appropriately authorized users.

(9) Anonymous use, impersonation, or use of pseudonyms on an information technology resource to escape accountability is prohibited.

(a) Examples of this include, but are not limited to, forging email or using any Internet service not affiliated with the university that can prevent accountability for its usage.

(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.

(a) Information Technology Services (ITS) has implemented wireless Local Area Network (LAN) services on the BGSU main campus and the Firelands campus. While this service allows mobility and easier access to the BGSU network, it means that the air space on campus now serves as a medium for network connectivity. The use of open air space poses a number of potentially difficult situations for both users and network administrators. Users who may need to make use of wireless equipment for special purposes such as research or other unique applications must contact ITS to coordinate this use of wireless air space.

(b) Effective July 1, 2024, access to the BGSU network will transition to a “wireless-first” approach. As of this transition date, all technology equipment purchases must support wireless networking (Wi-Fi). Exceptions to this policy include devices which require Power over Ethernet (PoE),

security cameras, door access systems, IP phones, certain building automation equipment and life safety devices. Additional exceptions to this policy may be evaluated on an individual case basis and must be submitted as an ITS (Information Technology Services) ticket. To further support this wireless-first initiative, future building construction or renovations will have one network wired port per office or single occupancy space.

(11) Responsibilities

(a) University Responsibilities

(i) 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.

(ii) Communicate, review, update, and enforce policies to protect information technology resources.

(iii) Take reasonable measures to mitigate security threats.

(b) User Responsibilities

(i) Read, agree to, and abide by all university policies and policy updates.

(ii) Practice safe computing when using information technology resources.

(iii) 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.

(iv) Users are responsible for activity resulting from their assigned information technology resources.

(12) 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 university policy or 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, university 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 practicable. 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.

(D) 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.

A violation of this policy may result in disciplinary action, up to and including termination of employment.

(E) Implementation of Policy

This policy is authorized by the Office of the Chief Information Officer (CIO) and has been approved by the appropriate university committee(s). 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.

(F) Related Policies

(1) 3341-6-6 BGSU E-Mail Account

(2) 3341-6-18 Data Use and Protection

(3) 3341-6-21 Faculty and Staff Email

(4) 3341-6-29 ITS Computer Lab Utilization

(5) 3341-6-33 My VPN

(6) 3341-6-39 Sensitive Data Privacy

(7) 3341-6-41 Social Networking Media Policy

(8) 3341-6-43 Student Email

(9) 3341-6-49 BGSU Web Privacy Policy

(10) 3341-3-84 HIPAA Hybrid Entity Designation of Health Care Components and Administrative Responsibilities

Equity impact statement: The policy has been assessed for adverse differential impact on members of one or more protected groups.

Registered Date: March 17, 2015
Amended Dates: March 31, 2016; December 22, 2017; April 1, 2024