

INFORMATION TECHNOLOGY USERS' PRIVILEGES AND RESPONSIBILITIES

BALL STATE UNIVERSITY INFORMATION SECURITY SERVICES

1. INTRODUCTION

Information technology plays a crucial role in the delivery of Ball State University's educational mission. In making use of these shared resources, members of the university community have a responsibility to help create an intellectual environment in which students, faculty and staff may feel free to create and collaborate with colleagues both on and off campus without fear that the products of these efforts will be violated by misrepresentation, tampering, illegal access, destruction, or theft. This policy outlines the ethical and acceptable use of information systems and resources at Ball State University as well as the duties and responsibilities incumbent upon everyone who makes use of these resources.

2. SCOPE

This policy applies to all students and employees, as well as all others who make use of Ball State University information technology resources and services. Violations of this policy are unethical and possibly unlawful and may result in sanctions as discussed below.

3. AVAILABILITY OF SERVICES

The university takes all reasonable steps to ensure that information technology resources are free from errors, viruses, and malicious activity by conducting regular security scanning of production systems and engaging in proactive security monitoring. However, due to the fact that information technology infrastructure is composed of a wide variety of systems including personal computers not under the control of the university, Ball State University does not guarantee that the safety or reliability of services or access are free from all dangers.

Ball State University will make reasonable efforts to maintain the confidentiality of the storage contents and to safeguard the contents from loss, but cannot be held liable for the inadvertent or unavoidable loss or disclosure of the contents, or for disclosure resulting from the unlawful acts of others. Because of these limitations, services and access are provided on an "as is" basis and to the extent permissible by law, the university hereby excludes all implied warranties and guarantees of availability or quality of services, including without limitation any expectation as to skill and care or timeliness of performance.

4. CENSORSHIP

Freedom of expression and preservation of an open environment within which to pursue scholarly inquiry and to share information is central to the academic mission of Ball State University. While freedom of expression will generally be protected, users of institutional systems must also respect the legal and ethical boundaries of such usage.

Ball State University reserves the right to limit or restrict the use of its information technology resources based on institutional priorities and financial considerations. Content found to be inconsistent with institutional purposes is subject to immediate suspension or removal by the administrator of the relevant system or their designee. Conduct and related content does not meet the institutional purposes of the university when it is found to be:

- a. In possible violation of federal, state, or local laws.
- b. May violate the copyright or other intellectual property rights of others.
- c. Harassing or threatening, or otherwise disruptive to the learning or working environment.
- d. In violation of other university policies, procedures, or contractual obligations.
- e. Inappropriate for the stated purpose of the system, service, or environment.

- f. A security risk affecting the confidentiality, integrity, or availability of services.
- g. Otherwise inconsistent with the mission of the university.

Anyone who becomes aware of conduct or content on university systems which may be in violation of the above requirements should report the incident as described in the *Reporting Suspected Security Breach or Policy Violation* section below.

Users whose information is removed will be notified of the removal as soon as is feasible. Users who wish to appeal such removal may do so through an appeal board made up of the governing body appropriate to the system and status of the user. If no appeal board exists the appeal may be made to the Director of Information Security Services.

5. CONFIDENTIALITY

In general, and subject to applicable law, the university reserves the right to access files, documents, and other information residing on university-owned or controlled equipment and services. All such infrastructure is subject to the policies of Ball State University, and the university may exercise its ability under certain circumstances to access, restrict, monitor and regulate these systems. Policy for such monitoring and access is described below:

a. Administrative Monitoring And Inspection

Although the university retains ownership and rights as described above, monitoring and administrative inspection of electronic systems will be strictly controlled. Any such monitoring will be governed by applicable U.S. and Indiana laws and by university policies. Monitoring of information systems communications may only be conducted when there is evidence or reasonable belief that there is risk of activity inconsonant with institutional purposes as defined above. Each such incident of monitoring and inspections of information systems or communications will be approved in advance by the Director of Information Security Services or his/her designee having the written pre-approval of the Assistant Vice President for Information Technology to engage in such monitoring and inspections. The Director of Information Security Services will establish detailed written technical procedures for such monitoring and will ensure ongoing adherence to such procedures. Records of all monitoring activity will be maintained by the Director of Information Security Services and shared with the Assistant Vice President for Information Technology. When monitoring reveals evidence of a violation of the law or university policy, the results of such monitoring will be reported to appropriate university administrators and may be shared with external entities including law enforcement agencies.

b. Non-Intrusive Monitoring

All users of university systems should be aware that non-intrusive monitoring of campus network traffic and security scanning of information systems occurs routinely, to assure adequate confidentiality, availability, and integrity of university systems and to identify and resolve problems. When problem traffic patterns suggest that information security, integrity, or performance has been compromised, Information Security staff will investigate and protective restrictions, including the commencement of intrusive monitoring as described above, may be applied until the condition has been rectified.

c. University Employees

University employees are provided with the use of university resources for work-related purposes. Accordingly, employees may be directed to produce certain work files or to make the information in a computer account accessible to a supervisor or other employee. In the event that business-related files stored on an employee's account or workstation become inaccessible because of absence, death, or severance of employment from the university, the supervisor of the department may request access to such business-related files be granted to an alternate employee.

d. Public Records

Under Indiana law (Indiana Code 5-14-3) any official university documents in the files of employees of the State of Indiana may be found to be a public document, and hence subject to inspection through the public records act.

e. **Other Administrative Access**

Under certain circumstances, the Director of Information Security Services in consultation with the Assistant Vice President for Information Technology may authorize access to certain information by third parties. For example, personal e-mail or other communications may be released to the relatives of a deceased student or employee. In such circumstances, the Director of Information Security Services will direct the technical information access procedures and will document each such incident in writing to the Assistant Vice President for Information Technology.

6. PERSONAL & COMMERCIAL USAGE OF INFORMATION TECHNOLOGY RESOURCES

Ball State University information technology resources exist to support the university's mission of education, research, and public service. These facilities and resources are provided in large part by funding from taxpayers of Indiana for the academic use of our students, faculty and staff. We all must be responsible stewards of these resources. Generally the use of university information technology resources is limited to institutional purposes such academic research, study, instruction, discharge of employee duties in conjunction with official business of the university, and other purposes related to university sanctioned activities. Personal and commercial usage is governed by the following policies:

a. **Permitted Personal Usage**

Incidental personal usage of Ball State University information technology resources by students and employees of the university is acceptable, provided the usage adheres to all applicable university policies and does not result in additional costs to the university. Note that licensing of some software and information systems is restricted to educational use only and hence may not be used for even incidental personal purposes unless permitted within the terms of the relevant license agreement.

b. **Permitted Commercial Usage**

The use of Ball State University information technology systems for academically related but commercial purposes is permitted only with approval of the Office of Academic Research and Sponsored Programs. Researchers who require substantial computer resources as part of grants and consulting contracts may be required to reimburse BSU for a portion of the resource costs.

c. **Personal and Commercial Uses Not Permitted**

Technology resources, including Internet access through the university network, may not be utilized in ways which may be inconsistent with the university's tax-exempt status or legal obligations, such as using university systems for hosting or advertising commercial services for private financial gain, political campaigning, or services to outside organizations not recognized by the university as being entitled to make use of university resources. Personal usage of a nature disruptive to the learning or working environment, such as subjecting other members of the university community to pornographic content unrelated to an academic purpose is also prohibited. Under no circumstances may incidental personal or commercial usage involve violations of the law, interfere with the fulfillment of an employee's university responsibilities, or adversely impact or conflict with activities supporting the mission of the university.

7. INDIVIDUAL RESPONSIBILITIES

Thousands of students, faculty and staff share information technology resources at Ball State University. Irresponsible usage by even a small number of users has the potential to seriously disrupt the work of others within the community. All users are expected to exercise due diligence in the care of their own information, and to be civil and respectful of other users of these systems and technology resources. The following responsibilities are incumbent upon all users of Ball State University Information Technology resources:

a. **General Requirements**

i. **Liability for Personal and Harassing Communications**

Individual users are responsible for their own words and actions. Other than official publications, the university is not expected to be aware of, and is not responsible for, material that individuals may post, send, or publish. Harassing communications are prohibited and include repeated contacts with a person who has requested to be left alone absent some legitimate institutional purpose for such communication. Harassment may also involve malicious public disclosure of private facts, threats, defamation, and vulgar or repulsive content posted about an individual or group.

- ii. **Responsibility to Read E-Mail from the University**

Certain official communications from the university are delivered to students and employees through their assigned e-mail address. Each person has a responsibility to maintain and regularly check their e-mail account, whether hosted at Ball State University or elsewhere, and to ensure their account is capable of receiving these official communications so that important email messages sent by the University are not missed.
 - iii. **Reporting Suspected Security Breach or Policy Violation**

Anyone who discovers or suspects an information security breach involving confidential information of the university has a duty to report the breach to the Office of Information Security Services by e-mail at security@bsu.edu or by phone at 765-285-1549. Reporting must not be delayed in order to collect more information or to make a determination if a breach has actually occurred.
- b. Responsibility to Protect Confidential Information And Access**
- i. **Ability to Access Does Not Grant an Unlimited Right**

Legitimate use of resources does not extend to whatever one is capable of doing with them. Although information security controls may permit access, a person may not access confidential information unless they have some legitimate reason for doing so. For example, employees with access to confidential student records have no right to access them absent an approved legitimate business purpose.
 - ii. **Sharing of Passwords Is Prohibited**

User accounts are generally assigned to individuals and may not be shared with any other person. No university employee or student may ask for a password assigned to another person. Where there is a legitimate need for access, proxy rights or similar methods may be used which do not require the sharing of individually assigned passwords.
 - iii. **Disclosure of Confidential Information to Third Parties**

Unauthorized access or disclosure of confidential information or information otherwise protected by the university is prohibited by Indiana and federal law. Questions regarding appropriate access or disclosure of information should be directed to the area of the university having administrative responsibility for it, typically Business Affairs, Student Affairs, or Marketing & Enrollment Management as appropriate.
 - iv. **Access Revocation Upon Change of Position or Severance of Employment**

Employees have a duty to renounce access to confidential information upon severance from the university or a change in position in which such access has not previously been approved. Supervisors of employees having such access must ensure that access rights have been revoked upon such severance or change in position or status.
- c. Responsibility to Refrain From Doing Harm**
- I. **Minimum Standards for Connected Systems**

Students, employees, and guests of the university who connect computer systems to the university network have a duty to ensure that these systems are free from malicious software including viruses, spyware, root kits and other programs which may attempt to flood or attack other university system. Computers or devices which do not meet minimum standards may be isolated and disconnected without notice.
 - II. **Subversion of Security**

Attempted bypass or subversion of security restrictions is prohibited. Unauthorized attempts to access files, passwords, or other confidential information of others, and unauthorized vulnerability scanning of systems other than those owned by the user is prohibited without prior approval of the Director of Information Security Services.
 - iii. **Misrepresentation of Identity**

Using information systems to initiate or continue communications using the name or identity of another person without the explicit authorization of the person whose identity is being impersonated is prohibited.

8. POLICY REGARDING DEPLOYMENT OF INFORMATION SYSTEMS

Policies and standards regarding information security and deployment of information systems are contained within the *Production Information Systems Integration and Supportability Standards, Procedures, and Practices* which can be found at <http://www.bsu.edu/security/itpolicy/>. These policies apply to all production information systems at Ball State University.

9. SUSPENSION OF SERVICES AND OTHER SANCTIONS

Access to university information technology resources is a privilege. Violations of the above policies and standards may result in penalties ranging from a reprimand and temporary loss of access, to referral to the appropriate university office for imposition of further evaluation and possible sanctions including the possibility of expulsion from the university and dismissal from a position. Student conduct utilizing information technology resources or facilities which may violate the Code of Student Rights and Responsibilities will be referred to the Office of Student Rights and Community Standards for possible disciplinary action. Certain violations of this policy may also be prohibited under Indiana or federal law, and are therefore subject to possible criminal prosecution.