INFORMATION TECHNOLOGY USERS' PRIVILEGES AND RESPONSIBILITIES

BALL STATE UNIVERSITY OFFICE OF 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 may result in sanctions as discussed in Section 10 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 is not 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. CONFIDENTIAL INFORMATION

Ball State University is dedicated to safeguarding and maintaining the confidentiality, integrity, and availability of our student, employee, organizational information, and information technology resources. "*Confidential Information*" includes all files, data, information, contracts, agreements, specifications, analyses, studies, samples, drawings, photographs, documents, numbers, proposals, and other information, whether verbal or written, that an employee receives or learns in connection with the employee's assigned duties or interactions with a division, unit, or area, or that may impact the confidentiality, integrity, or availability of information technology resources. *Confidential Information* may be paper-based, electronic, or stored or transmitted in some other form. *Confidential Information* does not include information that is in the public domain, such as handbooks and other general information published on the university's website.

Examples of *Confidential Information* include, but are not limited to, the following:

a. Academic information, such as grades and class schedules
b. Bank and credit card account information, income, credit history, and consumer report information
c. Disciplinary or employment records or related information

d. Loan information, including loan applications and loan servicing, collection and processing
e. Money wiring and other electronic funds transfers
f. Other non-public financial information, including personally identifiable information relating to a financial transaction
g. Social Security Numbers, driver's license numbers, or similar identification codes or numbers
h. Student account balance information, financial aid information
i. Donor information
j. Information security procedures, policies, and capabilities surrounding the university's information technology resources and systems
k. Information security credentials (e.g., username and password combination, multi-factor authentication tools, PIN keys, etc.)
l. Work plans and other documents and information deemed confidential for the effective and efficient operation of the university.

At times, *Confidential Information*, as defined by the university, may be subject to disclosure pursuant to a public records request filed with the Office of General Counsel or other legal obligation. However, employees are expected to abide by the definition in this policy and, unless it is a part of their job responsibilities, should not attempt to determine whether information is disclosable under any state or federal law, or otherwise assume that it is disclosable. Furthermore, the existence of information in a publicly available format or medium does not imply approval to otherwise disclose it. For example, certain employee and student directory information (such as telephone numbers and street addresses) may appear in a printed directory; however, disclosure of the same information in another format (such as an electronic file) requires separate approval from an authorized official of the university and, if necessary, the subject(s) of the information.

5. Freedom of Expression & Removal of Content

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. However, the university's information technology systems are not intended to be public forums, but rather are designed to support specific teaching, learning, working, research, and administrative activities of the institution. As such, Ball State reserves the right to utilize its information technology resources in a manner that supports these activities and to adjust the types and levels of systems available.

Content may be removed from the university's information technology systems in a manner consistent with the university's Statement on Rights and Responsibilities, Commercial Activity on University Property policy, and Non-Commercial Expressive Activity and Assembly on University Property policy. Likewise, Ball State reserves the right to remove content from its information technology systems for information-technology-specific reasons such as storage limits, systems management, spam cleanup, error or bad data removal, information security, and general system maintenance.

In addition, Ball State may reasonably regulate the time, place, and manner of expression on its information technology systems to ensure they do not disrupt the teaching, learning, working, research, and administrative activities of the university. As examples, this may result in the removal of content that is incongruent with the stated purpose of a given system or forum, would cause the university to violate a contractual obligation with a third party, or constitutes a security risk affecting the confidentiality, integrity, or availability of services.

If a person has a concern about content on the university's information technology systems, contact the Office of Information Security Services at security@bsu.edu. If a person wishes to appeal the removal of any content from the university's information technology systems, the person must follow the procedures outlined in the Commercial Activity on University Property policy or Non-Commercial Expressive Activity and Assembly on University Property policy, as applicable, including submitting a written appeal to the Vice President for Information Technology and Chief Information Officer within the required timeframe.

6. Monitoring & Accessing Information

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, including @bsu.edu email accounts and other Ball State information technology systems, without prior notice, and users therefore should have no expectation of privacy when utilizing such resources. All such infrastructure is subject to the policies of Ball State University, and the university may access, restrict, monitor and regulate these systems. The 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 and only at the approval of the Vice President and General Counsel or the Vice President of Information Technology or their designee. Each such incident of monitoring and inspections of information systems or communications will be approved in advance by the Vice President and General Counsel or the Vice President of Information Technology or their designee. Technical controls for monitoring will be coordinated through the Executive Director of Information Security, who will establish detailed written technical procedures for monitoring and inspection and will ensure ongoing adherence to such procedures. Records of all monitoring activity will be maintained by the Executive Director of Information Security and immediately reported to the 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. Other Monitoring And Controls

All users of university systems should be aware the university will audit, log, review, and utilize information stored on or passing through networks or services for many reasons such as attack detection, assuring compliance with applicable law and university policy, retrieving or diverting information needed to conduct university business, or other administrative purposes. Such 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, the Office of Information Security Services staff will investigate and engage appropriate tools, techniques, and methods as may be necessary to ensure the security of the environment.

c. Data Access By University Employees

University employees are provided with access to university data for approved work-related purposes only. Employees are subject to additional polices published at https://www.bsu.edu/security/itpolicy/ and should check with their supervisor or the applicable data access policy with questions regarding data access or use.

d. Public Records

Under Indiana's Access to Public Records Act (Indiana Code 5-14-3 et seq), public records are subject to disclosure upon request (unless the Office of General Counsel determines that an exception to the law applies). Any records maintained by the university, including paper copies and documents and communications located in @bsu.edu email accounts or other Ball State information technology resources, may be found to be a public record.

e. Ball State Email Accounts

@bsu.edu email accounts are university-owned accounts for which students and employees are granted access in order to conduct university-related activities. These accounts should not be viewed as personal accounts, and users should compose electronic communications with recognition of the fact that any content could be accessed and reviewed and that these communications could be forwarded, intercepted, printed, or stored by others. Though it is not routine practice, at all times supervisors may access the @bsu.edu accounts of their subordinates in order to ensure university business is being properly and timely conducted. In addition, Information Technology may recall, delete, or block emails or other electronic records from university accounts that contain viruses, malware, were sent by the university in error, or where job functions or access rights are adjusted because of a change in employment, job duties, or other status.

f. Other Administrative Access

Under certain circumstances, the Executive Director of Information Security in consultation with the 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 Executive Director of Information Security will direct the technical information access procedures and will document each such incident in writing to the Vice President for Information Technology.

7. 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 Research Integrity. 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.

8. 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 information contained within Ball State's information technology resources, and to use these systems and technology resources responsibly. The following responsibilities are incumbent upon all users of Ball State University Information Technology resources:

a. General Requirements

i. Liability for Personal 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.

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*, including inappropriate access or disclosure, has a duty to report the situation 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. Ball State's procedures for Reporting a Suspected Information Security Incident contain additional information on this topic.

b. Responsibility to Protect Information And Access

i. Device Security

If any device under an employee's control—including personal computers, tablets, laptops, and other similar devices—may be used to access, transmit, or store *Confidential Information*, the employee must maintain the security of the device, including running certain security and management software as configured by Information Technology, the use of a password, using password protected "screen savers", utilizing approved antivirus and antispyware software, and any other measures as may be required under IT policies and procedures. Required tools provide security, management, and inventory funds and are centrally managed and administered by Information Technology. All mobile devices connecting to university resources, such as email, will also be configured with security parameters to prevent data theft. The employee must also maintain security by refraining from sharing passwords or multi-factor authentication tools, as well as accepting approved prompts to update and patch university systems. The employee should also remove any software that is no longer needed and promptly install and update security patches and updates for all software installed on their device.

ii. Sharing of Passwords Is Prohibited

User accounts are generally assigned to individuals and may not be shared with any other person. The person to whom the account is assigned is responsible for the account's usage. Passwords should not be disclosed to anyone, nor should anyone be given access to a Ball State information technology system using someone else's username and password. 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. If there is a reason to believe a password has been lost, stolen, or otherwise compromised, the matter should be immediately reported to the IT Helpdesk (765-285-1517) so that the password may be disabled or reset.

iii. Employee Duties And Responsibility To Protect *Confidential Information*

Employees must safeguard and maintain the confidentiality, integrity, and availability of all *Confidential Information* at all times, and only access, use, and/or disclose the minimum *Confidential Information* necessary to perform their assigned job duties. *Confidential Information* may be disclosed to other individuals or organizations only for legitimate business, research, or academic purposes and only after approval has been received from an authorized official of the university. Employees must also be aware and are subject to additional policies published at https://www.bsu.edu/security/itpolicy/.

iv. Downloading or Transmitting of *Confidential Information* is Prohibited

Employees are prohibited from downloading or extracting *Confidential Information* to any removable storage, such as external hard drives, compact discs, or SB flash discs, or transport or transmit such information off-site or to any non-university owned system or entity without explicit approval to do so from the owner of the information, with prior technical review by the Executive Director of Information Security or designee.

v. Duty to Renounce Access

In the event that an employee's duties and responsibilities or job assignment changes, or if their employment with the university ceases for any reason, the employee is responsible for continuing to maintain the confidentiality, integrity, and availability of all *Confidential Information*. The employee is also responsible for promptly notifying the appropriate information technology systems administrator or the Office of Information Security Services so that the employee's access to *Confidential Information* may be properly curtailed or removed. All employees are prohibited from accessing or disclosing *Confidential Information* in a manner inconsistent with their current job duties or after their employment with the university ends.

vi. Must Follow Off-Boarding Processes

If an employee's employment with the university ends, the employee is expected to follow all human resource and information technology off-boarding processes, including those related to the retention/destruction of records,

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*, and unauthorized vulnerability scanning of systems other than those owned by the user, is prohibited without prior approval of the Executive Director of Information Security.

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.

9. Policy Regarding Deployment of Information Systems

Policies and standards regarding information security and deployment of information systems and handling university data along with related procedures can be found at http://www.bsu.edu/security/itpolicy/. These policies, procedures, and standards apply to all information systems and data processing at Ball State University.

10. 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 Conduct 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 or other legal sanctions.