

Model Confidentiality and Information Access Agreement

This model *Confidentiality and Information Access Employee Agreement* (“Agreement”) or a substantially similar agreement tailored to the specific Vice Presidential area must be read, signed, and complied with by all employees having access to *Confidential Information*, whether as a part of their assigned duties or which they may encounter as a consequence of working in an organizational unit which handles such information.

Model Confidentiality and Information Access Employee Agreement:

Ball State University is dedicated to safeguarding and maintaining the confidentiality, integrity, and availability of our student, employee, and organizational information. “*Confidential Information*” includes all of this information that is personally identifiable and non-public. *Confidential Information* may be paper-based, electronic, or stored or transmitted in some other form. Examples of *Confidential Information* include, but are not limited to, the following:

1. Academic information, such as grades and class schedules
2. Bank and credit card account information, income, credit history, and consumer report information
3. Disciplinary or employment records or related information
4. Loan information, including loan applications and loan servicing, collection and processing
5. Money wiring and other electronic funds transfers
6. Other non-public personally identifiable information relating to a financial transaction
7. Social Security Numbers, drivers license numbers, or similar identification codes or numbers
8. Student account balance information, financial aid information

The existence of information in a publically 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 the printed Ball State University Directory; however disclosure of the same information in another format (such as an electronic file) requires separate approval from an authorized individual.

Protection of *Confidential Information* requires the following minimum standards, to which I agree as a condition of my continued employment:

- 1. Download or Transmission of Confidential Information:** I will not download or extract Confidential Information to any removable storage such as compact discs or USB flash discs, or transport or transmit such information off-site or to any non-university computer system or entity without explicit approval to do so from the owner of the information, with prior technical review by the Information Security Officer or designee.
- 2. Access to Confidential Information:** I understand and agree that I must safeguard and maintain the confidentiality, integrity, and availability of all *Confidential Information* at all times. I will only access, use, and/or disclose the minimum *Confidential Information* necessary to perform my assigned duties. I will disclose such information to other individuals/organizations only for legitimate business, research or academic purposes and only after I have received prior approval to do so from an authorized individual.

- 3. Desktop and Laptop Computer Security:** If any computer under my control may be used to access, transmit, or store *Confidential Information* I will to the best of my ability maintain the security of this computer including the use of passwords, password protected “screen savers”, approved anti-virus and anti-spyware software, and other measures as may be required under UCS policies or procedures. I will refrain from using unapproved “adware”, “shareware”, “freeware”, or any other unauthorized software. I will also remove any software that is no longer needed and promptly install and update security patches and updates for all software installed on my desktop or laptop computer system.
- 4. Server Hosting:** I understand that procedures for hosting servers or information systems are covered by a separate set of procedures (the UCS “Hosting Agreement”) and that I will comply with the provisions of such before initiating the acquisition process, deployment, or selection of servers or services.
- 5. Duty to Protect Passwords:** I understand that the username(s) and passwords I have been assigned are *Confidential Information* for purposes of this Agreement, and that I will be held accountable for their use. I will not disclose my password(s) to anyone nor will I allow anyone to access any Information System using my assigned Username and Password for any reason. In the event my password is lost, stolen, or if I should have reason to suspect it has been compromised, I will immediately notify the UCS Helpdesk (765-285-1517) or Computer Operations (765-285-1549) so that my password may be disabled or reset.
- 6. Duty to Renounce Access:** In the event my duties and responsibilities or job assignment changes, or in the event my employment with the university ceases for any reason, I affirm that I will maintain the confidentiality, integrity, and availability of all *Confidential Information* and will promptly notify the appropriate Information Systems administrator or other authority so that my access to *Confidential Information* may be property curtailed or removed.
- 7. Information Security Breach:** I will immediately report any suspected breach of any Information System as directed in the official procedures for *Reporting An Information Security Incident Or Suspected Violation*.
- 8. Policy Violations:** I will immediately report suspected policy violations, such as inappropriate access or disclosure of *Confidential Information*, to the Office of University Compliance. In no event will I disclose suspected violations or breach to any person or entity other than the *Director of University Computing Services, the Information Security Officer, the Office of University Compliance, UCS Computer Operations after-hours support (765-285-1549)* or others as I may directed.
- 9. Appropriate Use:** I will not use Ball State University information systems to transmit, retrieve, or store any communications consisting of discriminatory, harassing, obscene, solicitation, or illegal information. Other aspects of appropriate use are covered in the *Information Technology Users’ Privileges and Responsibilities* policy.
- 10. Security Monitoring/Testing Software or Hardware:** I will not use software, tools, or techniques (human, technical, or otherwise) designed or intended to break/exploit or “test” security measures without explicit approval from the Office Of Information Security Services (OISS).

11. Audit & Security Review Of BSU-Owned Computer Systems: I understand that I have no expectation of privacy in any information accessed or created by me on BSU-owned computer systems during my employment with Ball State University. Ball State University may audit, log, review, and utilize information stored on or passing through university owned networks or computers for many reasons, such as to maintain the confidentiality, security, and availability of *Confidential Information* and to assure compliance with university policy.

12. Sanctions: I understand that violations of this Agreement may result in disciplinary action as described in the applicable employee handbook, up to and including termination of employment, suspension and loss of privileges, termination of authorization to work with *Confidential Information*, as well as legal sanctions.

Please refer any questions related to this Agreement to your supervisor
or the *Information Security Officer*.

By signing this Agreement, I acknowledge that I have read and fully understand and agree to comply with all of its terms and conditions. I also understand that Information Technology will revoke my current access and/or deny me future access to BSU-owned computer systems unless I sign, date and return this Agreement in a timely manner.

Employee's Signature

Date

Employee's Printed Name

Date

Please Return This Completed Agreement To Your Department Or Unit Head