BALL STATE UNIVERSITY
NEW EMPLOYEE INFORMATION TECHNOLOGY SECURITY DOCUMENTATION

Policies, Procedures and Forms
Information technology policies form the foundation of any security infrastructure. They define how information technology will approach security. They define how employees and students need to approach security, and how certain incidents will be handled. As part of the onboarding process, new employees are encouraged to read and sign the **Employee Confidentiality Agreement** *(also titled "Model Confidentiality and Information Access Agreement"). *[**Links**](#) **to this form and all current versions of the policies, procedures and forms**, are available at: www.bsu.edu/security/itpolicy. Below are the Ball State information technology policies, procedures and forms that affect you as an employee or student.

Policies:

- **Information Technology Users' Privileges and Responsibilities:** Overall policy for all employees which 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.

Procedures and Standards:

- **Authentication and Access Control Standards**
- **Remote Password Reset Procedure**
- **Report a Potential Security Breach:** This policy describes procedures employees must follow when an information security breach is suspected and outlines the roles and responsibilities for incident response when an actual breach has occurred. This policy applies to all university employees and all individuals having access to information for which the university has a duty to protect.
- **Procedures for Hosting Information Systems Managed by Units**
- **Guidelines for Copyright Compliance**

Policy and Procedures Related to University Data:

- **Data Management Procedures and Governance Structure:** If you are responsible for maintaining or using university information in your department, this guide will help you understand who and where to contact for help as well as how university data is management is organized.
- **Cellular Phone and Data Procedure:** This procedure describes the options and requirement for a University Employee to either (1) request reimbursement for a cellular phone or cellular data device, or (2) request purchase or assignment of a university-owned cellular phone or cellular data device.
- **Transfer or Disposal of Computers, Storage Media, and Paper Documents**

Forms:

- **University Guest Account Access Request**
- **Employee Confidentiality Agreement:** This Model Confidentially and Information Access Employee Agreement must be read, signed, and complied by all employees having access to Confidential Information.
- **University Data Stewards:** A list of individuals who can be contacted for access control of student and university data.
- **Electronic Information Access Form**