Information Technology
Authentication and Access Control Standards

Ball State University Information Security Services

1. Introduction

Ball State University information systems contain sensitive information assets which are crucial to the ongoing operation of the university, and for which the University has a legal obligation to protect from inappropriate disclosure. The following standards define authentication and access control requirements necessary to safeguard these assets from unintended disclosure.

2. Scope & Application of These Standards

These standards apply to all students, employees, outside persons or organizations as well as any other entities accessing or using Ball State University information systems.

3. Confidential Information

For purposes of these standards, *Confidential Information* includes all information for which the University has a responsibility to protect from inappropriate disclosure. Persons having access to *Confidential Information* have a heightened responsibility to insure systems and passwords are not compromised.

4. Authentication and Access Controls Defined

Authentication establishes identity, while access permissions define the set of resources available to an individual who has been authenticated. Authentication is generally provided by the campus *Enterprise Directory Authentication Service*, while access permissions are controlled by local systems administrators. For example the local administrator of a sensitive financial-records system may remove this access from an employee upon their retirement; however the same employee might retain access to general services such as e-mail.

5. Responsibility to Revoke Access Permissions

Local systems administrators have a responsibility to monitor their environments and remove access from individuals no longer having a demonstrated need for such information. The review process for such removal must occur immediately upon change of employment status or assignment. Additionally, local administrators must regularly (not less than twice yearly) document a review the access permissions list for their systems.

6. Access Permissions Do Not Grant Unrestricted Access Rights

Although an employee may have electronic access permissions to read or modify institutional data, such permissions do not grant blanket authority to access or modify such information. All access to confidential information must be for a bona fide institutional purpose consistent with official responsibilities and assigned duties.

7. PERMITTED AUTHENTICATION SYSTEMS

The primary authentication mechanism for all Ball State University information systems is the *Enterprise Directory Authentication Service* (EDAS). All Ball State University employees and students are eligible to receive a BSU Computer username and password for this service. Generally students receive these credentials during the admission process, which employees obtain them by visiting the UTS Information Desk at BL101. Additional authentication systems apart from the EADS include the IBM RACF system, as well as other permitted methods described below.

a. BSU Computer Username and Password: Where practical and approved, all information systems requiring authentication of employees or students will use EDAS. This system provides standards based LDAP, Kerberos, NTLM authentication services employing strong encryption. The system is also built on a distributed model which is highly available, secure, and interoperable with existing and emerging technologies and complies with Technical Password Requirements as described below. Contact the Office of Information Security Services (OISS) for additional information before attempting to integrate with this authentication system, which requires certain technical protocols be followed to ensure security is maintained.

b. Resource Access Control Facility (RACF): The RACF system controls certain administrative access to application software running on the university IBM mainframe. No systems outside the IBM mainframe use the RACF credential. The RACF system complies with Technical Password Requirements as described below. Only employees with demonstrated and approved need to access applications running on the IBM mainframe are granted access to use this authentication method.

c. Other Permitted Authentication Systems: Methods of authentication other than the two described above should be avoided, but are sometimes necessary due to systems incompatibility or other reasons. Such systems must be approved by OISS prior to acquisition, development, and deployment. These systems must comply with the Technical Password Requirements described below. Purchased, developed, and acquired systems must be evaluated to include proper support for integration with EDAS.

8. PASSWORDS RESPONSIBILITY AND GENERAL PROCEDURES

a. Responsibility: Each person is individually responsible for compliance with these procedures, and for keeping passwords secure by not sharing or treating them in a way others may discover them. Suspected disclosure or compromise of a password to any other person must be immediately reported to OISS and the password changed.

b. Password Distribution Procedures: Initial usernames and passwords must be distributed in a manner so as to limit the number of people having opportunity to learn the initial password. Username/password combinations distributed on paper shall be either handed directly to the account owner immediately upon printing (walk-up stations) or delivered to the account owner via envelope sealed at the point of origin and delivered through a secure method. Passwords shall not be saved or archived by the issuing office in a recoverable format for any reason. Contact OISS for additional information concerning password distribution procedures.

c. Password Reset Procedures: Password resets performed through walk-up procedures require that the account owner to appear in-person and to present valid government or university issued picture identification. Under no circumstances may passwords be reset and released to anyone but the account owner. Passwords may never be given out over telephone for any reason. Automated resets such as by pre-registration of alternate trusted addresses are permissible, as are certain “remote” reset options for people traveling outside of Indiana. Such special procedures must be approved in advance from OISS and are described in *Remote Password Reset Procedures.*

d. Use of Assigned Usernames and Passwords: Assigned usernames and passwords are only to be used on official university managed systems. Passwords used to access Ball State University information systems may not be transmitted to any information system or service outside the university for any purpose. Under certain conditions services external to the university may rely on successful EDAS authentication (such as certain zero knowledge authentication methods) however approval for external systems authentication integration is required from OISS before implementation.

e. **Sharing of Passwords**: Passwords are issued to individuals and must not be shared or transferred to any other person including other employee, friend, family member, vendor or external provider. No EDAS or RACF accounts shall be used as shared-password accounts. Departmental EDAS accounts are not intended for shared-password access; proxy access may be granted to any EDAS account, which will provide the same functionality without the need for sharing passwords.

f. **Disclosure for Support Purposes**: No university employee is authorized to ask or demand the disclosure of a password for any of the permitted authentication systems (as described above) in the course of providing support services. Vendors requiring access to production systems for support purposes will be granted necessary access as provided in the *Accounts for Vendor & Partner Support* section below.

9. TECHNICAL PASSWORD REQUIREMENTS:

Passwords provide an important layer of information security. Selecting a strong password and keeping it confidential is an important part of securing Ball State University information assets. Although servers and systems will be configured to enforce these standards as closely as possible the ultimate responsibility for compliance with these requirements and for maintaining the secrecy of passwords remains with the individual.

a. **Length**: Passwords may be no less than eight characters in length. Longer passwords are preferred, as are so-called "passphrases" which may include spaces and a series of words. Systems not supporting at least eight character passwords shall be secured by some additional approved method providing enhanced security. Generally, longer passwords increase security as they are hard to guess.

b. **Complexity**: Passwords must contain a combination of at least three of the following groups of characters: (1) upper case letters (2) lower case letters (3) numbers (4) special characters such as punctuation or symbols. Passwords may not contain the username or the proper name of the individual, nor may they contain information specifically identifiable to the account owner such as the name of a pet, sibling, or spouse. Password complexity enhances security by reducing vulnerability to dictionary and related attacks.

c. **Expiration**: Unless other compensating controls are in place to prevent exhaustive password guessing, passwords must be changed at least once every six months. Where possible, user accounts not used for authentication purposes for a period of six calendar months should be disabled. Re-enabling accounts will follow a procedure not less stringent than that described below for password reset. Disabling inactive accounts helps limit the number of accounts open to attack.

d. **Change Before Use**: Upon account creation or password reset procedures described below, the account password must be changed by the account owner before use. Requiring a password change insures before use helps insure the active password is only known to the account owner.

e. **Authentication Failure Lockout**: After no more than five consecutive login attempt failures, the system being accessed shall lock out the attempted account username for a period for not less than five minutes. Temporary lockouts increase security by helping to make password guessing attacks infeasible.

f. **Reporting of Password Failures**: Repeated failures to an account should result in an automatic system warning message being generated and set to the account holder as well as a local systems administrator as well as directly to OISS.

g. **Passwords Not Stored in Unencrypted Format**: Systems shall not store passwords in an unencrypted format. Storing only a one-way hash of the password is preferred. In no event may any system other than the *Enterprise Directory Authentication* store or cache BSU Computer Username Passwords; each authentication must be accomplished by a separate call to the authentication system or by a Kerberos issued ticket issued through this system.

10. Workstation Access & Password Controls:

a. **Basic Secure Desktop Management**: Workstations used to access confidential data must take basic precautions to protect them from attack; some of these basic practices include:

   i. Using the latest version of antivirus software and updates.
   ii. Performing software and operating system updates frequently (daily and automatic if available).
   iii. Avoiding unapproved or unsupported downloaded "freeware" or "shareware".
   iv. Shutting off unneeded services such as local file or printer serving.

b. **Automatic Password Protected Screen Lock**: Secure workstations must be configured to use a password protected screen saver set to automatically lock the workstation at no more than 15 minutes of inactivity.

c. **Unattended Workstations**: Unattended computers used to access confidential information present a significant security risk if left unattended. Such workstations must be logging-out or a password protected screen saver must be manually activated to lock the workstation immediately.

d. **Workstation Power-Off**: Unless specifically advised otherwise, shutting down a computer at the end of the work day is permissible; however those who choose to turn off their computers are responsible for insuring required security updates complete when the systems are powered on. Certain workstations should not be powered off during the evening hours due to required security scans which run during this time.

e. **System Startup or "Boot" Passwords**: All computers used to access or store confidential information shall require a password upon power-up. Workstation computers used on campus having the technical capability to do so should be joined to the BSU Domain, in which case the startup username and password will be the BSU Computer Username Password. Many workstations must be joined to the BSU Domain for security scanning purposes; however workstations not joined to the BSU Domain must be secured using a password not less secure than required by the *Technical Password Requirements*.

11. Portable Computers, Removable Storage, and Off-Campus Systems:

a. **Portable Computers**: Confidential information must be protected to insure it cannot be maliciously harvested from lost or stolen computers; this risk is heightened with laptop and other portable devices requiring security. In addition to the *Workstation Access & Password Controls* defined above, Portable computers must protect confidential data using strong encryption.

b. **Removable Storage**: Removable storage and portable media such as backup tapes and disks containing confidential information require special handling and storage procedures. Contact OISS for additional information concerning approved portable devices including encrypted portable devices and storage media.

c. **Home & Office Off-Campus Computer Systems**: Computers located off-campus which are used to access confidential information such as work from home workstations must be maintained with the same rigor as on-campus systems used to access such information. In addition to the *Workstation Access & Password Controls* defined above, confidential data stored on these systems shall be protected by strong encryption and the home or remote network shall be protected by a local firewall.

12. Wireless Internet Access Guest Accounts for Visitors:

Guests visiting Ball State University can gain access to the Ball State University wireless guest network by connecting to the bsuguest SSID. Access requires agreeing to terms of service and does not grant access to on-campus resources.

13. Accounts for Vendor & Partner Support:

Vendors and partners providing technical support services will be required to complete an approved Non-Disclosure Agreement prior to obtaining access to any production system containing confidential information. Upon approval, the vendor will be issued a temporary username and password which will be tracked and disabled upon conclusion of the support incident. In the case where support from a particular vendor is recurring, the username shall be disabled when not actively being used by the vendor to resolve a particular support incident. Access logs of vendor support account activation and deactivation as well as the name and contact information of the support provider must be logged. Contact OISS for assistance in providing necessary access to any production system.

14. Exceptions to These Standards:

These standards have been designed to provide the security necessary to protect the confidential information assets of Ball State University. Exceptions and deviations from these standards must be authorized by OISS.

15. Changes to These Standards:

OISS and the Vice President of Information Technology may modify these standards at any time.