



Information Technology

Production Information Systems

Integration And Supportability

Standards, Procedures, & Practices

Last Revised April 27, 2007

Table of Contents

Overview And Brief Summary	5
Executive Oversight Group	9
Administrative Processes, Procedures, and Systems Group	13
Authentication & Access Control Standards	17
GLBA Information Security Program	25
Standards For Production Information Processing Hardware, Software, and Data Protection.....	37
Specific Operating System, Server Hardware And Server Software Standards.....	43
Information Technology Confidentiality and Information Access Agreement.....	49
Procedures For Reuse Or Disposal Of Electronic Storage Media	55
Reporting An Information Security Incident Or Suspected Violation	59
Application Development Standards.....	63
Computer Account Expiration & Removal Procedures	67
Remote Password Reset Procedures.....	71
Production Server Hosting Procedures	75
DMZ Server Hosting Procedures	79
Third-Party Non-Disclosure Agreement	89

Overview And Brief Summary

This manual contains the comprehensive set of standards, procedures, and practices required for acquisition, development, and deployment of production information systems at Ball State University. The procedures and standards presented are necessitated by regulatory compliance obligations, as well as institutional needs for systems integration and supportability.

In a highly connected and distributed environment such as Ball State University, the security of the institution as a whole is only as strong as the weakest entry point. Attackers will not spend their time and energies attempting to breach a highly guarded system if another system having lax controls and equally lucrative information is discovered.

Security and auditability of information systems is of pinnacle importance, and resonate through each of the required procedures and standards. Because of the tremendous risk unsecured information systems present, it is *imperative* every server and system comply with these procedures and standards.

Executive Oversight and APPS Group Principles:

The role and responsibilities of the *Executive Oversight Group* and the *Administrative Processes Procedures and Systems Group* (APPS Group) are defined, these being the primary decision making bodies within the University controlling the deployment of production information systems.

Authentication & Access Control Standards:

These standards describe permitted methods for assigning and managing access to electronic information systems within the University environment.

GLBA Information Security Program:

The Gramm-Leach-Bliley Act (GLBA) places certain requirements on institutions such as Ball State University with regard the handling and processing of financial information, both in electronic and paper formats. The procedures and standards presented in this document must be complied with whenever financial information processing is involved or affected.

Standards For Production Information Processing Hardware, Software, and Data Protection:

These general standards describe the process and fundamental requirements for purchase or acquisition of information systems hardware, software integration, security risk assessment, vendor support, encryption, and data protection (backup/business continuity) standards.

Specific Operating System, Server Hardware And Server Software Standards:

These specific standards provide direction in the selection of supportable server operating systems, server hardware, and technical integration requirements for production systems at Ball State University.

Information Technology Confidentiality and Information Access Agreement:

The *Confidentiality and Information Access Agreement* must be read, signed, and complied with by all Information Technology employees having access to confidential information. Although each Vice Presidential area within the University may draft their own agreement specific to their environment, all University employees having such access should sign a similar agreement.

Procedures For Reuse or Disposal of Electronic Storage Media:

Unless confidential information is properly removed, disposal or reuse of digital media can result in inadvertent disclosure of confidential information. Indiana law (IC 24-4-14) provides significant penalties for any person improperly disposes of confidential information. These procedures ensure adequate disposal and transfer methods are followed.

Reporting An Information Security Incident Or Violation:

Ball State University is required under Indiana Law (IC 4-1-11) to make timely notification of breach where confidential information is reasonably believed to have been acquired by an unauthorized person. These university-wide breach notification standards have been designed to provide compliance with university obligations and also to support established incident response procedures.

Application Development Standards:

University Computing Services has established Development Standards for ASP.NET, SQL Development, and Mobile Development. Any university unit approve to engage in applications development for production systems and services must adhere to these standards which help maintain supportable systems and applications as well as adequate integration and security.

Computer Account Expiration & Removal Procedures:

These procedures define the standards and practices for account removal as well as the separation of account authentication from application and service authorization.

Remote Password Reset Procedures:

These procedures describe the required steps and methods for performing password and authentication reset when an in-person appearance would be impossible or would be impractical due to extreme hardship. Password resets not preformed in-person must follow these procedures.

Production Server Hosting Procedures:

Servers hosing production data and services must be deployed in a secure, auditable, and supportable manner. These procedures inventory system components and document responsibilities for server deployment, eliminating “service gaps” which could result in server failure or security compromise.

DMZ Hosting Procedures:

The general hosting requirements for production systems may not be conducive to the requirements of academic investigation. These procedures provide researchers with an environment to host servers in a controlled environment conducive to experimentation, while also insuring the security of production services and data.

Third-Party Non-Disclosure Agreement:

Vendors and other outside entities requiring access to confidential information controlled by Ball State University must have an approved and executed non-disclosure agreement before access is permitted.

Executive Oversight Group

Executive Oversight Group

The purpose of the *Executive Oversight Group* is to define institutional priorities and establish standards for the adoption and creation of information technology systems. Approved projects must fulfill the functional requirements of the individual unit as well as the larger requirements for campus information systems integration, support, security, and availability. The following core principles define the *Executive Oversight Group* prioritization and standards making decision making process:

1. The *Executive Oversight Group* will have final responsibility for setting overarching administrative systems priorities and technology standards across the entire institution.
2. Priorities and standards defined by the *Executive Oversight Group* will be sufficiently specific and comprehensive so as to enable the *APPS Group* to make self-regulated approval and priority assignments.
3. Information Technology standards will be actively maintained and updated to reflect existing and emerging technologies. The *Executive Oversight Group* will have responsibility for insuring these standards are communicated and adhered to.
4. Approved systems will be well integrated and avoid isolated islands of service. Integration will be at a level sufficient to avoid duplication of human effort and inconsistency of services.
5. No systems may be purchased, developed, or otherwise acquired or deployed prior to completion of a formal and consistently applied planning process designed to evaluate alignment with institutional needs and requirements. This formal planning process will be approved by the *Executive Oversight Group* and applied by the *APPS Group* to every proposed system and project.
6. The *Executive Oversight Group* will act in an oversight capacity to insure appropriate needs analysis, prioritization, and formal planning is sufficient to prevent waste and maintain focus on proposed systems having the highest institutional priority and in keeping with established standards.
7. Information security, including the confidentiality, integrity, and availability of critical institutional information systems will be of primary importance; systems having inadequate security will be removed from consideration.

Administrative Processes, Procedures, and Systems Group

Administrative Processes, Procedures, and Systems Group

The *APPS Group* is responsible for managing system priorities, purchases, and acquisitions. Adoption and creation of information technology systems must adhere to the standards and institutional priorities established by the *Executive Oversight Group*. Approved systems will fulfill the functional requirements of the individual unit as well as the larger requirements for campus information systems integration, support, security, and availability. The following core principles will define the *APPS Group* decision making process:

1. The *APPS Group* will have responsibility for faithfully insuring adherence to established standards for all purchased, developed, or otherwise acquired systems. Proposed projects or systems failing to meet established standards and alignment with the highest institutional priorities will be rejected or revised to correct such deficiencies.
2. No administrative systems will be purchased, developed, or otherwise acquired or deployed which are not in accord with the highest institutional priorities and standards as defined by the *Executive Oversight Group*.
3. Members of the university community which contribute data to, or consumes data from, the proposed information system must have an opportunity for involvement in the approval and application management process.
4. For each approved project and system, the *APPS Group* will conduct appropriate and documented needs analysis, prioritization, and formal planning and will evaluate the costs, benefits, and risks of each approved project and system in accordance with the Executive Oversight Group's overarching priorities and technology standards.
5. An objective evaluation and decision will be made regarding the feasibility of purchase, development, or outsourcing. Preference will be given toward purchase where there are no identifiable unique requirements and where solutions available on the open market can be effectively integrated, secured, maintained, and supported. An absence or lack of a positive outcome for these factors will shift the preference toward outsourcing or in-house development.
6. Approved systems will be well integrated and avoid isolated islands of service whenever possible and reasonable to do so. Integration will be at a level sufficient to avoid duplication of human effort and inconsistency of services.
7. Information security, including the confidentiality, integrity, and availability of critical institutional information systems will be of primary importance; systems having inadequate security will be removed from consideration.

Authentication & Access Control Standards

Authentication & Access Control Standards

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:

1. Scope & Application of These Standards:

These standards have been developed by the Office of Information Security Services (OISS) within University Computing Services apply to all students, employees, outside persons or organizations as well as any other entities accessing or using Ball State University information systems.

2. 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.

3. 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.

4. 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.

5. 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.

6. 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 after admission, while employees obtain them by visiting the UCS Information Desk at RB165. 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 OISS for additional information before attempting to integrate with this authentication system, which requires certain technical protocols be followed to insure 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. Such systems must be approved by OISS prior to acquisition, development, and deployment. These systems must comply with the *Technical Password Requirements* described below. Future purchased, developed, or acquired systems must be evaluated to include proper support for integration with EDAS.

7. Password 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.

- 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.
- G. Multi-Factor Authentication:** Certain system access levels may require multi-factor authentication. Contact OISS for additional information before attempting to integrate with any multi-factor system.

8. 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 “pass phrases” 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 harder to guess.
- B. Complexity:** Passwords must contain a combination of at least four of the following groups of characters: (1) upper case (2) lower case (3) letters (4) numbers (5) special characters such as punctuation or symbols. Password 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 the vulnerability to dictionary and related attacks.
- C. Expiration:** Passwords must be changed at least once every six months. User accounts not used for authentication purposes for a period of six calendar months will be disabled. Re-enabling these 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. Changed 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 of 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 will result in an automatic system message being generated and sent to the account holder as well as a security administrator. Tracking multiple authentication failures may help in alerting security personnel to an attack.
 - 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.

9. 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. This procedure must be followed when leaving the office for a few minutes as well as when leaving the office at the end of the day.
- 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*.

10. 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 enhanced security. In addition to the *Workstation Access & Password Controls* defined above, Portable computers must protect confidential data using strong encryption. Where possible, two factor authentication methods should also be used for authentication and decryption. Contact OISS for additional information concerning approved two-factor authentication and encryption methods.
- 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 & Other 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.

11. Wireless Internet Access Guest Accounts for Visitors:

Procedures to provide guests visiting Ball State University with wireless Internet access during their time on campus are covered by the *Wireless Access Guest Account Procedures* maintained by the OISS.

12. Accounts for Vendor & Partner Support:

Vendors and partners providing technical support services will be required to compete 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.

13. 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 OTIS.

14. Changes to These Standards:

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

GLBA Information Security Program

GLBA Information Security Program

1. **Overview:**

This document summarizes Ball State University's (the "Institution's") comprehensive written information security program (the "Program") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm Leach Bliley Act ("GLBA"). The Program incorporates by reference the Institution's policies and procedures and is in addition to any such policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, the Family Educational Rights and Privacy Act ("FERPA").

2. **Scope of Program:**

This document describes the Program elements pursuant to which the Institution intends to (i) ensure the security and confidentiality of covered data and information, (ii) protect against anticipated threats or hazards to the security or integrity of such *Covered Data and Information*, and (iii) protect against the unauthorized access or use of such *Covered Data and Information* that could result in substantial harm or inconvenience to any customer.

3. **Covered Data and Information:**

For purposes of this Program, Covered Data and Information means all information required to be protected under the Gramm Leach Bliley Act ("GLBA"). Covered Data and Information specifically includes both paper and electronic records of Student Financial Information (defined below) required to be protected under the GLBA. In addition to this coverage which is required under federal law, the Institution chooses as a matter of policy to also include in this definition any credit or debit card information received in the course of business by the Institution, whether or not such credit or debit card information is covered by the GLBA.

4. **Student Financial Information:**

Under this Program, *Student Financial Information* is nonpublic personal information, which consists of personally identifiable financial information that is not publicly available and that the Institution has obtained from a customer in the process of offering a financial product or service, or such information was provided to the Institution by any financial institution. *Offering a financial product or service* includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of *Student Financial Information* include, but are not limited to, the following:

- A. Bank and credit card account numbers
- B. Income, credit histories, and other consumer report information
- C. Loan information, including loan applications and loan servicing
- D. Loan collection and delinquent loan processing
- E. Money wiring and other electronic funds transfers
- F. Financial aid information
- G. Student account balance information
- H. Other non-public personally identifiable information relating to a financial transaction.

5. **Designation of Representatives:**

The members of the Institution's GLBA Security Planning and Compliance Committee (the "Committee") shall be responsible for coordinating and overseeing the Program. A subset of

these members will form the GLBA Steering Committee (the “Steering Committee”) which will have additional responsibilities as described in this document. The members of the regular Committee and Steering Committee are listed in Appendix A. The Committee may designate other representatives of the Institution to develop and implement particular elements of the Program. Questions regarding the implementation of the Program or the interpretation of this document should be directed to the Office of University Compliance. Internal Audit and Information Security personnel will also conduct reviews of the areas that have access to *Covered Data and Information* to assess the internal control structures put in place and to verify compliance with the requirements of this policy.

6. **Elements of the Program:**

A. *Risk Identification and Assessment.* The Institution intends, as part of the Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Program, the Committee will establish procedures for identifying and assessing such risks in each relevant area of the Institution's operations, including:

- i. ***Employee Training and Management.*** Those employees whose job duties require them to work with *Covered Data and Information* or work in an area where they may be exposed to such information shall receive training regarding the access, use, disclosure, and security requirements regarding *Covered Data and Information*.
 1. Directors and supervisors are responsible for insuring that such employees receive adequate training, and are required to maintain records of those employees that have received training.
 2. The Committee will periodically evaluate the effectiveness of the Institution's employee orientation and training practices relating to access and use of *Covered Data and Information* and will work with the Institution's Human Resource Services Department to adjust training as needed to cover relevant policies and procedures.
 3. Each employee receiving training under this section shall be required to sign and submit as a condition of their ongoing employment an agreement to maintain the confidentiality of *Covered Data and Information* and to report suspected violations or breaches to the Office Of University Compliance.
- ii. ***Information Processing Risks, Controls, Processing, and Disposal.*** The Committee will identify each unit within the Institution that handles or processes *Covered Data and Information* using electronic methods of information storage, processing, or transmission. Responsibility for security assurance for these systems shall include the following:

1. The Steering Committee will have responsibility for review and approval of procedure and process integration issues relating to financial data or financial transactions covered by this policy whether electronic or paper based.
2. The Institution's Department of University Computing Services will have responsibility for general information security for electronic information systems, including technical standards for hardware and software, as well as general security monitoring and remediation for information systems. Remediation will consist of system isolation, segregation, or shutdown until the vulnerabilities are closed or neutralized.
3. Generally, the department or unit hosting the system will be responsible for application layer administration and support, which may include provision for vendor or third-party support services to maintain adequate confidentiality, integrity, and availability of production services.
4. Responsibility for the establishment and implementation of procedures related to the use of Social Security Numbers as well as BSU-ID information is held by the BSU-ID committee. Systems that process, transmit, store, or otherwise utilize Social Security Numbers must comply with the Social Security Number Policy available at <http://www.bsu.edu/bsuid/policy/>.

Details regarding responsibility for information systems which process, store, or transmit *Covered Data and Information* are included in Appendix B.

- iii. ***Procedures For Production Information Systems.*** The Committee will work with Enterprise Systems Administration representatives from the Institution's Department of University Computing Services regarding the establishment of procedures for server hosting and deployment. Such procedures will prescribe, among other things, logical and physical access controls, software and hardware replacement and upgrade, disaster recovery, change management, service and data integration, as well as systems administration responsibilities such as patch implementation and monitoring of security threats. Additional details are included in Appendix B.
- iv. ***Detecting, Preventing and Responding to Attacks.*** The Committee will coordinate with the Institution's Computer Security Incident Response Team (BSU-CSIRT) to evaluate and recommend procedures for and methods of detecting, preventing, and responding to attacks and other information security incidents. The BSU-CSIRT will have responsibility for implementing and coordinating threat and vulnerability detection, security incident and breach response, as well as disseminating information related to known attacks and other threats to the integrity of information systems and networks utilized by the Institution.

- v. ***Designing and Implementing Safeguards.*** The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Committee will, on a regular basis, review implemented and planned safeguards and controls and will evaluate the effectiveness of such safeguards and make appropriate recommendations for modifications as advances and changes in technology require. As appropriate, the Committee will also review ongoing security testing, monitoring, and change control processes and evaluate the effectiveness of such safeguards.

B. *Overseeing Service Providers.* “*Service Providers*” refers to all third party vendors who, in the ordinary course of the Institution’s business, are provided access to covered data. These third parties may include, for example, businesses retained to transport and dispose of covered data, collection agencies, and systems support providers. Due to the specialized expertise needed to design, implement, and service new technologies, third-party vendors may be needed to provide resources that the Institution determines not to provide on its own. In the process of selecting third-party vendors that will maintain or have access to covered data and information, the evaluation process shall include the ability of the service provider to safeguard confidential financial information. The Committee will work with the Office of University Compliance and other offices as appropriate to make certain that service provider contracts contain appropriate terms to protect the security of covered data. While specific third-party contracts will require individual review and specifically tailored provisions, characteristics of appropriate provisions will include:

- i. A specific definition or description of the confidential information being provided;
- ii. A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- iii. An explicit acknowledgement that the contract allows the contract partner access to confidential information;
- iv. An assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information;
- v. A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;
- vi. An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles the Institution to be indemnified for losses caused by the breach, and to then terminate the contract without penalty; and

- vii. A provision ensuring that the contacts confidentiality requirements shall survive any termination agreement.

Such terms, as appropriate, shall apply to all existing and future contracts entered into with such third party service providers.

C. *Adjustments to Program.* The GLBA requires this Information Security Program to be subject to periodic review and adjustment. The Committee is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on the Program.

Appendix A:

The Committee shall include the following members (those with underlined names are also members of the Steering Committee):

Mr. Ken Brown

Director, Athletic Business Services

Ms. Judith A. Burke

Director of University Human Resource Services

Mr. Gene Burton

Director, Department of Public Safety

Mr. Dan Byrnes

Dir Sports Facilities & Recreation Services

Ms. Mary Cosby

Director, Financial Information Systems/Technology

Ms. Tracy Curtis

Controller, Ball State University Foundation

Mr. Brad Faust

Assistant Dean Library Information Technology Services

Dr. Alan Hargrave

Director of Housing and Residence Life

Ms. Leisa Julian

Director of Finance

Mr. Loren Malm

Assistant Director UCS - Security, Policy, Systems, and Assessment

Mr. Bill McCune

Associate Vice President, Controller & Business Services

Ms. Amy Reed

Director of Advancement Services

Mr. Thomas Roberts

Director of Auditing

Dr. Joanna Wallace

Associate Dean of the School of Extended Education

Mr. Curtis Westfall

Director of Systems Technology for Enrollment, Marketing, and Communications

Mr. Bob Zellers

Director, Scholarships & Financial Aid

Appendix B:

1. Standards For Production Information Processing Hardware:

Individual units deploying systems Information Systems which will process *Covered Data and Information* shall follow these procedures for hardware acquisition and deployment:

- A. UCS Server & Peripheral Hardware Standards:** The Enterprise Systems Group within University Computing Services has established supportability standards for various hardware platforms including those for server, storage, backup/recovery, network connectivity, and other physical characteristics. All units deploying production systems which will process *Covered Data and Information* are strongly encouraged to work with the Enterprise Systems Group before selecting a hardware vendor.
- B. Hardware Purchased Outside UCS Standards:** In the event a unit must select a hardware vendor that falls outside the UCS supported vendors due to bundling by the software vendor or because of other restrictions or recommendations the software vendor has established, the unit shall work with UCS to conduct a risk analysis that will evaluate the various options for mitigation of risk. In the most likely scenario, UCS will proscribe additional support services from the software or hardware vendor necessary to maintain adequate security and availability. Individual units shall bear the cost of proscribed hardware and related services.
- C. Spare Hardware/Replacement Strategy:** Individual units must work with their hardware vendor to agree on an eventual replacement/upgrade path for servers and related peripherals. All units shall make appropriate budgetary provisions for hardware replacement, upgrade, maintenance, and support. In some cases, the unit may be required to purchase additional spare equipment or enhanced hardware support to insure adequate availability and security. The unit shall work with the Enterprise Systems Group within University Computing Services to make this determination.
- D. Completion and Approval of UCS Hosting Agreement:** Units must complete and adhere to the requirements of the UCS Hosting agreement. These requirements address identification of server support contacts within the department, assignment of roles to assure there are no “service gaps” as well as other issues relating to security and availability of production systems. The Hosting Agreement must be signed by the chair or unit head, and approved by the Enterprise Systems Group within University Computing Services.

2. Standards For Production Information Processing Software:

Individual units deploying systems Information Systems which will process *Covered Data and Information* shall follow these procedures for server software and related services, including vendor hosted services:

- A. Business Process Integration:** Few, if any, financial information processing systems operate in isolation. Frequently some interface and compatibility is required with existing Institutional processes. Units shall obtain approval from the Steering Committee for systems that need to integrate with financial processes. If there is any question as to whether a system might require integration or communication with other Institution financial processes, approval shall be sought and obtained prior to acquiring the system or issuing a purchase order for its acquisition.
- B. Credit Card And Other Payment Processing:** Information systems that process credit card, debit card, ACH, or other forms of electronic payment have enhanced security and integration requirements. Such systems require special approval from the Steering Committee, which shall be sought and obtained prior to acquiring the system or issuing a purchase order for its acquisition.
- C. Technical Integration:** Technical integration of information systems shall be a primary consideration of any unit considering purchase or acquisition. The University Computing Services Enterprise Systems Group will provide the unit with guidance regarding technical integration including supported development languages and development platforms, Web Services Architecture (WSA) requirements, and other technical integration issues. University Computing Services will provide guidance in advance so that incompatible platforms, development languages, and information systems can be pre-screened from consideration. If there is any question as to whether a system might require integration or communication with other Institution information systems, approval shall be sought and obtained prior to acquiring the system or issuing a purchase order for its acquisition.
- D. Information Security Technical Risk Assessment:** Every information system that will or may need to process *Covered Data and Information* shall have a security review conducted before the proposed information system is purchased or otherwise put into production. Such a security review will be conducted by the Office of Information Security Services within University Computing Services. Although each system is unique, relevant issues are likely to include supportability of the platform, the nature of the information the system will process, any external communications requirements (such as those that transverse the campus firewall), the methods and techniques used for securing data on the system, and any on-campus communications with other information systems or workers. Security review and approval shall be sought and obtained prior to acquiring the system or issuing a purchase order for its acquisition.
- E. Software Vendor Support Contracts:** Individual units must work with their software vendor to obtain support and services necessary to maintain the proposed system. All units shall make appropriate budgetary provisions to maintain these services and support through the life-cycle of the system. In some cases, the unit may be required to purchase

an uplifted support contract (such as 24/7 support) to insure adequate availability and security. The unit shall work with the Enterprise Systems Group within University Computing Services to make a determination as to what support services are appropriate.

- F. Encryption of Sensitive Data:** The transmission, storage, and processing of *Covered Data and Information* may require approved encryption technologies. The unit shall work with the Enterprise Systems Group within University Computing Services to make a determination as to which situations require encryption and which methodologies are appropriate.
- G. Data Protection & Business Resumption Strategy:** The unit will acquire an adequate backup and recovery system, and develop a business resumption plan defining the procedures for recovering from a catastrophic failure or event which results in production server downtime or data loss/corruption. The unit will work with the software and hardware vendor to identify and select the most appropriate methods and technologies. The plan developed by the unit shall address required hardware, software, vendor support, staffing, assignment of duties, and procedures for recovery. This plan and procedures shall be filed with the University Computing Services Enterprise Systems Group and kept up-to-date by the unit.

Standards For Production Information
Processing Hardware, Software, and
Data Protection

Standards For Production Information Processing Hardware, Software, and Data Protection

1. **Overview:**

In order to assure information security, systems availability, and integration of information processing systems, Information Technology submits the following as needs for future systems purchased or developed. In summary these needs are:

- A. Hardware & Software Technical Standards:** When purchasing computer hardware or software which will be used for production systems, established standards (hardware, software, and data protection standards are described in detail below) must be followed. Purchases which rely on platforms and technologies not identified as supported by Information Technology must be avoided.
- B. Project Request/Development Standards:** When requesting application development services, completing and adhering to the project request and Software Development Life Cycle (SDLC) approval and documentation procedures established by the University Computing Services Information Systems Development & Support Group (ISDS) and obtaining all appropriate Area Coordinator approvals before requesting project initiation or modification.
- C. Process Integration:** Commitment of all Area Coordinators to work together and make process and data integration a priority – shunning “islands” of service for those that can be integrated with BSU processes and technologies.
- D. Supplies Data To Other BSU SOA Systems:** Each Area Coordinator must, wherever possible, ensure the selection of systems and applications which make information ‘owned’ or generated by the unit available in real-time methods compatible with BSU SOA and other Information Technology standards.
- E. Consumes Data From Other BSU SOA Systems:** Each Area Coordinator must, wherever possible, ensure the selection systems and applications able to consume information ‘owned’ or generated by other units in real-time methods compatible with BSU SOA standards, and must configure their systems and applications to do so.

2. **Standards For Production Information Processing Hardware:**

Individual units deploying Information Systems shall follow these procedures for server hardware and related components. The following standards apply regardless of where hardware is located or the method through which it is funded:

- A. UCS Server & Peripheral Hardware Standards:** The Enterprise Systems Group within University Computing Services has established supportability standards for various hardware platforms, including those for server, storage, backup/recovery, network connectivity, and other physical characteristics. All units deploying production systems are strongly encouraged to work with the Enterprise Systems Group before selecting a hardware vendor, or a specific hardware model.

- B. Hardware Purchased Outside UCS Standards:** In the event a unit must select a hardware vendor that falls outside the UCS supported vendors due to bundling by the software vendor or because of other restrictions or recommendations the software vendor has established, the unit shall work with UCS to conduct a risk analysis that will evaluate the various options for mitigation of risk. In the most likely scenario, UCS will prescribe additional support services from the vendor necessary to maintain adequate security and availability. Individual units shall bear the cost of such hardware and related services.
- C. Spare Hardware/Replacement Strategy:** Individual units must work with their hardware vendor to establish an eventual replacement/upgrade path for servers and related peripherals. All units shall make appropriate budgetary provisions for hardware replacement, upgrade, maintenance, and support. In some cases, the unit may be required to purchase spare equipment or enhanced hardware support to ensure adequate availability and security. The unit shall work with the Enterprise Systems Group within University Computing Services to make this determination.
- D. Completion and Approval of UCS Hosting Agreement:** Units must complete and adhere to the requirements of the UCS Hosting agreement. These requirements address identification of server support contacts within the department, assignment of roles to assure there are no “service gaps” as well as other issues relating to security and availability of production systems. The Hosting Agreement must be signed by the chair or unit head, and approved by the Enterprise Systems Group and Operations within University Computing Services.

3. Standards For Production Information Processing Software:

Individual units deploying systems Information Systems shall follow these procedures for server software and related services, including vendor hosted services. The following standards apply regardless of where the software application is hosted or the method through which its purchase is funded:

- A. Institutional Process Integration:** Units shall develop a process and data integration plan before proceeding with a purchase or deployment decision. If there is any question as to whether a system might require integration or communication with other institutional processes, approval from the other Area Coordinators shall be sought and obtained prior to acquiring the system or issuing a purchase order for its acquisition.
- B. Technical Integration:** Technical integration of information systems shall be a primary consideration of any unit considering purchase or acquisition. The Enterprise Systems Group and the ISDS Group within University Computing Services will provide the Unit with guidance regarding technical integration including supported development languages and development platforms, Web Services Architecture (WSA) and SOA requirements, and other technical integration issues such as security and authentication (Active Directory) integration. University Computing Services will provide guidance in advance so that incompatible platforms, development languages, and information systems can be pre-screened from consideration. If there is any question as to whether a system might require integration or communication with other institutional information systems, approval shall be sought and obtained prior to acquiring the system or issuing a

purchase order for its acquisition.

- C. Information Security Technical Risk Assessment:** Every information system shall have a security review conducted before the proposed information system is purchased or otherwise put into production. Such a security review will be conducted by the Office of Information Security Services within University Computing Services. Although each system is unique, relevant issues are likely to include supportability of the platform, the nature of the information the system will process, any external communications requirements (such as those that transverse the campus firewall), the methods and techniques used for securing data on the system, and any on-campus communications with other information systems or workers. Security review and approval shall be sought and obtained prior to acquiring the system or issuing a purchase order for its acquisition.
- D. Software Vendor Support Contracts:** Individual units must work with their software vendor to obtain support and services necessary to maintain the proposed system. All units shall make appropriate budgetary provisions to maintain these services and support through the life-cycle of the system. In some cases, the unit may be required to purchase uplifted support contracts (such as 24/7 support) to insure adequate availability and security. The unit shall work with the Enterprise Systems Group within University Computing Services to make a determination as to what support services are appropriate.
- E. Encryption of Sensitive Data:** The transmission, storage, and processing of confidential Information may require approved encryption technologies. The unit shall work with the Enterprise Systems and ISDS Groups within University Computing Services to make a determination as to which situations require encryption and which methodologies are appropriate.

4. Data Protection & Business Resumption Strategy:

The unit will implement an adequate backup and recovery system, and develop a business resumption plan defining the procedures for recovering from a catastrophic failure or event that results in production server downtime or data loss/corruption. The unit will work with the software and hardware vendor to identify and select the most appropriate methods and technologies. The plan developed by the unit shall address required hardware, software, vendor support, staffing, assignment of duties, and procedures for recovery, and shall be approved by the University Computing Services Enterprise Systems Group before implementation. An up-to-date plan and procedures shall be kept on file with UCS Operations.

**Specific Operating System,
Server Hardware And
Server Software Standards**

Specific Operating System, Server Hardware And Server Software Standards

These specific standards supplement the general “*Standards For Production Information Processing Hardware, Software, and Data Protection*” guidelines by providing direction in the selection of supportable server operating systems, server hardware, and technical integration requirements for production systems at Ball State University. Specific standards will evolve as new product release cycles are initiated by supported product lines identified below.

While the following specific hardware, software, and integration standards are generally supported, each deployment is unique, and not all hardware or software configurations will be appropriate in every situation. As such, these standards should be used as a *minimum starting point for investigation* of possible solutions, then working directly with the *UCS Enterprise Systems* and the *UCS Information Systems Development & Support Group* to arrive at specific supportable selections from this guide.

1. Supported Operating System Standards

University Computing Services has standardized on the Windows operating system for production hardware systems and also supports the IBM Mainframe. The Enterprise Systems Group within UCS can generally provide operating system level support for Microsoft supported Windows server systems platforms including patch management, security vulnerability testing and remediation, integrated MOM system health and status monitoring and alerting, integration with enterprise domain authentication and PKI systems, system and storage sizing and OS support consultation services, support contract procurement assistance, server license management and consulting, and related services for the following systems:

- A. Windows 2003 Standard
- B. Windows 2003 Standard R2
- C. Windows 2003 Web
- D. Windows 2003 Enterprise
- E. Windows 2003 Datacenter
- F. Windows Storage Server 2003 R2
- G. Windows Compute Cluster Server 2003

(Both 64 and 32 bit variants are supported for recommended hardware platforms.)

Unsupported operating system environments present inherent integration challenges as well as significant risk of extended service downtime, information loss, and security breach. Operating systems other than those listed above (*such as the various UNIX and Linux variants*) are not supported, and utilization of unsupported platforms for production data is highly discouraged and will be denied where UCS determines significant risk to institutional data, services, or processes has been insufficiently mitigated.

2. Supported Server And Storage Hardware Standards

All of the following hardware systems are part of HP's ProLiant server family, currently in its fifth major product release cycle. Each release cycle has increased the available systems' capabilities and performance while maintaining a relatively stable price point for each server class. Each server model is configured, either as standard equipment or via option kits as necessary, with redundant options including: N+1 power supplies, redundant fan systems, and hardware RAID controllers. Each newly configured system must have at least 2 GB of RAM and a redundant 36 GB storage volume.

A. Dual Processor Capable Systems

- i. HP ProLiant DL365 Series
- ii. HP ProLiant DL385 G2 Series

B. Quad Processor Capable Systems

- i. HP ProLiant DL585G2

C. Expansion Storage Devices

- i. HP StorageWorks Modular Smart Array 50
- ii. HP StorageWorks Modular Smart Array 70
- iii. HP Smart Array P800 Controller

Deployment of unsupported server hardware presents inherent integration challenges as well as significant risk of extended service downtime, information loss, and in some instances security breach. Hardware configurations or vendors other than those listed above are not supported, and utilization of unsupported hardware for production data is discouraged and will be denied where UCS determines significant risk to institutional data, services, or processes has been insufficiently mitigated. These hardware specifications are current as of January, 2007.

3. Supported Integration Standards For Production Systems

Effective integration involves alignment of *system*, *development language*, and *database* considerations. The following sections provide specific guidance in these areas, however it should be noted that in particular instances, *closed systems* which utilize unsupported databases or languages may be approved. Approval in such cases requires analysis of UCS systems and development personnel to determine whether or not the unsupported databases and languages are sufficiently abstracted by the application vendor's SOA or API support. For example, selection of a particular application using the Oracle database may be approved, if it is determined that the application vendor provides SOA (or API) integration sufficient to remove the requirement of direct Oracle database integration.

A. System Integration

University Computing Services has standardized on implementing system integration

using Service Oriented Architecture (SOA) and requires systems to support or to utilize SOA. For applications that implement or consume web services SOAP based messaging is preferred. The implementation of a Service Oriented Architecture at Ball State does allow for a wide variety of web service protocols but requires additional work to integrate these services if they do not follow the SOAP based messaging standard.

System Integration techniques other than those listed above, such as file extracts and manual data re-entry are not supported, and utilization of unsupported system integration techniques are discouraged and will be denied where UCS determines significant risk to institutional data, services, or processes has been insufficiently mitigated. Unsupported system integration techniques present inherent integration challenges as well as significant risk of extended service downtime, information loss, and security breach.

B. Development Languages

University Computing Services has standardized on the .NET v2.0 development platform with C# as the supported language for web based application development and COBOL v3.4 for mainframe application development, and requires applications which require integration or support to utilize or support these languages.

Development languages other than those listed above, such as Java and proprietary languages, are not supported, and utilization of unsupported languages are discouraged and will be denied where UCS determines significant risk to institutional data, services, or processes has been insufficiently mitigated. Unsupported languages present inherent integration challenges as well as significant risk of extended service downtime, information loss, and security breach.

C. Database Platforms

University Computing Services has standardized on DB2 v7.0 and Microsoft SQL Server 2000/2005 as the database platforms and requires applications which require integration or support to utilize or support these databases.

Unsupported databases present inherent integration challenges as well as significant risk of extended service downtime, information loss, and security breach. Database languages other than those listed above, such as Sybase, MySQL and Informix are not supported, and utilization of unsupported databases are discouraged and will be denied where UCS determines significant risk to institutional data, services, or processes has been insufficiently mitigated.

Information Technology Confidentiality
and Information Access Agreement

Information Technology Confidentiality and Information Access 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.

This Confidentiality and Information Access Agreement (“Agreement”) must be read, signed, and complied with by all Information Technology 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.

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.
- 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 “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 to the Information Security Officer or to the Director of University Computing Services. I may also report such information to the UCS Computer Operations after-hours support (765-285-1549).
- 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 Computer 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 Information Security.
- 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, 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

Procedures For Reuse Or Disposal Of Electronic Storage Media

Procedures For Reuse Or Disposal Of Electronic Storage Media

These Procedures Are Under Revision And Will Be Included Soon

Reporting An Information Security Incident Or Suspected Violation

Reporting An Information Security Incident Or Suspected Violation

These Procedures Are Under Revision And Will Be Included Soon

Application Development Standards

Application Development Standards

These Procedures Are Under Revision And Will Be Included Soon

Computer Account Expiration & Removal Procedures

Computer Account Expiration & Removal Procedures

These Procedures Are Under Revision And Will Be Included Soon

Remote Password Reset Procedures

Remote Password Reset Procedures

These Procedures Are Under Revision And Will Be Included Soon

Production Server Hosting Procedures

Production Server Hosting Procedures

These Procedures Are Under Revision And Will Be Included Soon

DMZ Server Hosting Procedures

DMZ Server Hosting Procedures

University Computing Services recognizes that in certain situations, the general hosting requirements for production systems may not be conducive to the requirements of academic experimentation and investigation. The purpose of these procedures is to provide researchers with an environment to host servers in a controlled environment conducive to research while also insuring the security of production services and data.

When These Special Procedures May Be Applied

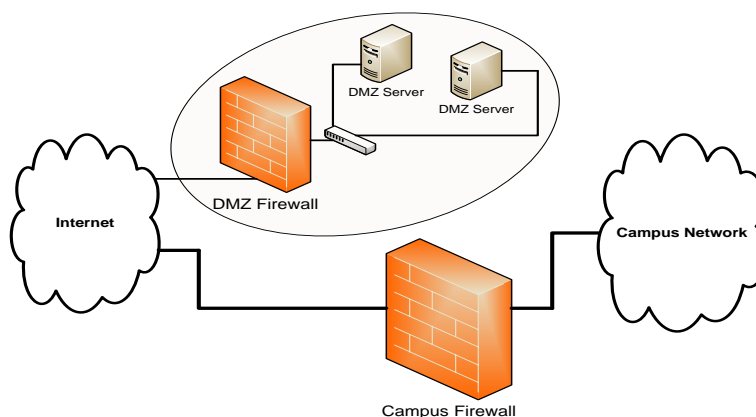
These procedures do not apply to systems which store or transmit information for which the university has a responsibility to protect or keep confidential. These procedures also do not apply where periodic service disruptions would have a significant negative impact on the operation of the unit or other units within the university. Only systems designated for research and/or testing purposes, and which meet the other requirements set forth below are eligible to for hosting under these special procedures.

Approvals Required

Academic units within the university wishing to host their own servers for purposes of research as described under these procedures must obtain the signature of their dean or administrative unit head, and the approval from the Office of Information Security Services within University Computing Services. Upon final approval, approved systems will be eligible for placement within the “DMZ hosting” area.

Executive Summary of DMZ Hosing Procedures

Ball State University DMZ Hosting involves placing the requested server (the “DMZ Server”) behind a special segment of the campus firewall, which is isolated from production systems. A DMZ Server has bidirectional access to the Internet, with access *from* the Internet being more flexible than is permitted for systems inside the traditional campus network. Access from campus systems to the DMZ Server is accomplished by connecting out through the campus firewall and back in through the DMZ firewall. Conceptually, the layout for approved DMZ Servers will resemble:



SPECIFIC REQUIREMENTS FOR DMZ HOSTING

1. Exclusive Duty And Responsibility Of The Academic Unit

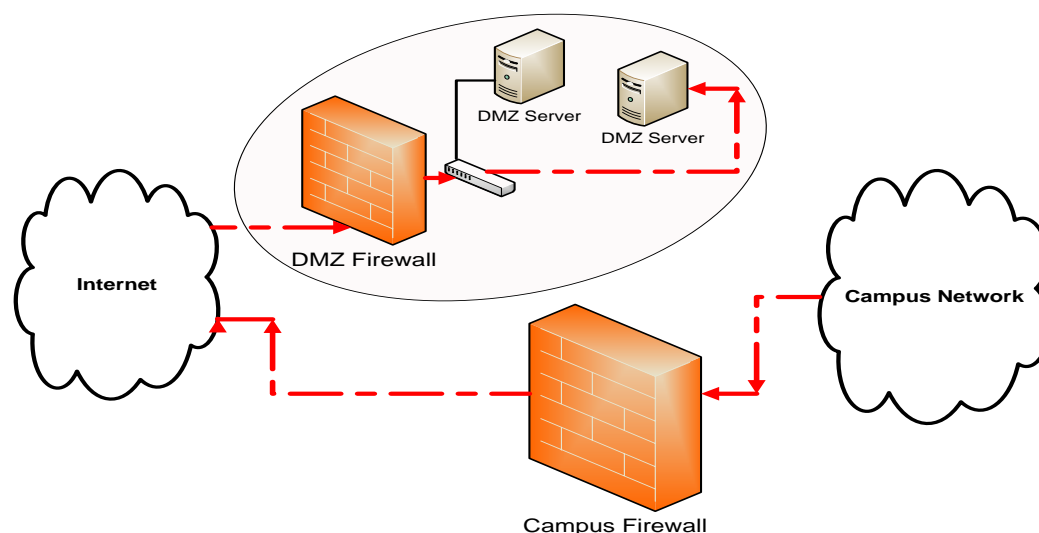
The academic unit (the “Unit”) recognizes that it has an exclusive duty and bears sole responsibility for the protection of DMZ Servers it chooses to manage under these procedures. Liability may extend outside the university in the event the security of the Unit’s DMZ Server is compromised. The Unit therefore agrees to commit adequate resources to maintenance and upkeep, which may require ongoing commitment of employee time for the specific purpose of systems management, reassignment of staff, and purchase of outside consulting or support services where internal departmental staffing is found to be inadequate.

2. Costs And Expenses

The Unit will be responsible for the costs in procuring whatever servers, software, peripherals, connections, services, or any other expenses it requires to operate and maintain its systems under these procedures. Even where UCS or the Office of Information Technology provides funding or resource allocation, this assistance will not diminish the responsibility of the Unit as described within these procedures. Units may request approval for up to ten (10) DMZ Servers or IP Addresses under these procedures.

3. Logical Isolation From The Ball State University Campus Network

Any connection to DMZ Servers from on-campus will occur through the campus firewall. Access to a DMZ Server from an on-campus or off-campus computer will be accomplished using appropriate openings made to the DMZ Firewall. Conceptually, these connections will appear as follows:



As shown in the above diagram, the connection to the DMZ Server from the campus network exits through the campus firewall and then connects through the DMZ Firewall to reach the desired DMZ Server. Under no circumstances is any connection made to the DMZ Server without passing through the DMZ Firewall, nor is it possible for a DMZ Server to *initiate* a connection back through the campus firewall. No specific openings will be made in the campus firewall for DMZ Servers, however openings may be made through the DMZ Firewall to DMZ Servers. Bandwidth to and from the DMZ will be regulated and partitioned.

4. Confidential Or Legally Protected Information And Related Regulations

Apart from usernames and passwords specific to DMZ Servers, no information the university has an

obligation or responsibility to keep confidential shall be hosted on or processed through a DMZ Server. In unique circumstances the UCS Office of Information Security may provide written approval for hosting or processing certain information.

5. Only Necessary Software Is To Be Enabled And Maintained

The Unit has a duty to constantly maintain the security of the systems it manages. Although servers hosted in the DMZ are somewhat isolated from campus, the University also has a responsibility to refrain from causing harm to systems outside the university. Administrators of DMZ Servers must avoid installing software or applications not needed for research or testing, and must maintain an accurate inventory of software installed or enabled. DMZ Server administrators must also promptly inform UCS about significant changes and remove or disable features no longer needed. Installed software must be kept up-to-date with current versions as recommended by the provider, and must be maintained in keeping with industry or community best-practices for secure deployment.

6. Prohibition Against Hosting Production Systems In The DMZ

These procedures are designed to provide members of the BSU academic community with an opportunity to deploy specialized applications for the purpose of small-scale testing and academic research. DMZ Servers are permitted solely for the purpose of academic research and experimentation, and in no event shall services relied upon by members of the university community (or commercial services) be hosted on them.

7. Access To DMZ Servers And Server Accounts

Administrative-level access to DMZ Servers must be limited to those named researchers having a legitimate need to access the system with administrative rights. User level accounts must be restricted to those having a legitimate research purpose, and these participants must be informed of the nature of the research/testing and the associated risks of the environment. Neither administrator nor user level accounts shall be created with matching credentials to servers or services outside of the DMZ; for example DMZ Server authentication credentials may not be set to match those of BSU Production systems. All access must conform to any relevant license restrictions.

8. Service Tunneling Or Proxy Services On DMZ Servers

In no event may DMZ servers be used for “tunneling” through ad-hoc virtual private networks, proxies, or other methods. For example, using a socket-level proxy to access the Internet through a computer located on the BSU Campus would constitute misuse of the DMZ Server.

9. Server Hardware And Physical Hosting Requirements For DMZ Servers

Before purchasing or selecting server hardware, the Unit shall obtain written approval for its hardware plan from the Enterprise Systems Group within University Computing Services. All hardware must be approved before installation into the DMZ racks. All server hardware installed under these procedures must reside in the UCS DMZ Rack within the Central Computer Room.

10. Security Scanning, Port Scanning, Network Discovery, And Other Related Issues

DMZ Servers may not be used for port scanning, security penetration or evaluation testing of other systems or devices, promiscuous packet capture (“sniffing”), network device discovery, or other related functions. Configuration of a DMZ Server as a “honey pot” or in any way designing the system to attract attacks or malicious activity is also prohibited.

11. Duty To Report And Act On A Suspected Or Known Security Breach

In the event the Unit becomes aware or has reason to suspect that a security breach of its DMZ

system has occurred, the Unit has both a responsibility to act to prevent further compromise of the system and to promptly notify UCS so that the breach can be investigated. The appropriate steps include immediately disconnecting the suspected server(s) from the network, and contacting UCS Operations Support Services at 765-285-1549 to report the incident. Operations Support Services may be reached at this number 24 hours a day. Questions that the Unit may receive about any alleged computer security incident from news media, students, or other areas should be referred to the Office of University Communications.

12. Data Protection & General DMZ Server Availability

The Unit may wish to periodically backup research and configuration data from the DMZ Servers and may do so using a method of the Unit's choosing, provided other systems or operations are not negatively impacted by the proposed method. Generally, DMZ Servers will be available for use however *they may be periodically unavailable* for network maintenance or other similar issues. In the event DMZ Services must be disabled for routine maintenance or other changes, UCS will attempt to notify the named contacts prior to taking the servers offline. All DMZ Servers will be bandwidth limited by a shared DMZ connection.

13. Patches and Updates, Hardware Repair, Spare Equipment and Console Access

Server and application patches as well as hardware repair are the responsibility of the Unit. University Computing Services recommends setting systems for "automatic update" to the greatest extent possible to help keep patches up-to-date. The Unit may also wish to obtain hardware spares prior to deployment, if the research or testing would be negatively impacted by an extended outage. The central KVM system is not available for DMZ hosts; clients must therefore either connect remotely (remote administration such as with Remote Desktop can be enabled through the DMZ Firewall) or make arrangements with the UCS Enterprise Systems Group to utilize the "crash cart" locally within the Robert Bell Computer Room.

14. Access To DMZ Systems From The Internet

Access may be provided directly to DMZ Servers. Selection of ports and protocols (and associated server-based software utilizing these ports) must be disclosed before deployment; however restrictions on port openings will be more flexible than is possible with production systems due to the enhanced isolation of DMZ Servers. Requests for changes to outside access require specific advance approval and must be made in writing to the attention of the UCS Information Security Officer. The written request must detail the purpose of the proposed access, the duration for which access is needed, whether or not access can be limited to a particular source and destination, and the specific access requested.

15. Unresolved Security Vulnerabilities Will Result In Immediate Disconnection or Shutdown

The Unit is responsible for providing the designated contacts to be notified in the event problems are discovered or suspected with the DMZ Server. DMZ Servers with vulnerabilities will be taken offline immediately and remain offline until the required patch or update is obtained, installed, and tested by the Unit. The DMZ will be monitored via IDS/IPS and other tools managed by Information Security Services.

16. Responsibility To Review And Act On UCS Security Audit Recommendations

At the time of initial deployment and then periodically, the Office of Information Security within University Computing Services will provide the Unit with a security assessment of the DMZ Server maintained by the Unit. The Unit agrees to participate in these reviews, provide information needed

to complete them, and implement any required changes promptly.

17. Removal From DMZ Hosting

Servers that are repeatedly cited for security lapses or other violations will be removed. The perceived dedication of the Unit to resolve problems, the severity of the lapse or breach, and the relevant history are some of the factors that will be considered.

18. Computer User's Privileges And Responsibilities University Wide Policy

These procedures are subordinate to and inclusive of the university wide policy regarding Computer User's Privileges and Responsibilities, which includes important information about acceptable use standards of computer technology at Ball State University. Of particular importance and interest to Units participating in this program are sections dealing with *indemnification of liability, institutional purpose, security, and restrictions on usage*. The Computer User's Privileges and Responsibilities policy can be found at the following address:

<http://www.bsu.edu/web/ucs/policy/>

DMZ Systems Inventory & Contact Information

In the event of a systems outage or a suspected security vulnerability or breach, this contact information will be used to notify the Unit of the issue. In the event of an issue related to security, access to the system will be immediately blocked or the system shutdown until the Unit resolves the vulnerability and so notifies UCS Information Security Officer.

1) System Name: _____ **2) Operating System:** _____

(The System Name listed above should be the same as assigned at the operating system level, and must not conflict with any other system. Please list the operating system such as: "Windows 2003")

3) DNS Name Request: _____ **.DMZHOST.BSU.EDU** **Check if needed:**

*(All DNS Names within the DMZ will be assigned name with a **dmzhost.bsu.edu** suffix, so for example an acceptable server name would be "SCIENCEBLOGTEST.DMZHOST.BSU.EDU".)*

4) External IP Address Request: _____ **Check if needed:**

(If approved, the system will be assigned an internal address through DHCP. If a static external IP address is needed, please check the box above and one will be assigned and you will be notified when it is ready.)

5) Purpose of System: _____

*(Please include a brief description of the proposed research system above, including the proposed hardware configuration. If purchasing hardware, **be certain to obtain written approval for your hardware plan before purchase, as all hardware must be approved before installation into the DMZ racks.** Also include a listing of proposed application software.)*

6) Requested Firewall Openings: _____

(Please include a listing proposed firewall holes and protocols (IP/UDP) for the research system described above, including relevant from/to address openings. Please be advised that under no circumstances will specific ports be opened through the main campus firewall to permit the initiation of connections from DMZ Servers to on-campus systems. Access to DMZ servers from campus and off campus will be possible; please list required ports and protocols. Also include a listing of proposed application software.

Contact Information For Security Incidents – DMZ Systems:

Contact	Name	Work	Home	Cellular	Do Not Call Hours
Primary					
Secondary					
Administrative					

(If you do not wish to be called after hours, please specify those hours above, otherwise you may get a call at 2:00am if problems occur. However, if you specify "Do Not Call" hours you will not be notified until these hours have passed, which may mean your system will be down for an extended period.)

Approval Of Dean Or Administrative Head

I understand that the above named individuals have requested permission to maintain a computer server and have this server exposed to the Internet as described above. I understand my unit will bear an exclusive responsibility for the server being deployed under these procedures, and that it is possible liability may extend to parties outside the university in the event the security of the server is compromised.

I will insure that the procedures described above are followed, and I understand that in the event of a security incident or threat systems will be taken off-line or shutdown until such time as the vulnerability is corrected.

I agree with the assignment of the primary, secondary, and administrative contacts from my area as identified above and will appoint an appropriate alternative contact (or take action to remove the server) should any of these individuals become unavailable to fulfill their role as described within these procedures.

Name of Dean/Administrative Head: _____

Signature of Dean/Administrative Head: _____ Date: _____

The Space Below This Line Is Reserved For University Computing Services Use

Enterprise Systems Group Hardware Plan Approval: _____ Date: _____

Operations Support Approval & Notes: _____

Ent. Systems DMZ Hosting Approval: _____ Initial Scan: _____ Date: _____

OISS DMZ Hosting Approval: _____ Date: _____

DMZ Hosting Implemented & Client Notified: _____ Date: _____

Third-Party Non-Disclosure Agreement

Third-Party Non-Disclosure Agreement

Confidential information may not be disclosed to third-parties unless a non-disclosure agreement has been mutually executed by the third-party vendor and Ball State University.

A sample acceptable non-disclosure agreement is provided below, however substantially similar non-disclosure terms may be incorporated into other agreements. Business Affairs must approve all contracts before disclosure or transfer of confidential information.

BALL STATE UNIVERSITY MUTUAL NON-DISCLOSURE AGREEMENT

This agreement, made as of the last date set forth on the last page hereof (the "Effective Date"), by and between Ball State University (hereafter "Ball State University") and _____ (hereafter "Vendor"), and sets forth the terms and conditions of the disclosure and receipt of certain confidential information between the parties. The party disclosing Confidential Information, as herein defined, shall be referred to as the "Discloser" and the party receiving such "Confidential Information" shall be referred to as the "Recipient." The term "Confidential Information" shall refer to the confidential information disclosed by any party to this Agreement.

The parties signing this document agree as follows:

1. Confidential Information may include information that is disclosed to Recipient by Discloser in any manner, whether orally, visually or in tangible form (including without limitation, documents, devices and computer readable media) and all copies thereof.
2. Tangible materials that disclose or embody Confidential Information shall be marked by Discloser as "confidential," "proprietary" or the substantial equivalent thereof. Confidential Information disclosed orally or visually shall be identified by Discloser as confidential at the time of disclosure and promptly thereafter identified as confidential in a written document provided to Recipient.
3. Except as expressly permitted herein, for a period of three years from the effective date (Non-Disclosure Period), Recipient shall maintain in confidence and not disclose Confidential Information. Upon termination of this Agreement, Recipient's right to use Confidential Information, shall immediately terminate.
4. Upon termination, or upon demand by Discloser at any time, or upon expiration of this Agreement, Recipient shall return promptly to Discloser or destroy, at Discloser's option, all tangible materials that disclose or embody Confidential Information; provided, however, that Recipient may retain one copy of Discloser's Confidential Information for archival purposes only.
5. Recipient shall have the right to use Confidential Information solely for the purpose(s) specified within this agreement ["Permitted Purpose(s)"].
6. Recipient shall disclose Confidential Information only to those of its employees who have a need to know such information for the Permitted Purpose(s).

7. Confidential Information shall not include any information that recipient can demonstrate:
 - i. was in Recipient's possession without confidentiality restriction prior to disclosure by Discloser hereunder;
 - ii. was generally known in the trade or business practiced by Discloser at the time of disclosure through no act of Recipient;
 - iii. has come into the possession of Recipient without confidentiality restrictions from a third party and such third party is under no obligation to Discloser to maintain the confidentiality of such information; or
 - iv. was developed by Recipient independently of and without reference to Confidential Information.
 - v. If a particular portion or aspect of Confidential Information becomes subject to any of the foregoing exceptions, all other portions or aspects of such information shall remain subject to all of the provisions of this Agreement.
8. Recipient agrees not to reproduce or copy by any means Confidential Information, except as reasonably required to accomplish the Permitted Purpose(s). The Confidential Information shall not be disclosed or revealed to anyone except employees of Recipient who have a need to know the information for evaluation in connection with the described Permitted Purpose(s) and who are aware of their obligations under this Agreement to maintain the Confidential Information as confidential.
9. Recipient agrees to accept the Confidential Information and to employ all reasonable efforts to maintain the Confidential Information as confidential, such efforts to be no less than the degree of care employed by Recipient to preserve and safeguard its own confidential information; provided however, that such efforts shall not be less than a reasonable degree of care.
10. Recipient shall not remove any proprietary rights legend from, and shall upon Discloser's reasonable request, add proprietary rights legends to, materials disclosing or embodying Confidential Information.
11. Vendor acknowledges and agrees that Ball State University is a state agency subject to the provisions of the Indiana Open Records law, I.C. 5-14-et seq., and that disclosure of some or all of confidential information provided pursuant to this Agreement, and of the Agreement itself, may be compelled pursuant to that law. In the event that Recipient is required by the Indiana Open Records Act, or any other law, to disclose Discloser's Confidential Information, Recipient shall promptly notify Discloser, consult with Discloser regarding whether there are legitimate grounds to narrow or contest such disclosure, and only disclose that information that the University, in the opinion of legal counsel, is legally obligated to disclose.
12. Discloser understands that Recipient develops and acquires technology for its own products and/or internal applications, and that existing or planned technology independently developed or acquired by Recipient may contain ideas and concepts similar or identical to those contained in Discloser's Confidential Information. Discloser agrees that entering this Agreement shall not preclude Recipient from developing or acquiring technology similar to Discloser's without obligations to Discloser, provided Recipient does not use the Confidential Information to develop such technology.
13. Ball State University's Confidential Information will not be introduced in any future products marketed by the other party to this Agreement.
14. Neither party has any obligation under or by virtue of this Agreement to purchase from or furnish to the other party any products or services, or to enter into any other agreement, including but not limited to, a development, consulting, purchasing or technology licensing agreement.
15. Other than as expressly specified herein, Discloser grants no license to Recipient under any copyrights, patents, trademarks, trade secrets or other proprietary rights to use or reproduce Confidential Information.

Neither party shall use or cause to be published in any kind of media or communication the name, logo or other identifying information of any of the parties to this Agreement without the prior expressed written consent of the other party.

16. Notwithstanding any other provisions of this Agreement, Recipient agrees not to export, directly or indirectly, any United States (U.S.) source technical data acquired from Discloser or any products utilizing such data to any countries outside the U.S. if such export would be in violation of the United States Export Control Laws or Regulations then in effect.
17. The interpretation, application, and enforcement of this Agreement shall be governed by the laws of the State of Indiana without reference to choice of law principles. Any claim, suit, or cause of action involving the interpretation, application, or enforcement of this Agreement shall be commenced in Delaware County Circuit Court in Muncie, Indiana.
18. This Agreement expresses the entire agreement and understanding of the parties with respect to the subject matter hereof and supersedes all prior oral or written agreements, commitment and understandings pertaining to the subject matter hereof. Any modifications of or changes to this Agreement shall be in writing and signed by both parties.
19. Unless earlier terminated in accordance with the provisions hereof, this Agreement shall remain in full force and effect for the duration of the Non-Disclosure Period, whereupon it shall expire. Either party may terminate this Agreement at any time, without cause, effective immediately upon written notice of termination; however, in the event this Agreement is terminated prior to expiration of the Non-Disclosure Period, its provisions shall survive and remain in effect for the remainder of the Non-Disclosure Period, with respect to Confidential Information disclosed prior to the effective date of termination.

PERMITTED PURPOSES

A. The Permitted Purpose with respect to Confidential Information disclosed to Ball State University shall be a presentation/discussion on:

B. The Permitted Purpose with respect to Confidential Information disclosed to Vendor shall be:

CONFIDENTIAL INFORMATION

A. Ball State University identifies the following as its Confidential Information to be disclosed hereunder:

B. Vendor identifies the following as its Confidential Information to be disclosed hereunder:

Vendor	Ball State University
By: _____	By: _____
Title: _____	Title: _____
Firm: _____	Dept: _____
Date: _____	Date: _____
Signature: _____	Signature: _____

