ARKANSAS STATE UNIVERSITY-BEEBE
INFORMATION
TECHNOLOGY
SERVICES

Information Technology Services (ITS)

Rules, Processes, and Procedures

V3.0E June 2020

Contents

8000 COMPUTER RULES, PROCESSES AND PROCEDURES

8001 Appropriate Use of Computer Resources

Arkansas State University-Beebe (ASUB, College) provides computing, networking, and information resources for students and employees. This process and associated procedure apply to all users of technological resources provided by ASUB and ensures the appropriate use of desktop computers, portable computers, network resources and peripherals at the college. All consumers of technological resources are obligated to use such resources in an appropriate, considerate, efficient, ethical and lawful manner consistent with the rules and guidelines set forth in the associated procedure.

Users shall have no expectation of privacy and should be aware that data created with software licensed to ASUB and stored on hardware owned by ASUB is the property of the college.

Reference:
United States Code of Federal Regulations Title 18 Part I Chapter 47 Section 1030

8002 Computer Software Use

The purpose of this guidance is to prevent copyright infringement and to protect the integrity of the college's computer environment. ASUB intends to comply with all computer software copyrights and to adhere to the terms of software licenses that the college acquires. Therefore, it is the expectation that no person shall use or cause to be used on the College's computer devices or systems any software that is not licensed to ASUB or does not fall into one of the following categories:

1. The software is in the public domain and does not have restrictions that would prevent its use at ASUB.
2. The software is covered by a licensing agreement with the software author, authors, vendor or developer, whichever is applicable.
3. The software has been donated to the college and a written record of the contribution exists along with a license for its use.
4. The software has been purchased by the college and a record of the purchase exists.
5. The software is being reviewed or demonstrated by the user in order to reach a decision about possible future licensing.
6. The software has been written or developed by a college employee for the specific purpose of being used at the college.

In all the preceding categories, copies of the authorization, agreement, license, or original media will be maintained by Information Technology Services (ITS).

It is also the expectation that there will be no copying of copyrighted or proprietary programs on computers belonging to ASUB. The software developer copyrights most software and, unless expressly authorized to do so, ASUB has no right to make copies of the software except for backup or archival purposes. College personnel may not duplicate any licensed software or related documentation for use either on college equipment or elsewhere unless expressly authorized to do so by agreement with the licenser. Unauthorized duplication of software may subject employees and/or the college to both civil and criminal penalties under the United States Copyright Act.

According to U.S. copyright law, any person who makes an unauthorized copy is liable to the copyright owner for actual damages and profits or statutory damages of up to $200,000, plus court costs and attorney fees. In addition, in certain cases the infringer may be criminally prosecuted and subject to a fine of up to $500,000 and imprisonment of up to five years for first offenses.

All software will be installed by ITS. Users are required to inform the ITS in advance of any software needing installation.

Information Technology Services will conduct random audits of all college computers to ensure that the college follows software licenses.

Reference:
United States Code: Title 17 - Copyrights

8003 Electronic Mail

Arkansas State University-Beebe provides email accounts to employees when their duties require electronic communication for the purpose of correspondence relating to official college business, education, instruction, professional development, and occasional non-commercial personal use. Inappropriate use of ASUB email accounts is strictly prohibited. Arkansas State University-Beebe is a state agency and as such, all correspondence sent or received via ASUB e-mail accounts may be monitored and disclosed to third parties including law enforcement personnel.

Procedure:

Inappropriate uses of ASUB provided e-mail accounts is strictly prohibited. Examples of inappropriate use include, but are not limited to, the following:

a. Any illegal activity
b. Producing unsolicited mass mailings [spamming]
c. Intentional distribution of viruses, Trojan horses, worms, or other rogue programs
d. Posting or sending any message that is contradictory to the mission of ASUB.
e. ‘Hacking’ into another user’s e-mail account, or viewing another’s e-mail without permission
f. Distribution of chain letters
g. Personal profit or commercial use

h. Distribution and forwarding of alarming e-mail not related to ASUB such as scams and hoaxes
i. any act that violates the Title IX and/or Sexual Harassment Policy

Any alarming e-mail such as scams and hoaxes should be forwarded to ITS for appropriate action. E-mail account users should be aware that ASUB is a state agency and as such, all correspondence sent or received via an ASUB e-mail accounts may be monitored and disclosed to third parties including law enforcement personnel due to the Freedom of Information Act (https://arkansasag.gov/resources/foia/).

8004 Internet Use

This guidance is implemented to ensure that Internet access does not impair network security, result in inappropriate use, or impede learners from performing their duties as an employee or student.

Any use of the Internet for such purposes as gambling, viewing pornographic material, or any activity that is unlawful or degrades, impacts, or restricts acceptable uses is strictly prohibited. All ASUB computers are subject to periodic audits, and violations of this guidance may result in temporary or permanent restriction of access.

References:
US Children's Internet Protection Act 28
US Code Title 17 Copyrights

Procedure:

Internet access is provided for the purposes of enhancing education, research and development, and conducting college business. Acceptable uses include staying current with developments in a specific discipline, researching for class projects, or learning about new technologies. Other appropriate uses include communications with peers and researching products for purchase. All ASUB computers are subject to periodic audits, and violations of ASUB Rules, Processes and Procedures may result in temporary or permanent restriction of Internet access. Offenses in violation of local, state, or federal law will result in restriction of network access and will be reported to the appropriate law enforcement agency.

8005 Portable Computer Responsibilities and Use

Arkansas State University-Beebe provides employees with computing devices that are to be used in the best interest of the college.

When an employee is assigned a computing device, he/she takes responsibility to protect the device, any accessories provided, and the installed software on and off campus. If the device is damaged or stolen, the user can be held financially liable for the loss.

Employees are not allowed to add, modify, replace, or remove any component or software of the computing device without prior approval from the Chief Information Technical Officer. Repairs or changes to the device can only be performed by an ITS department employee or by a contracted maintenance company under the direction of an ITS employee.

Computing devices are ASUB property, and employees should not use the assigned device for purposes other than those related to their ASUB position and duties. In addition, employees are expected to respond to the ITS request relating to the device in a timely manner. This includes making the device and accessories available when requested.

Procedure:

Portable computers are to be used in the best interest of ASUB.

Portable computers are intended to be used when an employee requires the ability to travel and use electronic files outside of his/her office at ASUB. The flexibility of portable computers is recognized as a means of enhancing an employee's work in the area of instruction. This will allow faculty the flexibility to prepare for course instruction and deliver the material with the least number of obstacles and distractions.

When an employee is assigned a portable computer, he/she is taking responsibility to protect the portable computer hardware components and the installed software on and off campus. In the event that the portable computer is damaged or stolen, the user can be held financially liable for the portable computer loss. The value of the loss will be deemed at the time of loss by a calculation to be determined by ASUB chief financial officer. Therefore, it is in the best interest of computer users to ensure that their homeowners/renters insurance and automobile insurance can cover the loss of a portable computer and that the user is able to fund the deductible as indicated in his/her insurance policy. If a user does not agree or is unable to provide financial insurance for the portable computer, the portable must remain on campus.

If the portable computer is stolen, the employee is required to immediately notify the appropriate police department or security office and the ASUB Information Technology Services as soon as possible. If the portable computer is stolen off campus, the local police department should be notified where the portable computer was stolen, and a police report should be completed. If the portable computer is stolen on campus, campus security should be contacted to complete an incident report. In both cases, a copy of the report must be provided to ITS. Information Technology Services must also be notified if the portable computer is damaged.

8006 E-Mail Retention and Archiving

All material, electronic or otherwise, created by employees and volunteers of ASUB in the course of their employment or accessed by employees on ASUB equipment is the property of the College. Archived ASUB Microsoft 365 emails are stored on the local user's computer. Access to these files is not guaranteed in perpetuity.

Procedure:

All Arkansas State University-Beebe e-mail information transmitted or received through the internal e-mail system shall be categorized as general correspondence. There shall be no attempt to treat any correspondence as priority e-mails unless directed to do so by an authorized entity.

General correspondence covers information that relates to interactions and the operational functions of the college. The individual employee is responsible for e-mail retention and archiving of general correspondence where this is likely to be of continuing usefulness. It shall be the responsibility of the ITS to maintain backup tapes from the internal e-mail server for the purpose of disaster recovery only.

8007 Electronic Signature

Arkansas State University-Beebe utilizes e-signatures which are reviewed periodically for appropriateness and continued applicability.

An e-signature may be accepted in all situations if requirement of a signature/approval is stated or implied unless laws specifically require a written signature. The college does not limit the right or option to conduct the transaction on paper or in non-electronic form and the right to have documents provided or made available on paper at no charge. The e-signature must be protected by reasonable security measures as applicable to established computer functions of the College.

Procedure:

The Electronic Signature procedure is supported by methods that are practical, secure, and balance risk and cost. It is not the intent of this guidance or procedure to eliminate all risk, but rather to provide a process that gives parties assurance that appropriate analysis was completed prior to implementation of e-signature, and that the level of user authentication used is reasonable for the type of transaction conducted.

The e-Authentication Risk and Requirements Assessment (eRA) procedure is the risk and assurance level evaluation tool to be used at ASUB. User authentication entails verifying the user’s unique credentials, username and password. This requires validation against specific ASUB held information in the Active Directory. Security and access to ASUB specific information is determined by a “record custodian.” Record custodians are responsible for compliance with all legal obligations related to information, and in that capacity have final authority for the utilization, access, and release of data under their jurisdiction. In some instances, there are multiple custodians for various sets of data.

College transactions enabled by e-signatures will be evaluated using the eRA procedure. (This includes any existing implied or explicit e-signatures in use prior to the adoption of the guidance.) For risk assessment and review purposes, similar types of transactions may be grouped together under one agreement. Implemented e-signatures will be reviewed periodically for appropriateness and continued applicability.

8010 GUIDANCE ON INFORMATION SECURITY

Arkansas State University-Beebe (ASUB) maintains electronic information resources which are essential to performing College business. Like any other capital resources owned by the College, these resources are to be viewed as valuable assets over which the College has both rights and obligations to manage, protect, secure, and control. College employees, students, and other affiliates are expected to utilize these resources for appropriate purposes, protect access to them, and control them appropriately. Examples of information resources include, but are not limited to, computer systems, network systems, software and data.

Definitions

A. **Chief Information Technology Officer (CITO)** – works in conjunction with information resource owners, data administrators, and departmental data security liaisons to ensure that access rights to systems and data are consistent and applicable as individuals' jobs require.
B. **Resource Owner** - An administrative officer within the College-given responsibility for managing specific information resources within a functional area. These resources may be equipment-related or data-related.
C. **Resource Steward** - An individual appointed by a Resource Owner to manage a subset of the resources designated as being within the area of responsibility of that Owner.
D. **Resource User** - Any individual requiring access to College information resources while meeting the requirements of the work position or an educational curriculum.

8010.1 Purpose

This guidance sets forth the mechanisms by which data stored on College-owned computing systems and utilized by College employees and students is secured and protected. This guidance is adopted and promoted in order that:

A. The college can meet its record-keeping and reporting obligations as required by state and federal law, the Board of Trustees and College administrators.
B. The college can comply with the Family Educational Rights and Privacy Act of 1974 (FERPA - the Buckley Amendment) and other statutes and policies protecting the rights of individuals.
C. The college can consistently maintain data integrity and accuracy.
D. The college can assure that authorized individuals have timely and reliable access to necessary data.
E. The college can assure that unauthorized individuals are denied access to computing resources or other means to retrieve, modify or transfer data.
F. Every employee, student, and affiliate of ASUB must be aware of these risks, and act in a way to protect the information resources of the college.

8011 Scope

This guidance applies to all individuals associated with Arkansas State University-Beebe, including, but not limited to:

- faculty
- staff
- students
- student workers
- contractors
- temporary staff

This guidance applies to the all college-owned information technology hardware and its software, including, but not limited to, desktop workstations, departmental servers, and institutionally available resources, such as:

- servers
- personal computers
- network systems
- access card systems
- computer integrated telephony
- other technology hardware

The guidance applies to all College data, and reports derived from College data; and it applies to all programs utilizing College operational data.

Responsibilities for Information Security

A. The Chief Information Technology Officer (CITO) is responsible for ensuring that Arkansas State University-Beebe has adequate information security, and that this guidance is observed. To that end, the CITO and ITS directors/managers have the added responsibility of developing and publicizing the information security framework and monitoring its compliance.

B. The CITO coordinates the standards, procedures, and guidelines necessary to administer access to College information resources. The CITO works in conjunction with information resource owners, the College Data Administrator, and functional users to develop this material.

C. As expected, every employee, student and affiliate at ASUB is responsible for protection of College assets, including information systems equipment and data. Each employee, student and affiliate is responsible for notifying the CITO whenever he or she observes actions which seem to be contrary to this guidance. The CITO is responsible for responding appropriately to actual or perceived breaches by working together with the Resource Owners and the Information Technology personnel directly responsible for the resource in question.

8012 Passwords

A. Security

1. No one should access college information systems without an authorized network account ID and password. Receiving a network account ID requires approval of the individual(s) responsible for the system in question.
2. A network account ID may be revoked or disabled to protect the system at any time. Network account access will be revoked if the employee, student or affiliate terminates the relationship with the college.
3. Inactive network accounts are temporarily disabled until continued need can be established. Each user is required to change his or her password at least every 90 days. ITS will automatically enforce this when a user has not changed his/her password within the time of expiration.
4. College applications systems must be configured so that only users with authorized network accounts can access them.
5. Network users logged into systems and computers should not leave their workstations unsecured.

B. Guidelines

The following password protection guidelines should be followed:

1. Passwords are not to be shared except in emergency circumstances or when there is an overriding operational necessity.
2. Passwords should be changed *immediately* after sharing.
3. Passwords should not be kept in a location accessible to others or secured in a location for which protection is less than that required for information that the password protects.
4. Passwords or any other sensitive information are not to be sent via email.
5. Stolen or compromised passwords should be changed immediately
6. Passwords are not to be written down and post it in an unsecured area such as a computer’s monitor.
7. ASUB employees are not to provide their user ids and passwords to anyone in person or via e-mail

C. Password Management

All authorized users must enroll in the password management system in order to change and retrieve forgotten passwords. For security reasons, the help desk will no longer be resetting passwords over the phone. Persons not enrolled in the system and need assistance with their password will need to come in person to the help desk with a valid ASUB ID.

To enroll in the password management system, network users will need to go to ASUB Password Management System.

8013 Rules, Process and Procedures Awareness

A. Every student, employee, and affiliate of ASUB should have access to a copy of this guidance via the ASUB ITS webpage. All new students and employees should be made aware of the importance of information systems security and their responsibilities in the process. All effort should be made to include this guidance in existing communication mechanisms for dissemination.

B. Prior to network accounts being issued, the Resource Stewards of each department are responsible for notifying employees of the security practices of their departments, and the guidance of the College.

C. All students must be made aware of the Information Security Guidance. The Vice Chancellor of Student Services (VCSS) is responsible for notifying students of information security practices relating to students.

D. All affiliates must be made aware of the Information Security Guidance. The sponsoring official is responsible for notifying the affiliate of information security practices relating to affiliates.

8014 Access to Equipment

Only authorized persons whose work requires it will be allowed access to information systems resources. All information systems resources will be protected against fire, water, physical damage and theft. The appropriate protection will be selected from among physical barriers, environmental detection and protection, insurance, and other risk management techniques.

8015 Data Protection and Security

All data and program files on college information systems will be protected against unauthorized changes. Sensitive data and program files will be protected against unauthorized reading and copying. ASUB requires that all employees save their data files on the network drives instead of the storage on the local PC. Furthermore, employees who make copies of data on thumb drives and CDs must take responsibility to ensure that sensitive information such as social security numbers, credit card numbers and addresses of ASUB employees and students have additional layers of protection. College information systems shall be configured to control which network accounts can read and/or write to any given file. Every file shall be associated with an owner. The owner of each file is responsible for specifying whether the file is sensitive and which network accounts should be allowed to read and/or write to it.

All college data must be stored in devices that are backed up by the data center. This essentially means that individual users and departments that need to work with college data locally on their workstations must store the data on the network to protect from inadvertent loss of data.

8016 Violations

Violations of this guidance incur the same types of disciplinary measures as violations of other College rules, processes or procedures including, but not limited to, the revocation or disablement of the network account.

If network account credentials are compromised or unauthorized and sensitive data is discovered on employee desktop computer, laptop, tablet, or other mobile device during routine scan, the following disciplinary measures will incur.

- **First offense**: communication to user and supervisor + disabling of network account + one business day to report to ITS for mandatory one-on-one training.
- **Second offense**: communication to user and supervisor + disabling of network account + one business day to report to ITS for mandatory one-on-one training + recommendation of formal write-up to be placed on employment records and report to legal.

Documentation of the corrective action is taken on the Corrective Action Report (CAR). The CAR will then be housed in the employee or student record.

Corrective Action Report (CAR)

CAR Nº CAR-YYYY-001	**Corrective Action Report (CAR)**	Date CA Taken:

Department or Section where CA is required:	**ITS**

1. DETAILS: Corrective Action required as a result of:

☐ Internal audit	☐ Suggestion (improvement)
☒ IT Security Incident	☐ Others
☐ Customer complaint	________________________________

2. REFERENCES: Documents used or referred-to (e.g. manuals, procedures, flowcharts, standards, records ...)

3. DESCRIPTION: Description of suggestion, complaint or incident.

Detected or Observed by: ITS Systems team	Department: ITS

4. DISPOSITION: Immediate remedial action

Completed by:	Date:	Implementation date:

5. CORRECTIVE ACTION: Action taken to correct/prevent suggestion, complaint or incident	
Corrective Action:	
Proposed by: IT Security	Date:
	Proposed implementation date:
6. FOLLOW-UP OF IMPLEMENTATION CORRECTIVE ACTION:	
Implementation of corrective action is: 1.	
Name:	Date:
Implementation of corrective action is:	
Name:	Date:
Implementation of corrective action is:	

Name:	Date:
Implementation of corrective action is:	

8017 Revisions

As an ongoing document, the ASUB Information Security Guidance will be reviewed on an annual basis, in cooperation with Resource Owners and Department of Information Technology advisory groups. All affected parties are encouraged to correspond with the Chief Information Officer regarding any suggestions for revising this document.

8018 Cloud Computing Guidance

Scope

This guidance applies to all persons accessing and using 3rd party services capable of storing or transmitting protected or sensitive electronic data that are owned or leased by ASUB. Additionally, consultants or agents of ASUB and any parties who are contractually bound to handle data produced by ASUB must be in accordance with the College's contractual agreements and obligations.

Purpose

The purpose of this guidance is to ensure that ASUB Protected or Sensitive data is not inappropriately stored or shared using public cloud computing and/or file sharing services. Cloud computing and file sharing, for this purpose, is defined as the utilization of servers or information technology hosting of any type that is not controlled by, or associated with, ASUB for services such as, but not limited to, social networking applications (i.e. blogs and wikis), file storage (Dropbox, Microsoft), and content hosting (publishers' text book add-ons). A list of acceptable and unacceptable cloud services is included here for ease of reference

Listing of Cloud Services

This listing is meant to serve only as a partial list of cloud services.

Services Approved for University Use	Services Not Approved for University Use
Microsoft OneDrive	Box
	iCloud
	Amazon Cloud Drive
	Google Drive

Individuals who use enterprise Microsoft accounts for College work are responsible for ensuring that Sensitive information is not placed or stored in unapproved or inappropriate locations. When using Microsoft for College information, use it only for institutional information classified as Public or Sensitive. Pay special attention to access levels when sharing files and folders with other collaborators to ensure that data is not inappropriately shared. You should not use your enterprise Microsoft account to collect, process, or store data covered by laws such as FERPA or GLBA.

Contractual Expectations

The College will seek and endorse vendors who deliver solutions that meet the following requirements.

Both the College and cloud-computing vendor must declare the type of data that they might transfer back and forth because of their relationship. A contract must have clear terms that define the data owned by each party. The parties also must clearly define data that must be protected.

The contract must specifically state what data the College owns. It must also classify the type of data shared in the contract according to the College's classification schema: Public, Sensitive, or Protected. Departments must exercise caution when sharing College-classified sensitive or protected data within a cloud computing service.

The contract must specify how the cloud-computing vendor can use University data. Vendors cannot use College data in any way that violates the law or University policies.

If you have questions about this requirement, please contact IT Security at its@asub.edu.

Rationale for Guidance

This guidance endorses the use of cloud services for file storing and sharing 1) with vendors who can provide appropriate levels of protection and recovery for College information, and 2) with explicit restrictions on storage of College Protected Information. While cloud storage of files can expedite collaboration, and sharing of information anytime, anywhere, and with anyone, there are some guidelines that should be in place for the kind and type of College information that is appropriate for storing and sharing using these services. Even with personal use, one should be aware of the level of protection available for your data using such a cloud service.

There are a number of information security and data privacy concerns about use of cloud computing services at the College. They include:

- The College no longer protects or controls its data, leading to a loss of security, lessened security, or inability to comply with various regulations and data protection laws.
- Loss of privacy of data, potentially due to aggregation with data from other cloud consumers.
- The College dependency on a third party for critical infrastructure and data handling processes.
- Potential security and technological defects in the infrastructure provided by a cloud vendor.
- The College has limited service level agreements for a vendor's services and the third parties that a cloud vendor might contract with.
- The College is reliant on the vendor's services for the security of some academic and administrative computing infrastructure.

8018.1 Data Classification

The following table outlines the data classification and proper handling of ASUB data.

Data Classification	**Cloud Storage (See appendix for approved services)**	**Network Drive *(Username and Password Required)***	**Local Storage**
Restricted	**Not Allowed**	**Allowed**	**Not Allowed**
Limited Access	**Allowed but Not Advised**	**Allowed**	**Allowed but Not Advised**
Public	**Allowed**	**Allowed**	**Allowed**

Use of central and departmental servers, where ASUB authentication is required, is the best place to store all categories of College data, particularly Restricted Data. It is never acceptable to store Restricted Data on any cloud service.

General Data Protection Terms

The College must specify particular data protection terms in a contract with a cloud-computing vendor. In this way, ASUB creates a minimum level of security for College data. A minimum level of security ensures that the College data is kept confidential, is not changed inappropriately, and is available to the College as needed.

The College should consider the following contract terms to ensure a minimum level of information security protection:

- Data transmission and encryption requirements
- Authentication and authorization mechanisms
- Intrusion detection and prevention mechanisms
- Logging and log review requirements
- Security scan and audit requirements
- Security training and awareness requirements

Compliance with Legal and Regulatory Requirements

The College has many federal laws that it must follow, these include the Family Educational Rights and Privacy Act of 1974 (FERPA), and the Gramm-Leach-Bliley Act (GLBA).

Finally, cloud-computing services that use, store, or process College data must also follow applicable guidance. Such guidance may include ITS rules, processes and procedures, and the College's data handling requirements.

8019 Firewall Exception Procedure

Firewall exceptions added to the ASUB firewall most adhere to the following:

- Firewall exceptions (open ports) must be requested in writing
- Requests must be justified and approved by Chair/Dean/Dept. Head
- Requests must be reapproved every 6 months
- ITS may scan devices that can be accessed via open ports for security issues. All issues found must be corrected/justified in two weeks or the firewall exception will be closed
- ITS may close an open port at any time for security reasons
- ITS may, at its discretion, decline to open a port
- ITS may require that a device be moved to the DMZ instead of opening a firewall port
- Maintaining devices in the DMZ is the responsibility of the department the owns the device
- Devices in the DMZ may be scanned by ITS for-security issues and sensitive data
- ITS may disable access to a device in the DMZ if it fails said scans
- Devices failing scans must be corrected/justified in two weeks or access to the device will be disabled
- According to IBM Security Intelligence, one in five recipients of a phishing message will fall victim to it and hand over sensitive information, such as usernames, passwords and account numbers. This is an area where IT Security wants the College to be well below average. Knowing what tricks our faculty, staff, and students fall for will help us better target our security awareness training materials.

8019.1 IT Security Self-Phishing and Counter-Phishing Training Procedure

IT Security may conduct self-phishing programs in order to aid the ASUB students and employees in better recognizing phishing attempts. Since phishing is one of the primary methods malicious actors use to compromise credentials and other sensitive information, it is important that they be able to recognize such attempts and not respond to them. The best way to accomplish this is through training. This training will focus on conditioning users to identify and report phishing emails.

See **Appendix B** for IT Security Incident Response Plan

8019.2 VPN Access

The Security Task Force recognizes the importance of maintaining the integrity and security of ASUB technology assets. VPN access to the ASU-J computer network is currently open to all employees. When connected to VPN, computers have direct access to the network without going through the external firewall. This unrestricted access to the network could increase its exposure to viruses, malware, and could allow hackers using compromised accounts greater access to the College's network.

VPN Access Procedure

VPN's access allows users unrestricted access the ASUB computer network from locations external to campus. This unrestricted access to the network could increase the College's exposure to viruses, malware, and could allow hackers using compromised accounts greater access to the ASUB network.
In light of the above, ASUB has adopted the following procedures for VPN access**:**

- Remove users who haven't accessed VPN in the past 12 months from the data this procedure is approved
- Chair/Dean/Dept. Head approval for all remaining accounts
- Chair/Dean/Dept. Head approval for all new access
- 12-month renewal of access approval
- Connections must support Layer 2 Tunneling Protocol (L2TP) as a minimum standard
- Access may be suspended/terminated by ITS at any time if access could cause security issue
- VPN access is logged, and the logs will be retained for 5 years
- Logging may include connection/disconnection times, IP address received from DHCP, connecting IP address, IP address(es) accessed, and the username that opened the connection
- ITS may require devices connecting via VPN to be scanned for patch levels of OS/software, current antivirus software, or other security related issue. Users can check/download updates for their operating system by clicking on Windows Update in the Control Panel for Windows based machines and Software Updates under System Preferences on iOS-based machines.
- Devices failing security scan may be denied VPN access

8020 Computer Administrative Rights

Introduction and Guidance Section

Arkansas State University-Beebe (ASUB, College) provides desktops and laptops to employees to perform college related functions. This guidance is intended to support the goal of ensuring the highest-level stability and usability of the ASUB issued computers. This is based on the premise that computers are productivity tools where stability and usability are most important. In such environments, limiting **administrative privileges** is an Information Technology Services (ITS) best practice because change management is one of the foundations of providing stable computing environment.

Administrative rights are restricted by default on all desktops and laptops since they can have a profound impact on stability and usability. Due to the availability of trained and experienced support staff and the inherent dangers of inappropriate, uninformed, or unintentional use of logins with administrative rights, the College's rule is to restrict the use of administrative rights.

Administrative rights are typically reserved for ITS personnel who are responsible for providing administrative services such as system maintenance and user support. However, in unique instances, administrative rights may be issued to faculty and/or staff on either a temporary or ongoing basis to perform tasks within the scope of their employment. Users who have demonstrated the ability to configure and manage their workstations and who possess an understanding of the responsibility of maintaining appropriate security measures may be granted administrative rights on their computer. Users who have been granted administrative rights on their workstations are herein referred to as **power users**.

8020.1 Power User Responsibilities

Power users are responsible for:

- changing their AD password every 60 days;
- maintaining the integrity of their workstation;
- any accounts they create on their own computer;
- maintaining software licensing information for any software personally installed on their workstation;
- routinely checking for and eliminating spyware, or any similar data gathering and reporting software, from their workstations;

- NOT sharing their username and password with others for access to the ASUB network;
- reporting any system failures and/or compromises in security measures to ITS Helpdesk;
- adhering to all ITS Rules, Processes and Procedures.

Power users must not install or use software that are considered insecure or that do not incorporate an encryption scheme. Additionally, all software must be legally licensed. These include but are not limited to email applications, FTP clients, and Telnet applications that do not employ secure connections.

8021 The Alternative to Power User Status

As an alternative to personally acquiring administrator rights on the workstation, the Information Technology division highly recommends contacting the ITS Helpdesk to schedule software installations.

8022 Information Technology Services Terms of Support

The ITS will continue to provide Microsoft system patches, application software patches, anti-virus updates, and application software to all ASUB workstations. ASUB computer users must not block or in any manner disable and/or revise any services on the workstation that may prevent these and other routine maintenance procedures.

ITS will not be able to restore a configuration customized by the user.   In the event of a computer failure, the ITS group will restore the original base image on the computer.

The base image includes an operating system and any software maintained by ITS. All documents that are synchronized to the network server will be restored if possible. All ASUB issued desktop machines must be administered in accordance with standard configurations, and all computers must:

- be joined to the ASUB Active Directory domain and;
- have remote management software installed to facilitate administration and upgrades and;
- have properly configured anti-virus software and;
- have service packs or patches as deemed necessary by ITS Staff.

Note: Network monitoring and intrusion detection is performed as deemed necessary and appropriate by designated ITS staff.

8023 Loss or Denial of Power User Status

If a user abuses his/her administrative access, the ITS will revoke this access immediately and will restore the original base image on the computer. Abuse is defined as, but not limited to:

- downloading software (intentionally or accidentally) that is malicious to the ASUB network;
- downloading unlicensed/illegal software;
- downloading copyrighted material without permission;
- public exposure of sensitive data
- not adhering to Information Technology policies and procedures.

Violation of this guidance or repeated support problems will result in revocation of the authorized user status and/or other sanctions.

8024 Applying for Authorized User Status

For audit purposes, ASUB must have on file documentation showing that Administrative Rights have been formally requested and approved. If an ASUB employee, would like to be granted the power user status, they must follow these steps:

1. Submit a formal request via e-mail articulating the need for such status
2. Receive approval from the Chief Information Officer
3. ITS staff member will configure the desktop and the user to have Power User status.

8030 CHANGE MANAGEMENT PROCESS AND PROCEDURE

8030.1 Scope

This process and procedure statement provide direction on the application of change management for server and infrastructure devices supporting Arkansas State University-Beebe (ASUB) internal and perimeter networks. For the purposes of this process and procedure statement, a change is defined as any alteration to software, hardware, or other aspect of the data processing environment and its attached networks.

This process and procedure statement apply to all employees, contractors, consultants, temporary firs and all other workers at ASUB, including those workers affiliated with third parties who require access to ASUB information systems at all ASUB locations.

This document addresses the procedures for Change Management within ASUB Information Technology Service Area. Only those changes that conform to the Change Management process described in this document are authorized for implementation. Within these standards are the rules of conduct relating to:

- Change Entry
- Change Review
- Testing
- Change Approval
- Change Announcement
- Change Management Meeting
- Implementation
- Report and Control

These processes and procedures shall be governed and performed in accordance with the Office of the Chief Information Technology Officer (CITO). ASUB reserves the right to change these processes and procedures without notification.

8031 Overview

The purpose of change management is to ensure that standardized methods and procedures are used to alter the production environment to minimize the risk for negative impact of change. The specific objectives of applying a change management system are to:

- Implement changes on the schedule
- Publish a calendar that specifies the “maintenance window” (when changes will be allowed) and network availability
- Eliminate or reduce the number of changes that are digressed due to issues without change planning and implementation
- Provide a back out plan for all changes
- Ensure change requests comply with change management standards
- Ensure implemented changes comply with baseline standards

The benefits to be gained from implementation of a change management process are improved system reliability and availability due to more control and thorough planning for installation of changes, as a result of improved communication and awareness of changes.

8032 Roles and Responsibilities

Change Driver

The Change Driver is the individual generating the change. The Change Driver assumes full responsibility for coordination and execution of changes to the production environment. Generally, this is an individual representing the department with the most to gain from the change.

Change Coordinator

The Change Coordinator assumes responsibility for scheduling and communicating the change to all appropriate work groups. This includes:

- Ensuring overall compliance with the documented change process (reviewing, modifying, and reporting as needed)
- Serving as the starting and the focal point for the change management process and procedures
- Monitoring all change requests and plans and ensuring the flow of information
- Keeping all interested parties informed and communicating changes to the appropriate work groups
- Reviewing all change requests for accuracy and completeness
- Scheduling and recording all changes
- Facilitating and conducting meetings, as required

Work Groups

Work Groups are responsible for implementing changes assigned to them. Whenever possible, Information Technology Services (ITS) will implement changes solely. If cooperation from other departments is necessary, all groups will coordinate the integration in a cooperative fashion. Under no circumstances will any entity integrate new applications into a production environment without the assistance from ITS.

Change Requester

The Change Requester is the individual identifying the need for the change and originating the change request process.

Change Management Team

The Change Management Team consists of the Change Coordinator (chairs meeting), Change Requester(s), Director of Enterprise Application, Director of Business and Technical Services, Director of User Support, Director of Assessment and End User Training, Chief Information Technology Officer (or designate), Help Desk Representative(s), Student Service Representative (s) and Other Department Representative(s) as needed.

Quality Assurance

Validates the test plan and procedures for the production change and sign-off or issue mitigation of the proposed production change.

CITO Office

The Chief Information Technology Office approves any exceptions to the formal change process for production systems.

8033 Types of Change

All changes in the Information Systems areas listed below are subject to the Change Management process:

- Hardware
- Applications, Systems and other Software*
- Procedures
- Environment
- Documentation

*See Appendix C for Software Purchase process and applicable form

8034 Elements of Change Management

Change Entry

Change Entry is accomplished by utilizing a software package that is designed to handle problems, change, and asset management or a suitable database or spreadsheet application.

Documenting all changes provides a consistent method for categorizing and gathering the information necessary for successful change implementation. The change request is the vehicle whereby the required information is consistently made available to all parties involved in the change management process.

Change Review

The Change Coordinator will review the changes pending implementation according to the following criteria:

- Proper category assignment—risk to internal and external customers and the production environment.
- Implementation plan—does it accomplish the purpose of the change.
- Test Plans—has there been adequate testing prior to determining outcomes?

- Recovery/Back out procedures—are these well documented? Is the back out procedure clear?
- Task dependencies—are they completed (cable moves, ID assignment, files relocated, etc.)?
- Impact of the change on other scheduled/pending changes

Testing

Testing must be performed in an appropriate testing area and not on the production network. Changes will then be staged for user acceptance. Changes will only be implemented into the production environment upon the user's signature that QA testing was conducted.

Change Approval

Authorized by the Change Management Team based upon the risk assessments, service levels and provided there is a business justification for the change.

Change Status Report

The change agenda, minutes and status report is generated and distributed timely for the Information Technology team meeting. This report will cover changes made during the prior week, changes scheduled for the current week, changes scheduled for the next four weeks, and any open changes previously scheduled but not completed.

Change Management Meeting

This meeting will be embedded in the Information Technology team meeting. The Change Coordinator will provide an agenda of newly submitted items and a change status schedule. The purpose of this meeting is to:

- Bring all interested parties together to assess the feasibility of implementing the change and provide status.
- To review the status of all open changes and schedule for the current and upcoming weeks.
- Discuss high impact changes.
- Introduce and discuss any new changes.
- Approve or disapprove each change as well as the Change Schedule.

Attendees (Change Management Team members) include but are not limited to:

- Change Coordinator (chairs meeting)
- Change Requester(s)
- Director of Enterprise Applications
- Director of Business and Technical Services
- Director of IT Client Services
- Chief Information Technology Officer (or designate)
- Help Desk Representative(s)
- Student Service Representative (s)
- Other Department Representative(s)

If all members are not present at the Change Management Meeting prior to the scheduled implementation of a high or medium impact change, the Change Coordinator pending subsequent review will postpone that change.

Implementation

Change management will track and document the implementation process and communicate the results via the weekly Change Management status report. Any problems associated with the implementation of changes will be discussed at the Change Management Meeting.

Report and Control

To evaluate the effectiveness of the Change Management process, the change coordinator will present monthly volume statistics to management.

Management Reporting

The general status of the change management system will be reported to management weekly as well as monthly basis.

Monthly Report

The monthly report consists of charts showing the number of changes submitted during the month by category (i.e. high, medium, and low risk), the number of problems caused by changes and the process measurements for the month.

Other Meetings

Postmortems will be convened on an ‘as needed’ basis. Post mortems will be held for changes resulting in significant problems to determine what, if anything went wrong and how any such problems may be prevented in the future.

8035 Change Category Definitions

All changes are assigned to one of the following categories based on risk. Risk is determined by the following criteria in order of significance. The individual process differs somewhat for each change category, but some general guidelines are applicable to all categories.

- Timing (the maintenance window in which change is to be performed).
- Who is affected by the change (internal customers, external customers, or both).
- Degree of complexity that the back out plan is based on:
- Length of time
- Number of tasks
- Number of groups to coordinate
- Who the groups are
- Types of changes
- Number of users affected
- Degree of complexity to install based on:
- Length of time
- Number of tasks
- Number of groups to coordinate
- Who the groups are
- Types of changes

The change driver (individual generating the change) assumes full responsibility for coordination and execution of changes to the production environment. The Change Coordinator assumes responsibility for scheduling and communicating the change to all appropriate work groups.

8036 Risk Assessment Definitions

High Risk Changes

These changes fall into the area marked Number 1 on the Risk Assessment Grid (See attached). These changes require detailed planning, scheduling, and coordination of activities and if possible are implemented in steps over an extended period. Formal reviews among all affected parties are required.

- Changes with High risk associated with maintenance window.
- External customers and critical internal departments will be without service if change fails.
- Back out extremely impossible, difficult, or undesirable.

Medium Risk Changes

These changes fall into the area marked number 2 on the Risk Assessment Grid. These changes require planning, scheduling, and coordination activities, and are implemented over time, if possible. Reviews may be requested at the discretion of the Change Coordinator.

- Changes with Medium risk associated with the maintenance window.
- Some significant internal departments will be without service if change fails.
- Back out possible, though not necessarily easy.
- Significant number of users will be without service if change fails.
- Implementation possible, though not necessarily easy.

Low Risk Changes

These changes fall into the area marked Number 3 on the Risk Assessment Grid found. These changes do not require detailed planning but may require scheduling and coordination among one or two other groups over a shorter period of time. No reviews are required.

- Changes with Low risk associated with the maintenance window.
- No external customers or significant internal departments will be without service if change fails.
- Back out relatively easy to perform.
- Limited number of users will be without service if change fails.
- Implementation easy to perform.

Emergency Changes

Emergency changes may be necessary to recover from a system failure, hardware problems or application problems. Emergency changes provide the flexibility required for the timely response to immediate problems. These problems include fixes to prevent recurring/imminent system failure, and the negative impact on business or production problems.

Exceptional Changes

Extenuating circumstances will occur, and changes will need to be made for certain business reasons. These circumstances must be documented and included as part of the request package. In addition, mutual consent between the Change Coordinator and the change requestor(s) must occur to allow for the possible re-prioritization of the Change Coordinator’s workload. Signatures at management level will be required.

Changes of this type are rare and high risk in nature in that they will not be subjected to the same criteria as those outlined above. Due to a shortened implementation period, the appropriate amount of allowances may not occur.

8037 Risk Assessment Grid

Change Categories	High	Medium	Low
Effect on Environment Timing (maintenance window)			
Effect on Environment Who the users are (External, Internal or both)			
Degree of Complexity to Back out/Recover How long to Back out/Recover Number of tasks Number of groups to coordinate Who are the groups? Types of changes			
Effect on the Environment Number of users			
Degree of Complexity to Install How long to install Number of tasks Number of groups to coordinate Who are the groups? Types of changes			

Score: Total Value will determine the potential risk for the organization for the change.

Score of 1 The highest risk value to the organization. These changes require detailed planning, scheduling, and coordination.

Score of 2 Requires intermediate risk level to the organization. Changes require moderate planning, scheduling, and coordination.

Score of 3 Requires minimal risk value. Detailed planning is not necessary however scheduling and coordination is needed.

APPENDIX A- Information Technology Strategic Plan (approval expected 6-17)

APPENDIX B - IT Security Incident Response Plan

APPENDIX C - Software Purchase Process and Request Form

APPENDIX D - Service Level Agreement

APPENDIX E – Student Connectivity Card

APPENDIX F – Information Technology Communication Plan

APPENDIX G – Service Guidance Document