8.0 CENTER FOR INFORMATION TECHNOLOGY SERVICES POLICIES AND PROCEDURES

Under the leadership of the Chief Information Officer (CIO), CITS is responsible for ensuring the sufficiency of technology and technology infrastructure to support the mission and vision of the university. This encompasses maintenance of existing technology including upgrade strategy, institution of standards and best practices, assurance of security, reliability and disaster recovery across platforms and sound long-range technology planning.

The policies and procedures in this manual govern and apply to all access to and/or use of information technology at Alcorn State University including students, faculty, staff, alumni, agencies, vendors, contractors and consultants. Any attempt to violate, undermine, circumvent or otherwise subvert the letter and spirit of the policies and procedures in this document will be subject to the appropriate consequences.

8.1 MISSION STATEMENT

To ensure state-of-the-art technology that provides reliable, secure, functional and easily accessible information resources and related services that empower our students, faculty and staff by focusing on customer needs and innovation.

8.2 HOURS OF OPERATION

CITS services are available during the following hours of operation: Monday through Thursday from 8 a.m. until 5 p.m. and Friday from 8 a.m. until 4 p.m. The ATSC Lab is open Monday through Friday from 8 a.m. until 8 p.m.

The hours of operation are subject to change. For issues that arise outside normal hours of operation, please leave a request for service via voice mail at ext. 6182 or send email to heldesk@alcorn.edu. Requests will be processed in the order in which they are received.

8.3 LOCAL ADMINISTRATIVE RIGHTS FOR END USERS

CITS does not extend local workstation administrative rights to end-users by default. This policy is intended to support the goal of ensuring the highest level of security, stability and usability for all computers on the ASU network. Computers set up by CITS for use on the Alcorn network are equipped with a standard configuration that is flexible and functional enough for normal day-to-day operations but secure enough to prevent inadvertent security attacks or reduced performance. If a user needs to obtain additional software or access a resource which requires local administrative rights, he or she should contact the CITS Help Desk for assistance.

In some instances, he or she may be granted local administrative rights to his or her workstation but only after demonstrating sufficient technical competence and a compelling reason.

Administrative rights may be revoked at the discretion of appropriate CITS personnel if it is determined that administrative rights have been misused or granted in error.

Contact the CITS Help Desk at (601) 877-2487 or helpdesk@alcorn.edu to request administrative access.

8.4 SOFTWARE

8.4.1 SUPPORTED SOFTWARE

CITS provides access to a number of software applications necessary for the University to carry out its mission. For the purposes of this document, access refers to acquiring, installing and supporting applications deemed mission critical to the University and applications requested by individual administrative units or academic departments.

Alcorn State University is committed to respecting copyright and intellectual property laws; therefore, any software installed on University inventoried computers must be properly licensed. Any student, faculty or staff that uses University technology resources to receive, obtain, install or allow to be installed on a University-owned computer improperly licensed (pirated) software shall be in violation of this policy and subject to disciplinary actions as prescribed by the Acceptable Use Policy and/or official actions deemed appropriate by the University administration up to and including criminal investigation and prosecution.

The list of supported software is revised periodically and available on the CITS website (www.alcorn.edu/CITS).

8.4.2 OFFICIALLY SUPPORTED SOFTWARE

Officially supported software refers to software applications acquired and installed by CITS for campus-wide distribution. Examples include the Banner ERP software or Microsoft productivity software products.

CITS is exclusively responsible for maintaining current licensing agreements and, as appropriate, vendor/developer maintenance contracts in support of these titles. CITS provides configuration and usability guidance as well as troubleshooting and problem resolution for these applications. In addition, CITS coordinates user training for officially supported software.

In order to ensure compliance with software metering policies, software must be installed through the www.Alcorn.edu domain. CITS is responsible for applying all updates and patches to officially supported software in a timely manner. Unless otherwise noted, CITS will support the latest two versions of designated officially supported software.

8.4.3 PARTIALLY SUPPORTED SOFTWARE

Partially supported software refers to software applications which are used for a limited purpose or specific audience. Examples of this kind of software might include SPSS or Monarch. CITS may acquire the license for these titles or they may be acquired through the requesting department's budget. CITS Help Desk support is limited to the trouble-free installation and proper function of the application itself, not usability issues. Users of partially supported software are expected to have other resources to assist with learning and using the software package. CITS may provide limited, "best effort" support as time permits.

8.4.4 UNAUTHORIZED SOFTWARE

Unauthorized software refers to software which serves no justifiable business need and/or which potentially negatively impacts the performance, efficiency or security of the employee, computer or network. This may also include access to certain websites or plug-ins needed to access these websites. Examples of unauthorized software or websites include P2P file sharing applications such as Ares, Morpheus or Limewire, improperly licensed software, software update tools or download managers.

Users are encouraged to consult the CITS Help Desk at (601) 877-2487 or helpdesk@alcorn.edu before installing or accessing questionable software applications or websites.

8.5 APPROPRIATE USE POLICY (AUP)

This policy governs the use of computers, computer-based networks and related equipment administered by Alcorn State University. The intent of this policy is to allow maximum freedom of use consistent with state and federal law, IHL/University policy and a productive work environment.

All individuals who need or desire to access the ASU computing and networking facilities must sign an Appropriate Use Policy (AUP), which outlines in detail the principles; expectations and consequences associated using these resources. A copy of the AUP in its entirety is available on the CITS website or by contacting the Help Desk at (601) 877-2487 or helpdesk@alcorn.edu.

CITS may also provide temporary access accounts as needed for consultants or vendors who need this access to perform services for the university.

8.6 CITS RIGHT OF EXAMINATION

By signing the AUP, the user acknowledges that CITS system or network personnel are duly authorized, under the direction of CITS management, to examine user files and activities if necessary. No guarantee of complete privacy is made. CITS management reserves the right to stop any process, restrict any individual's use, inspect, copy, remove or otherwise alter any data, file, or system resource that may undermine or adversely affect the overall performance or integrity of the computing and networking facilities.

CITS system and network administrators have taken reasonable precautions to ensure that potentially offensive materials do not reside on local facilities; however, CITS is not responsible for materials on remote sites. Individuals are cautioned to exercise judgment in accessing such materials.

Contact the CITS Help Desk at (601) 877-2487 or helpdesk@alcorn.edu to report suspected misuse of the appropriate use policy.

8.7 WIRELESS COMMUNICATIONS

This policy establishes the standards for the usage of wireless communication devices by the employees of Alcorn State University (ASU).

Employees may not directly or indirectly use, or allow the use of ASU property of any kind, including property leased to ASU, for other than officially approved activity. In addition, all employees shall protect and conserve ASU property including wireless communications equipment. Wireless communications equipment includes:

- Cellular phones
- Personal digital assistant devices
- Standard and two-way pagers
- Similar devices that perform some or all of these functions.

Employees are hereby notified that ASU will enforce this policy through a variety of methods and may monitor use of wireless communications equipment to assure compliance.

Wireless communication devices shall be used for legitimate state business only. Use of an ASU-provided cellular phone for personal calls will result in appropriate disciplinary action and/or the loss of the use of the phone.

Before a wireless communication device is provided to an ASU employee, the departmental director must certify in writing the need for the device and associated service. Each employee is responsible for working with his or her supervisor to determine the most cost-effective communication device and/or service for a given role.

Employees are required to:

- Know and understand the details of the wireless communication service plan utilized by that employee including unit costs and any monthly service caps.
- Review and certify billings for the device and service utilized.
- Assess the need for any change in usage patterns and/or plans based on actual utilization and cost.

- Verify billing details monthly and indicate by signature that the billing is correct, that all calls were work-related and that the calling plan is still appropriate to the employee's business needs.

Employees must be aware that cellular phone calling plans are selected based on the projected number of minutes required for the employee to conduct official business. Package minute plans are not to be construed as free minutes and are not provided for personal use.

Detailed call billing must be provided for all ASU cellular phone accounts, and all billings are considered public records subject to disclosure under the Mississippi Public Records Act. ASU shall not reimburse employees for any charges on personal wireless communication devices.

Employees should be aware that cellular phone transmissions are not secure transmissions. Confidential information regarding official business should be transmitted from a secure environment.

8.8 INFRASTRUCTURE MAINTENANCE AND UPGRADE

It is the goal of CITS to provide a robust technology environment with optimal features, functionality, security, redundancy and minimal downtime. It is necessary to perform maintenance and/or upgrade functions periodically, which may impact the end user's ability to access or operate one or more systems. Whenever these outages become necessary, CITS personnel work diligently to schedule them at times when system usage is lowest. CITS also provides as much advance notice to the user community and those who will be affected by the outage as possible. When possible, information about benefits of the maintenance or upgrade is also provided.

8.9 HARDWARE AND SOFTWARE STANDARDS

CITS will provide support for standardized, campus-wide hardware and software. The list of approved hardware and software is updated regularly and can be found at the CITS webpage at www.alcorn.edu/CITS. Please review these guidelines:

- To ensure software license compliance, CITS will not install any software without proof of purchase or a copy of a license agreement.

- When purchasing computer hardware, please refer to the current hardware standards document and select from the pre-approved list whenever possible.

- All non-standard hardware and software purchase requests must be accompanied by a letter of justification and must be approved by the CIO.

CITS offers consultation and assistance with hardware/software purchases. Limited support for non-standard equipment and software is also available, depending on the availability of technical resources.

8.10 EMERGENCY MAINTENANCE

Occasionally, CITS must quickly respond to a security threat, hardware malfunction or other unforeseeable situation, which threaten the security or stability of systems. Such situations are evaluated case by case, and necessary measures are taken. Whenever possible, users will be notified of the emergency status and given an approximate time to expect service to be restored. Following the outage, an explanation of the problem and resolution may be made available on the CITS website.

8.11 ADMINISTRATIVE SOFTWARE

Alcorn State University uses the SungardHE Banner software as its ERP solution for administrative computing. Access to this software is granted as needed based on an employee's role at the University. Temporary assignments or special scenarios are evaluated on a case-by-case basis. Students are not assigned credentials to access the baseline Banner system.

The team leader is responsible for ensuring that each person who is granted Banner access is fully aware of the FERPA and HIPPA regulations that govern access to and confidentiality of information in Banner. Current team leaders and contact information can be found on the CITS website or by contacting the Director of Administrative Technologies.

8.12 BANNER SYSTEM ACCESS

The Director of Administrative Technologies is responsible for assigning and revoking access to the Banner system based on established criteria and for resetting self-set passwords as needed. Each of the five Banner systems (Student, Finance, Financial Aid, Human Resources and Advancement) has a team leader whose responsibilities include requesting access for new users of the Banner system. It is the responsibility of the team leader requesting the access to ensure the employees gain only the access needed for their role or job responsibility. The team leader makes the request to the Director of Administrative Technologies who then creates the accounts with the appropriate access and returns the credentials to the team leader for distribution.

It is also the team leader's responsibility to inform the Director of Administrative Technologies when a person on his or her team needs different access due to a change in roles at the University.

For example, an employee in the Registrar's Office accepts a position in Advancement. The Student team leader must communicate to the Director of Administrative Technologies that the employee no longer needs access to the student forms and the Advancement team leader must let the Director of Administrative Technologies know what access is needed for the new role.

In the event an employee is terminated, the Office of Human Resources communicates directly with the Director of Administrative Technologies to remove Banner access for the employee.

Some Banner systems have internal levels of security, which are controlled within the software; specific team members are responsible for maintaining those security features but may request support or assistance from CITS if needed.

Contact the CITS Help Desk at (601) 877-2487 or helpdesk@alcorn.edu for questions about password safety or for instructions on how to change a password.

8.13 BANNER PATCHES AND UPGRADES

Pertinent major and minor releases of SungardHE Banner application will be conducted in an orderly and timely manner. In the event Banner users need a patch or upgrade implemented before the scheduled time, such users should communicate this situation to the appropriate Banner team leader. Every effort will be made to accommodate user requests for application-specific patches as long as the patches do not negatively impact the operation of other users.

8.14 APPLICATION DEVELOPMENT

CITS has developed a number of custom applications. Some enhance and extend the capabilities of the Banner suite of products, others are stand-alone applications and others still are custom integrations, which allow separate applications to communicate and share data.

The development of such customized applications is based in part on a demonstrated need for new functionality to make current processes more efficient and to have more resources available to build, implement and maintain the new application.

End users may submit a request for application development through the Banner team structure, if appropriate, or directly to the Director of Infrastructure for a feasibility review. If the proposal is accepted, a response will be generated within 2 weeks regarding the specifics necessary for completion.

8.15 BACKUP AND DISASTER RECOVERY

As part of the University's overall disaster recovery plan, CITS also maintains a comprehensive disaster recovery plan for IT systems. The plan for system backup and recovery is a critical function of disaster recovery.

CITS requires that all enterprise information stored electronically in computerized form be backed up on a routine basis to ensure its safety in the event of a severe hardware or software interruption, virus attack or other disaster. All operating software and application software necessary to access, recreate or generate the information is also backed up. A strict schedule of system backup is documented and maintained in CITS.

8.16 LOCAL BACKUP PROTOCOL

CITS performs backups of critical systems daily between 2 a.m., and 4 a.m. During this backup process, many of the applications need to be offline to carry out comprehensive backups. Banner, Blackboard, Voyager, etc. are examples of systems where a daily backup is done. These applications cannot be accessed during this time.

8.17 WEB POLICY

Maintenance of Alcorn's public facing website(s) requires a collaborative effort between CITS, University Relations and authorized content mangers. CITS is responsible for maintaining the technical environment to support the website(s) (i.e. web and media servers, content management system, web development, etc.). CITS is also responsible for developing appropriate web interfaces for internal web-based applications.

University Relations oversees policy and direction related to the accuracy, integrity and effectiveness of website content. Authorized content managers are responsible for maintaining the content on their respective site(s). CITS provides assistance and training for content managers assigned to maintain web content for their department or unit.

CITS is also responsible for maintaining the web server, including installation or upgrade of software, development of web templates for websites and applications and special requests and development of new functionality or integrations.

8.18 FEEDBACK

CITS will be proactive in seeking feedback through follow-up calls after a service request has been completed and through periodic online surveys. The University community is encouraged to provide feedback regarding the Help Desk services at any time by sending an email to helpdesk@alcorn.edu.

8.19 TELECOMMUNICATIONS

Telecommunications is the CITS unit, which handles the VOIP phone system and employee cell phone services. Telecommunication service for the VOIP phone system (office phones) includes installation, repair, billing, directory services, and long distance access codes.

Cell phone service includes initial setup and ordering of the phone. All cell phones must be used to conduct University business only. Employees issued a University cell phone must sign and comply with the state agency policy.

8.19.1 TELECOMMUNICATIONS SERVICE AUTHORIZATION

The Center for Information Technology must be contacted if you need to add, change or discontinue any of the following telecommunication services:

- Telephone/Cellular connection
- Telephone/Cellular equipment transfer
- Telephone/Cellular upgrade
- Telephone/Cellular services
- Addition/Removal of fax lines
- Telephone and voice mail features

8.19.2 LONG DISTANCE CODES

Employees have access to unlimited local calling only; the department head or supervisor must approve requests for long distance access. Employees are responsible for all long distance calls from their phone extension.

8.19.3 TELEPHONE BILLING

Telephone invoices are sent on a monthly basis to the departmental budget managers for business calls verification and signatures. Departments are individually billed for local calling and long distance calling.

8.19.4 TELECOMMUTING

CITS employees may be permitted to work remotely at the sole discretion of the Chief Information Officer (CIO) based on need and established guidelines and conditions for such work. Employees must report to office during normal (or assigned) University working hours unless the CIO gives official authorization in advance. In addition, employees authorized to work remotely must report to the office if directed to do so.

If a telecommuting employee’s work performance is not acceptable, the CIO may pursue the disciplinary process or decide to require the employee to work in the University office setting. If the telecommuting employee does not return on the expected date, this will be deemed a voluntary resignation and will be treated as such under University policies and procedures.

An employee must request permission from the CIO to work remotely. The employee making the request must read, complete and sign a detailed policy statement and a Self-Certification Safety Checklist.

Telecommuting employees will not be reimbursed for costs associated with working at home (e.g., electrical, heating and cooling, insurance, security, internet service, etc.) Employees will be permitted to check out University equipment such as computers, printers, etc. to facilitate completion of their work assignment. Equipment checked out for this purpose must be immediately returned at the end of the telecommuting assignment, termination of employment or upon request of the University.

The telecommuting employee is responsible for determining any income tax implications of maintain a home office area. The University will not provide tax guidance nor will the University assume any additional tax liabilities on a telecommuting employee's behalf. Telecommuting employees are encouraged to consult with a qualified tax professional to discuss these implications.