

10.6

Distance and Correspondence Education

An institution that offers distance or correspondence education:

- a. ensures that the student who registers in a distance or correspondence education course or program is the same student who participates in and completes the course or program and receives the credit.
- b. has a written procedure for protecting the privacy of students enrolled in distance and correspondence education courses or programs.
- c. ensures that students are notified, in writing at the time of registration or enrollment, of any projected additional student charges associated with verification of student identity.

Judgment

☒ Compliant ☐ Non-Compliant ☐ Not Applicable

Narrative

Albany State University is in compliance with this principle.

Albany State University (ASU) offers distance education, but the University does not offer correspondence education. Distance education students at ASU include those who take fully online courses through the University and those who complete a required component of courses offered in a traditional face-to-face mode via the learning management system (LMS). Commonly accepted practices for verifying and ensuring the identity of distance learners are followed at ASU. Those involve the use of unique and secure student numbers, user names, and passwords, supplemented as needed by photo identification and proctored examinations. Distance learning students are served through a standardized course management system that routinely informs them of ASU policies for the protection of the privacy of their student identities and secure passwords as well as their responsibilities to ensure academic integrity and honesty in the completion of distance education courses. ASU does not charge a standard fee for the verification of the identity of distance learners. However, the institution does advise distance learners of the fees associated with the course.

Student Verification of Identity

ASU offers distance education and ensures that the student who registers in a distance education course or program is the same student who participates in and completes the course or program and receives the credit. This is done by verifying the identity of a student who participates in class or completes coursework using methods such as (a) a secure login and password, (b) proctored examinations, and new or other technologies and practices that are effective in verifying student identification.

Verification of Student Identification at the Time of Admissions

Student identity verification and identity management begin upon acceptance to ASU as a student. A person who applies to ASU must provide personal information in the application along with documents that are used to verify the applicant's identity and credentials. Admissions staff verify the applicant's identity and credentials as outlined in the Board of Regents (BOR) of the University System of Georgia (USG) policy Section 4.3.4, Verification of Lawful Presence:

Each University System institution shall verify the lawful presence in the United States of every successfully admitted person applying for resident tuition status, as defined in Section 7.3 of this Policy Manual, and of every person admitted to an institution referenced in Section 4.1.6 of this Policy Manual [\[1\]](#).

Within the USG, approved forms of documentation accepted for identification are as follows:

- An approved FAFSA form or other documentation demonstrating eligibility for federal financial aid
- A certified U.S. birth certificate showing the student was born in the U.S. or a U.S. territory (a photocopy is not acceptable)
- A U.S. Certificate of Naturalization (USCIS form N 550 or N 570)
- A U.S. Certificate of Citizenship (USCIS form N 560 or N 561)
- A U.S. Certificate of Birth Abroad issued by the U.S. Department of State (DS 350) or a Consular Report of Birth Abroad (FS-240)
- A current U.S. passport
- A current driver's license issued by the state of Georgia after January 1, 2008 (for in-state tuition)
- A current military ID
- A current, valid Permanent Resident Card (USCIS form I-151 or I-551)
- An F, J, or M verified through the Student and Exchange Visitor Information System (SEVIS)

- Other types of visas verified through the Systematic Alien Verification for Entitlements (SAVE) Program [\[2\]](#)

Secure Login and Password

The ASU assigned number (ASU#), which is unique and different from the student's SSN, and the student's RAMID are permanently associated with the accepted student during the student's association with the University. Because the RAMID is used to access ASU's online resources and services, access is terminated when a student is no longer affiliated with ASU. The ASU# is not reassigned to another student at any time.

The ASU Password Construction Guidelines define the complexity requirements for RAMID passwords and their change frequency. This policy applies equally to students, faculty, and staff and states:

All passwords should meet or exceed the following guidelines. Strong passwords have the following characteristics:

- Contain at least 10 alphanumeric characters.
- Contain characters from at least two of the following four types of characters:

- o English upper case (for example A-Z)
- o English lower case (for example a-z)
- o Contain at least one number (for example, 0-9).
- o Contain at least one special character (for example, !\$%^&*()_+|~-='{}[]:~<>?,/).

- Poor, or weak, passwords have the following characteristics:

- o Contain less than eight characters.
- o Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- o Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- o Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- o Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- o Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
- o Are some version of "Welcome123" "Password123" "Changeme123" [\[3\]](#)

These requirements are enforced via technical mechanisms.

ASU students participating in any mode of online course delivery at the University are required to follow guidelines and procedures set forth by ASU in ASU's Information Technology Services (ITS) Acceptable Use Policy [\[4\]](#). Specific excerpts of that policy pertaining to verification of student identity are stated as follows:

Acceptable Use Policy

Purpose

This policy provides guidelines for the appropriate use of information resources. Use of Albany State University's (ASU) network and computer resources should support the basic missions of the University in teaching, learning and research. Users of the ASU network and computer resources are responsible for proper use, protecting information resources, and respecting the rights of others.

Scope

The policy applies to all ASU students, faculty and staff, and all others using computer and communication technologies whether personally or University owned, which accesses, transmits or stores University or student information.

Policy

General Policy Users of Albany State University's information resources must protect their online identity from use by another individual, the integrity of computer-based information resources, and the privacy of electronic information. In addition, users must refrain from seeking to gain unauthorized access, honor all copyrights and licenses and respect the rights of other information resources.

Access Users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access. Attempts to gain unauthorized access to a system or to another person's information is a violation of University policy and may also violate applicable law, potentially subjecting the user to both civil and criminal liability. However, authorized system administrators may access information resources, but only for a legitimate operational purpose and only the minimum access required to accomplish this legitimate operational purpose.

Sharing ASU User IDs and Passwords Sharing of usernames and passwords used to access ASU information systems is prohibited.

Abuse of Computing Privileges Users of ASU information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the University.

Accountability Violation of this policy may subject the user to sanctions, including the loss of computer and/or network access privileges, disciplinary action, suspension, termination of employment, dismissal from ASU, and/or legal action.

ASU's ITS, in conjunction with the University System of Georgia's (USG) ITS Department, serves as the administrator of ASU's online courses. As such, ITS is responsible for the implementation of the University's secured student verification processes, which are essential to ensure that the student who participates in, completes coursework, and receives credit for an online course is the student of record. Verification of student identification for enrollment takes place at the Registrar level. Once a student is enrolled and assigned courses that are fully online or courses requiring online completion of assignments, ITS ensures and documents the student's access through the following process:

- ITS receives student data and admissions verification via the ASU Banner Web reporting portal.
- A template, which contains fields identifying the student, his/her unique identifier number (RAMID), course name, course number, email address, instructor, and other pertinent information, is downloaded directly from Banner Web.
- The list is forwarded to USG's ITS department for upload into the LMS. (ASU's LMS is hosted on USG's servers. The process for completion of uploads is generally 24 hours for submissions made by 3:00 p.m.).
- Students are automatically loaded into their respective courses. Confirmation of class enrollment is displayed on the front page of each student's homepage. Entrance into the LMS portal requires a secure login and password.
- The login is also a unique student identifier code. The student must enter his/her unique ID and a password reset link is forwarded to the email address associated with the username.
- The combination of the system generated unique ID and the student-created password provides the student access into the LMS environment and courses.
- ITS does not have access to any student or instructor passwords. If a password is lost, a system generated password reset is initiated by the ITS Helpdesk team, or the student may request a password reset by supplying the unique student identifier codes into the LMS.

ASU's Password Protection Standard [5] states:

General

Passwords are a primary means to control access to systems and should therefore be selected, used, and managed to protect against unauthorized discovery or usage. ASU maintains electronic information resources which are essential to performing University business. Similar to any other capital resources owned by the University, these resources are to be viewed as valuable assets over which the University has both rights and obligations to manage, protect, secure, and control. University 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 computer systems, network systems, and data.

Password Creation

All user-level and system-level passwords must conform to the University System of Georgia Information Technology (USGITS) Handbook Section 5.12 [6] and the ASU Password Construction Guidelines Standard. Where possible, users must not use the same password for various ASU access needs. User accounts that have system-level privileges granted through group memberships or programs such as pseudo must have a unique password from all other accounts held by that user to access system-level privileges. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines as defined in USG ITS Handbook Section 5.12.3 [7] and the ASU Password Construction Guidelines Standard.

Password Change

All system-level passwords (for example, root, enable, Active Directory administrators, application administration accounts, and so on) must be changed every ninety (90) days. All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed every one hundred and eighty (180) days. Password cracking or guessing may be performed on a periodic or random basis by the ASU Information Security Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the ASU Password Construction Guidelines.

Password Protection

- All passwords should be treated as sensitive, confidential information. Users should not write passwords down and store them anywhere in their office. Nor should they store passwords in a file on ANY computer system (including Personal Computing Devices or similar devices) without encryption.
- Passwords should not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Users should not share passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Users should not use the "Remember Password" feature of applications (for example, web browsers).
- If an account or password is suspected of being compromised, the incident should be reported to the appropriate access administrator and the user should change the password.
- Users Should Not Employ Any Automatic Log-In Actions
- ASU information system users should refuse all offers by software and/or Internet sites to automatically login the

next time that they access those resources.

- Besides the authorized user, passwords should never be shared or revealed to anyone. Temporary or “first use” passwords should be changed the first time that the authorized user accesses the system. Failure to change a temporary or “first use” password leaves the authorized user liable for all actions performed under the assigned account. If users need to share computer resident data, they should use approved network services or any other mechanisms that do not infringe on any ASU or USGITS standards.

Proctored Exams

Another mechanism used to ensure that the registered student in an online course is the one earning the credit involves the use of proctored exams. Taking a proctored exam requires on-site identity verification with a photo ID.

ASU uses proctors for ensuring the integrity of some online examinations. A proctor ensures the security and integrity of the exam process by requiring the student to present an official form of ID (state-issued drivers’ license, passport, or student ID – all with a picture photo). In some cases, the exams are administered onsite at a location where the student can access the online exams using the Learning Management System (LMS). In this case, the exam location has computers with Internet connections, and the student is required to log into the course with his/her user ID and password at the time of the proctored examination as indicated in ASU’s Academic and Online Support LMS Policy. On occasion, additional security measures are implemented by requiring an IP address location. This mandates that the student take the exam using a specific computer at a designated location. ASU’s online faculty development support staff encourages instructors to use best practices in online assessment and provides guidelines to them for promoting academic integrity [8].

Faculty members are able to use functions within the LMS that allow them to disable pager and right-click functions. Disabling the right click function in the Quiz component of ASU’s LMS (Desire2Learn, also known as D2L) prohibits students from navigating in and out of the LMS to copy, cut or paste information from other sources when taking a quiz. Additionally, disabling the pager function prohibits students from chatting with other individuals, thereby ensuring that answers to test questions cannot be solicited and/or received via chat or instant messaging when taking a quiz.

Technologies within the LMS allow instructors to require students to upload a photograph or other information for additional authentication of student identity. Additionally, recent updates to Banner Web allow instructors to upload students’ photos and align them with students’ names and ID numbers to verify students’ identities.

Guarantee of valid student identity is backed through relevant academic integrity and honesty policies in the Student Code of Conduct and their reinforcement [9]. Student Code of Conduct protections against academic dishonesty apply to all courses, including online. Accusations of misconduct by students such as those related to student identity and use of assigned student identity information are reported to and handled by ASU’s Division of Student Affairs.

Procedures for Protecting Student Privacy

All university policies and procedures regarding the security, confidentiality, and integrity of student records in general apply to students taking distance education courses [10], [11].

Students enrolling in any online course at the University are provided the guidelines and procedures set forth by ASU and supported in the University’s ITS Security Policies [11]. This plan articulates the specific steps the institution employs to protect the privacy of its online student users. Written procedures described in the Security Policy that pertain to the protection of online student privacy are as follows:

- Email policy [12]
- Password Protection Standard [13]
- Security Awareness Training [14]
- Appropriate Use Policy [15]
- Incident Response [16]
- Information-Security Anti-Virus [17]

Access to protected student information is restricted to the teaching faculty member, academic dean, academic chair, or online learning staff who need the information to perform their job duties. All university personnel who are granted access have signed confidentiality and security access agreements on file with Human Resources [18].

A Student Confidentiality statement provided on the homepage of GeorgiaView (GaView), ASU’s online learning platform, informs students that all information provided in GaView is protected [19][20].

Notification of Additional Charges

Students who self-register through the University’s self-service portal are informed to check the Distance Learning website, which includes requirements for proctored examinations [22]. Students who register for distance learning courses are sent an informational email through the University’s email portal four weeks prior to term start informing them of distance learning practices and urging them to check the distance learning website for potential costs, such as proctored experiences, associated with courses [23]. Table 1 depicts the type of fees (proctor, software, web-base e-instruction, and lab) associated with each online course. All student fees, such as technology fees, can be found on the University’s Tuition and Fees website and distance learners are pointed to the ASU Online Tuition and Fees table [24], [25].

Table 1. Online Courses with Additional Fees

Courses	Proctor	Software	Visit Instructor	Web-Based instruction	Field/Lab Experience
Accounting	X	X			
ASU First Year Experience	X				
Biology	X				
Business Administration	X				
Chemistry	X				
College of Arts and Humanities			X		
Communications				X	
Computed Tomography		X			
Computer Processing				X	
Computer Science	X				
Economics	X				
Education					X
English				X	
French	X				
Geology				X	
Health Information	X				
Health and Human Performance	X				
Healthcare Administration				X	
History	X				
Human Services Technology					X
Integrated Science					
Japanese	X				
Mathematics	X				
Medical Laboratory Technology	X				
Nursing Requirements					X
Office Administration & Technology Concentration		X		X	

Organizational Leadership				X	
Philosophy				X	
Physical Science					X
Political Science				X	
Psychology	X				
Spanish	X				
eCore Electronic Technology				X	
eCore Environmental Science				X	

Sources

-  01_BOR_Policy_Manual_Section_4.3.4
-  02_USG_Lawful_Presence
-  03_ASU_Password_Construction_Guidelines
-  04_Acceptable_Use_Policy
-  05_ASU_Password_Protection_Standard
-  06_USGITS_Handbook_5.12
-  07_USGITS_Handbook_5.12.3
-  08_ASU_Online_Course_Policy
-  09_Student_Code_of_Conduct_Academic_Integrity
-  10_Student_Confidentiality
-  11_Information_Security
-  12_ITS_Email_Policy
-  13_ITS_Password_Protection_Standard
-  14_ITS_Information_Security_Awareness_Training_Policy
-  15_ITS_Appropriate_Use_Policy
-  16_ITS_Incident_Response
-  17_ITS_Info-Sec_Anti_Virus
-  18_HR_Confidentiality_Security_Access_Agreement
-  19_GeorgiaView_Student_Confidentiality
-  20_GeorgiaView_Student_Confidentiality_FERPA
-  22_Distance_Learning_Website_Courses
-  23_Distance_Learning_Email_3_Weeks_Communication
-  24_Tuition_Fees_Schedules
-  25_Tuition_Table_Example
-  ASU First Year Experience Foundations of College Success_additional_requirements
-  Accounting_additional_requirements
-  Biology_additional_requirements
-  Business Administration_additional_requirements
-  Chemistry_additional_requirements

-  College of Arts and Humanities_additional_requirements
-  Communications_additional_Documents
-  Computed Tomography_additional_requirements
-  Computer Processing_additional_documents
-  Computer Science_additional_requirements
-  Economics_additional_requirements
-  Education_additional_requirements
-  English_additional_requirements
-  French_additional_requirements
-  Geology_additional_requirements
-  Health Information Technology_additional_requirements
-  Health and Human Performance_additional_requirements
-  Healthcare Administration_additional_requirements
-  History_additional_requirements
-  Human Services Technology_additional_requirements
-  Intergated Earth Sciences
-  Japanese_additional_requirements
-  Mathematics_additional_requirements
-  Medical Laboratory Technology_additional_requirements
-  Nursing_additional_requirements
-  Office Administration & Technology Concentration_additional_requirements
-  Organizational Leadership_additional_requirements
-  Philosophy_additional_requirements
-  Physical Science_additional_requirements
-  Political Science_additional_requirements
-  Psychology_additional_requirements
-  Spanish_additional_requirements
-  eCore Electronic Technology in the Educational Environment_additional_requirements
-  eCore Environmental Science_additional_requirements
-  integrated science

This Page Intentionally Left Blank

The following pages contain Supporting Documentation



ABOUT USG

OUR INSTITUTIONS

STUDENTS

NEWS & REPORTS

INITIATIVES & PRIORITIES

4.3.4 Verification of Lawful Presence

Each University System institution shall verify the lawful presence in the United States of every successfully admitted person applying for resident tuition status, as defined in [Section 7.3](#) of this Policy Manual, and of every person admitted to an institution referenced in [Section 4.1.6](#) of this Policy Manual.



CONTACT
270 Washington Street, S.W.
Atlanta, GA 30334
U.S.A.

WEBSITE INFORMATION
Privacy Policy
Accessibility
Compliance & Ethics Reporting

USG INSTITUTIONS
Map & Information
Institutional Directories

INFORMATION FOR:
Current Students
Prospective Students
International Students
Online Students
Veterans and Service Members
Faculty and Staff
USG Retiree Benefits
Vendors & Suppliers

POLICIES & REPORTS
University System of Georgia Policies

NEED HELP?
Human Trafficking Notice

DIVISIONS
Academic Affairs
Administration
Economic Development
Internal Audit
Strategy & Fiscal Affairs

ABOUT
University System of Georgia
Board of Regents
Chancellor
Campus Consolidations
Comprehensive Administrative Review
Newsroom
Employment

Briefing

Article Posted July 13, 2012



Verifying Eligibility for In-State Student Tuition (Lawful Presence)

The OIAC recently began an system-wide review of the implementation of BOR Policy Manual:

- § 4.1.6 – “Admission of Persons Not Lawfully Present in the United States”, and;
- § 4.3.4 – “Verification of Lawful Presence”

The review is designed to determine the level of compliance at each Institution with the requirements of these policies. The review will verify:

a)if students who receive in-state tuition are appropriately verified as eligible to receive in-state tuition rates because they are legal citizens established through citizenship, naturalization or permanent residency, and;

b)if ineligible students were enrolled at institutions that denied admission to all academically qualified applicant during the previous two academic years.

In addition to the requirements described by the BOR Policy Manual, institutions are required to include the following on all application forms:

- Language describing the penalties for false swearing as defined by O.C.G.A. § 16-10-71; and,
- An opportunity for the applicant to declare the eligibility or ineligibility for in-state tuition.

The specific language necessary to satisfy these requirements can be found on the USG Office of Student Affairs Web site.

While BOR Policy Manual § 4.1.6 is currently applicable to only five USG institutions, the criteria that governs this policy is relevant to all USG institutions. Institutions are held accountable for reviewing their admissions activity to ensure that their classification has not changed. Institutions seeking to change their admission classification status must send a letter of intent to the Office of Student Affairs prior to adopting the selective admission process. If approved, the institution will receive notification and instructions for implementation.

Beginning with the Fall 2011 term, USG institutions were required to verify the lawful presence of any student claiming eligibility for in-state tuition and who was enrolled for the first time at a USG institution. Per BOR policy, a student's eligibility for in-state tuition must be verified before that student is designated as eligible. The following forms of documentation have been approved as sources to verify a student's eligibility for in-state tuition:

- An approved FAFSA form or other documentation demonstrating eligibility for federal financial aid
- A Certified U.S. Birth Certificate showing the student was born in the U.S. or a U.S. territory (a photocopy is not acceptable)
- A U.S. Certificate of Naturalization (USCIS form N-550 or N-570)
- A U.S. Certificate of Citizenship (USCIS form N-560 or N-561)
- A U.S. Certificate of Birth Abroad issued by the Department of State (DS-350) or a Consular Report of Birth Abroad (FS-240)
- A current U.S. Passport
- A current Driver's License issued by the State of Georgia after January 1, 2008
- A current ID issued by the State of Georgia after January 1, 2008
- A current military ID (service member only, not dependent)
- A current, valid Permanent Resident Card (USCIS form I-151 or I-551)
- An F, J, or M visa
- Verification through the SAVE program

Institutions should carefully review the processes used to demonstrate a student's eligibility including FAFSA forms.

Posted by Ted Beck

Published in: [Policy Briefs](#)

HOME (HTTPS://WWW.ASURAMS.EDU/) > INFORMATION TECHNOLOGY SERVICES HOME (HTTPS://WWW.ASURAMS.EDU/TECHNOLOGY/)
> FORMS & POLICIES (HTTPS://WWW.ASURAMS.EDU/TECHNOLOGY/FORMS-POLICIES/) > PASSWORD CONSTRUCTION GUIDELINES

Password Construction Guidelines

Contents

- Purpose
- Scope
- General
- Statement of Guidelines
- You should never write down a password
- Passphrases
- Compliance
- Contacts
- References
- Version History

PURPOSE

The purpose of this guidelines is to provide best practices for the created of strong passwords.

SCOPE

This guideline applies to employees, contractors, consultants, temporary and other workers at Albany State University, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limited to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

GENERAL

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or the Albany State University network. This guideline provides best practices for creating secure passwords.

STATEMENT OF GUIDELINE

All passwords should meet or exceed the following guidelines. Strong passwords have the following characteristics:

- Contain at least 10 alphanumeric characters.
- Contain characters from at least two of the following four types of characters:.

- English upper case (for example A-Z)
- English lower case (for example a-z)
- Contain at least one number (for example, 0-9).
- Contain at least one special character (for example, !\$%^&*()_+|~-='{}[]:"';<>?,./).
- Poor, or weak, passwords have the following characteristics:
 - Contain less than eight characters.
 - Can be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
 - Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
 - Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
 - Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
 - Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
 - Are some version of "Welcome123" "Password123" "Changeme123"

YOU SHOULD NEVER WRITE DOWN A PASSWORD

Instead, try to create passwords that you can remember easily. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase, "This May Be One Way To Remember" could become the password TmB1w2R! or another variation.

PASSPHRASE'S

Passphrase's generally are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to unlock the private key, the user cannot gain access. A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrase should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*!\$ThisMorning!).

COMPLIANCE

- Compliance Measurement - The Information Security Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thru, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.
- Exceptions - Any exception to the policy must be approved by the Information Security Team in advance.
- Non-Compliance - An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

CONTACTS

The Chief Information Officer is charged with the responsibility to periodically review the policy and propose changes as needed.

REFERENCES

- ASU IT Security Website: <https://www.asurams.edu/technology/information-security/> ([/technology/information-security/index.php](https://www.asurams.edu/technology/information-security/index.php))
- USGBOR Handbook: http://www.usg.edu/information_technology_handbook/section5
(http://www.usg.edu/information_technology_handbook/section5)
- National Institute for Standards and Technology: <http://www.nist.gov> (<http://www.nist.gov>)
- SANS Institute: <http://www.sans.org> (<http://www.sans.org>)
- COBIT 5.0: <http://www.isaca.org/> (<http://www.isaca.org>)

VERSION HISTORY

Date	Version	Description
------	---------	-------------

- [Getting Started for Employees \(/technology/getting-started-employees/index.php\)](/technology/getting-started-employees/index.php)
- [Getting Started for Students \(/technology/getting-started-students/index.php\)](/technology/getting-started-students/index.php)
- [Personnel \(/technology/personnel.php\)](/technology/personnel.php)
- [Project Management Office \(/technology/pmo/index.php\)](/technology/pmo/index.php)
- [Accessing Campus WiFi \(/technology/accessing-campus-wifi.php\)](/technology/accessing-campus-wifi.php)
- [Enterprise Reports – Argos \(/technology/argos.php\)](/technology/argos.php)
- [Banner Student Information System \(/technology/banner-student-information-system.php\)](/technology/banner-student-information-system.php)
- [Card Services \(/technology/card-services/index.php\)](/technology/card-services/index.php)
- [Forms & Policies \(/technology/forms-policies/index.php\)](/technology/forms-policies/index.php)
 - [Info-Sec Anti-Virus \(/technology/forms-policies/info-sec-anti-virus.php\)](/technology/forms-policies/info-sec-anti-virus.php)
 - [Information Security Awareness Training Policy \(/technology/forms-policies/information-security-awareness-training-policy.php\)](/technology/forms-policies/information-security-awareness-training-policy.php)
 - [ITS Appropriate Use Policy \(/technology/forms-policies/its-appropriate-use-policy.php\)](/technology/forms-policies/its-appropriate-use-policy.php)
 - [ITS Email Policy \(/technology/forms-policies/its-email-policy.php\)](/technology/forms-policies/its-email-policy.php)
 - [ITS Incident Response \(/technology/forms-policies/its-incident-response.php\)](/technology/forms-policies/its-incident-response.php)
 - [ITS VPN Remote Access Policy \(/technology/forms-policies/its-vpn-remote-access-policy.php\)](/technology/forms-policies/its-vpn-remote-access-policy.php)
 - [Password Construction Guidelines \(/technology/forms-policies/password-construction-guidelines.php\)](/technology/forms-policies/password-construction-guidelines.php)
 - [Password Protection Standard \(/technology/forms-policies/password-protection-standard.php\)](/technology/forms-policies/password-protection-standard.php)
 - [ASK ITS Question Form \(/technology/forms-policies/ask-its-form.php\)](/technology/forms-policies/ask-its-form.php)
- [General Use Computer Labs \(/technology/general-use-computer-labs.php\)](/technology/general-use-computer-labs.php)
- [Help Desk \(/technology/helpdesk/index.php\)](/technology/helpdesk/index.php)
- [Information Security \(/technology/information-security/index.php\)](/technology/information-security/index.php)
- [IT Service Catalog \(https://helpdesk.asurams.edu/catalog_items.portal\)](https://helpdesk.asurams.edu/catalog_items.portal)
- [VP of Information Technology Services and CIO \(/technology/office-vpcio.php\)](/technology/office-vpcio.php)
- [New Department Fax Numbers \(/technology/newfaxnumbers.php\)](/technology/newfaxnumbers.php)
- [New Department Phone Numbers \(/technology/newphonenumber.php\)](/technology/newphonenumber.php)

ASU West Campus

2400 Gillionville Rd

Albany, GA 31707

Phone: (229) 500-2000 (tel:2295002000)



(<http://www.albanystate.edu>)

- **Accreditation** (</academic-affairs/accreditation.php>)
- **ASU Careers** (<https://www.albanystatejobs.com/>)
- **Maps** (</asu-campus-map/index.php>)
- **Students** (</student-affairs/index.php>)
- **Campus Safety** (</fiscal-affairs/police/index.php>)
- **ASU Foundation** (</institutional-advancement/asu-foundation/index.php>)
- **Events Calendar** (</academic-affairs/calendars/index.php>)
- **Flickr Photos** (<https://www.flickr.com/photos/albanystateuniversity/>)
- **Request a Transcript** (/enrollment-management/office_of_the_registrar/transcript-information.php)
- **ASU IT Help Desk** (</technology/helpdesk/index.php>)
- **Equal Employment Opportunity** (</human-resources/equal-employment-opportunity.php>)
- **Ethics & Compliance Hotline** (</internal-audit/hotline-reporting.php>)
- **Human Trafficking Notice** (<https://gbi.georgia.gov/documents/human-trafficking-notice>)

Copyright © (<http://a.cms.omniupdate.com/10?skin=oucampus&account=asurams&site=www&action=de&path=/technology/forms-policies/password-construction-guidelines.pcf>) 2018 Albany State University All Rights Reserved.

Albany State University is committed to principles of equal opportunity and affirmative action.



University Policy Acceptable Use Policy

Purpose

This policy provides guidelines for the appropriate use of information resources. Use of Albany State University's (ASU) network and computer resources should support the basic missions of the University in teaching, learning and research. Users of the ASU network and computer resources are responsible for proper use, protecting information resources, and respecting the rights of others.

Scope

The policy applies to all ASU students, faculty and staff, and all others using computer and communication technologies whether personally or University owned, which accesses, transmits or stores University or student information.

Policy

- **General Policy** Users of Albany State University's information resources must protect their online identity from use by another individual, the integrity of computer-based information resources, and the privacy of electronic information. In addition, users must refrain from seeking to gain unauthorized access, honor all copyrights and licenses and respect the rights of other information resources.
- **Access** Users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access. Attempts to gain unauthorized access to a system or to another person's information is a violation of University policy and may also violate applicable law, potentially subjecting the user to both civil and criminal liability. However, authorized system administrators may access information resources, but only for a legitimate operational purpose and only the minimum access required to accomplish this legitimate operational purpose.
 - **Sharing ASU User IDs and Passwords;** Sharing of usernames and passwords used to access ASU information systems is prohibited.
 - **Information Belonging to Others;** Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, passwords or other digital materials belonging to other users, without the specific permission of those other users.
 - **Abuse of Computing Privileges;** Users of ASU information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the University.
- **Usage** Use of the University's information resources must comply with ASU policies and legal obligations (including licenses and contracts) and all federal and state laws.

- **Prohibited Use** Users must not send, view or download fraudulent, harassing, obscene (i.e., sexually explicit), threatening, or other messages or material that are a violation of applicable law or University policy. In particular, contributing to the creation of a hostile academic or work environment is prohibited.
- **Copyrights and Licenses** Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file-sharing using the University's information resources is a violation of this policy.
- **Social Media** Users must respect the purpose of and abide by the terms of use of online media forums, including social networking websites, mailing lists, chat rooms and blogs.
- **Political Use** University information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws, and may be used for other political activities only when in compliance with federal, state and other laws and in compliance with applicable University policies.
- **Personal Use** University information resources should not be used for activities unrelated to appropriate University functions, except in a purely incidental manner.
- **Use of University Information** Users must abide by applicable data storage and transmission policies.
- **Integrity of Information Resources** Users must respect the integrity of information and information resources.
- **Modification or Removal of Information or Information Resources Without proper authorization** Users must not attempt to modify or remove information or information resources that are owned or used by others.
- **Other Prohibited Activities** Users must not encroach, disrupt or otherwise interfere with access or use of the University's information or information resources. For the avoidance of doubt, without express permission, users must not give away University information or send bulk unsolicited email. In addition, users must not engage in other activities that damage, vandalize or otherwise compromise the integrity of University information or information resources.
- **Academic Pursuits** The University recognizes the value of legitimate research projects undertaken by faculty and students under faculty supervision. The University may restrict such activities in order to protect University and individual information and information resources, but in doing so will take into account legitimate academic pursuits.
- **Access for Legal and University Processes** Under some circumstances, as a result of investigations, subpoenas or lawsuits, the University may be required by law to provide electronic or other records, or information related to those records or relating to use of information resources, ("information records") to third parties. Additionally, the University may in its reasonable discretion review information records, e.g., for the proper functioning of the University, in connection with investigations, or to protect the safety of individuals or the ASU community. The University may also permit reasonable access to data to third-party service providers in order to provide, maintain or improve services to the University. Accordingly, users of University information resources do not have a reasonable expectation of privacy when using the University's information resources.

Definitions (Optional)

Definitions associated with this policy are available in the Information Technology and Data Security Terms Glossary.

Accountability

Violation of this policy may subject the user to sanctions, including the loss of computer and/or network access privileges, disciplinary action, suspension, termination of employment, dismissal from ASU, and/or legal action.

Contacts

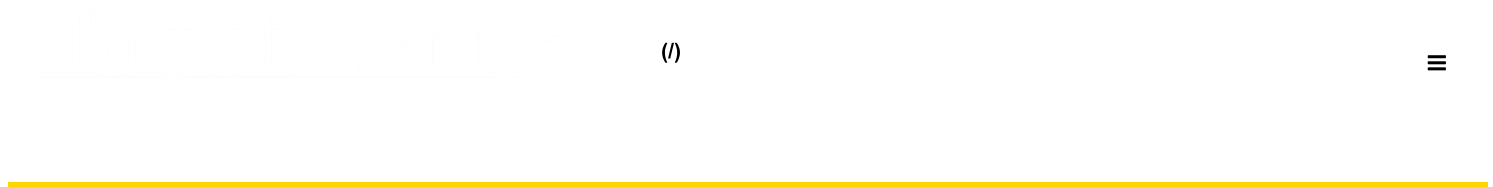
- Albany State University Chief Information Officer
- Albany State University Chief Information Security Officer

References

USG BOR IT Handbook, http://www.usg.edu/information_technology_handbook/section5

Last Update

July 31, 2018



Password Protection Standard

Contents

- Purpose
- Scope
- Standard
 - General
 - Password Creation
 - Password Change
 - Administrative Accounts
 - Server Administrator Passwords
 - Password Resets
 - Authority, Enforcement, Exceptions
- Standard Compliance
- Accountability
- Contacts
- References
- Version History

PURPOSE

The purpose of this document is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

SCOPE

This Standard applies to all individuals associated with Albany State University (hereinafter referred to “ASU”), including faculty, staff, student assistants, and contractors. This Standard applies to anyone accessing or utilizing ASU’s network or data. This use may include, but is not limited to, the following: personal computers, laptops, ASU-issued cell phones, and hand-held computing devices (e.g., iPad’s, Xyboards, USB memory keys, etc.), as well as ASU electronic services, systems and servers. This Standard covers departmental resources as well as resources managed centrally.

STANDARD

General

Passwords are a primary means to control access to systems and should therefore be selected, used, and managed to protect against unauthorized discovery or usage. ASU maintains electronic information resources which are essential to performing University business. Similar to any other capital resources owned by the University, these resources are to be viewed as valuable assets over which the University has both rights and obligations to manage, protect, secure, and control. University 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 computer systems, network systems, and data.

Password Creation

All user-level and system-level passwords must conform to the **University System of Georgia Information Technology (USGITS) Handbook Section 5.12** (http://www.usg.edu/information_technology_handbook/section5/C2267) and the ASU Password Construction Guidelines Standard. Where possible, users must not use the same password for various ASU access needs. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines as defined in USG ITS Handbook Section 5.12 and the ASU Password Construction Guidelines Standard

Password Change

All system-level passwords (for example, root, enable, Active Directory administrators, application administration accounts, and so on) must be changed every ninety (90) days. All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed every one hundred and eighty (180) days. Password cracking or guessing may be performed on a periodic or random basis by the ASU Information Security Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the ASU Password Construction Guidelines.

Password Protection

- All passwords should be treated as sensitive, confidential information. Users should not write passwords down and store them anywhere in their office. Nor should they store passwords in a file on ANY computer system (including Personal Computing Devices or similar devices) without encryption.
- Passwords should not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Users should not share passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Users should not use the "Remember Password" feature of applications (for example, web browsers).
- If an account or password is suspected of being compromised, the incident should be reported to the appropriate access administrator and the user should change the password.
- Users Should Not Employ Any Automatic Log-In Actions
- ASU information system users should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
- Besides the authorized user, passwords should never be shared or revealed to anyone. Temporary or "first use" passwords should be changed the first time that the authorized user accesses the system. Failure to change a temporary or "first use" password leaves the authorized user liable for all actions performed under the assigned account. If users need to share computer resident data, they should use approved network services or any other mechanisms that do not infringe on any ASU or USGITS standards.

Application Development

Application developers must ensure that their programs contain the following security precautions:

- Applications must support authentication of individual users, not groups.
- Applications must not store passwords in clear text or in any easily reversible form.
- Applications must not transmit passwords in clear text over the network.

- Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

STANDARD COMPLIANCE

Compliance Measurement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, periodic walk through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Information Technology Services will, whenever reasonably possible, configure accounts for automatic password expiration and set other options to encourage or remind individuals to change their passwords.

Exceptions

Exceptions must be justified in writing and accepted by the CISO of Albany State University or his/her designee. In the case of an information system managed by a third party, the University CISO can, in concurrence with the information owner, make a determination that the third party's security controls meet or exceed this standard. This exception must be based on an assessment of the third party's controls and documented in writing.

Non-Compliance

Violations of this Standard may be referred to appropriate administrative offices for disciplinary action. Violators may be subject to disciplinary outcomes as outlined in the Student Handbook and/or Employee Handbook. In addition to the other sanctions outlined in the handbooks, improper use of administrative accounts may result in immediate suspension and loss of privileges.

CONTACTS

The Chief Information Officer is charged with the responsibility to periodically review the policy and propose changes as needed.

REFERENCES

- ASU IT Security Website: <https://www.asurams.edu/technology/information-security/> ([/technology/information-security/index.php](https://www.asurams.edu/technology/information-security/index.php))
- USGBOR Handbook: http://www.usg.edu/information_technology_handbook/section5 (http://www.usg.edu/information_technology_handbook/section5)
- National Institute for Standards and Technology: <http://www.nist.gov> (<http://www.nist.gov>)
- SANS Institute: <http://www.sans.org> (<http://www.sans.org>)
- COBIT 5.0: <http://www.isaca.org/> (<http://www.isaca.org>)

VERSION HISTORY

Date	Version	Description
June 2007	1.0	ASU ITS
October 9, 2013	1.3	ASU Information Technology Governance Committee
June 2015	2.0	Major re-write by Information Security Team

► [Getting Started for Employees \(/technology/getting-started-employees/index.php\)](/technology/getting-started-employees/index.php)

► [Getting Started for Students \(/technology/getting-started-students/index.php\)](/technology/getting-started-students/index.php)

► [Personnel \(/technology/personnel.php\)](/technology/personnel.php)

► [Project Management Office \(/technology/pmo/index.php\)](/technology/pmo/index.php)

► [Accessing Campus WiFi \(/technology/accessing-campus-wifi.php\)](/technology/accessing-campus-wifi.php)

► [Enterprise Reports – Argos \(/technology/argos.php\)](/technology/argos.php)

- ▶ [Banner Student Information System \(/technology/banner-student-information-system.php\)](/technology/banner-student-information-system.php)
- ▶ [Card Services \(/technology/card-services/index.php\)](/technology/card-services/index.php)
- ▶ [Forms & Policies \(/technology/forms-policies/index.php\)](/technology/forms-policies/index.php)
 - ▶ [Info-Sec Anti-Virus \(/technology/forms-policies/info-sec-anti-virus.php\)](/technology/forms-policies/info-sec-anti-virus.php)
 - ▶ [Information Security Awareness Training Policy \(/technology/forms-policies/information-security-awareness-training-policy.php\)](/technology/forms-policies/information-security-awareness-training-policy.php)
 - ▶ [ITS Appropriate Use Policy \(/technology/forms-policies/its-appropriate-use-policy.php\)](/technology/forms-policies/its-appropriate-use-policy.php)
 - ▶ [ITS Email Policy \(/technology/forms-policies/its-email-policy.php\)](/technology/forms-policies/its-email-policy.php)
 - ▶ [ITS Incident Response \(/technology/forms-policies/its-incident-response.php\)](/technology/forms-policies/its-incident-response.php)
 - ▶ [ITS VPN Remote Access Policy \(/technology/forms-policies/its-vpn-remote-access-policy.php\)](/technology/forms-policies/its-vpn-remote-access-policy.php)
 - ▶ [Password Construction Guidelines \(/technology/forms-policies/password-construction-guidelines.php\)](/technology/forms-policies/password-construction-guidelines.php)
 - ▶ [Password Protection Standard \(/technology/forms-policies/password-protection-standard.php\)](/technology/forms-policies/password-protection-standard.php)
 - ▶ [ASK ITS Question Form \(/technology/forms-policies/ask-its-form.php\)](/technology/forms-policies/ask-its-form.php)
- ▶ [General Use Computer Labs \(/technology/general-use-computer-labs.php\)](/technology/general-use-computer-labs.php)
- ▶ [Help Desk \(/technology/helpdesk/index.php\)](/technology/helpdesk/index.php)
- ▶ [Information Security \(/technology/information-security/index.php\)](/technology/information-security/index.php)
- ▶ [IT Service Catalog \(https://helpdesk.asurams.edu/catalog_items.portal\)](https://helpdesk.asurams.edu/catalog_items.portal)
- ▶ [VP of Information Technology Services and CIO \(/technology/office-vpcio.php\)](/technology/office-vpcio.php)
- ▶ [New Department Fax Numbers \(/technology/newfaxnumbers.php\)](/technology/newfaxnumbers.php)
- ▶ [New Department Phone Numbers \(/technology/newphonenumber.php\)](/technology/newphonenumber.php)

ASU East Campus

504 College Drive
Albany, GA 31705

ASU West Campus

2400 Gillionville Rd
Albany, GA 31707

Phone: (229) 500-2000 (tel:2295002000)



(<https://www.facebook.com/AlbanyStateUniv>)

- [Accreditation \(/academic-affairs/accreditation.php\)](/academic-affairs/accreditation.php)
- [ASU Careers \(https://www.albanystatejobs.com/\)](https://www.albanystatejobs.com/)
- [Maps \(/asu-campus-map/index.php\)](/asu-campus-map/index.php)
- [Students \(/student-affairs/index.php\)](/student-affairs/index.php)

- **Campus Safety** (</fiscal-affairs/police/index.php>)
- **ASU Foundation** (</institutional-advancement/asu-foundation/index.php>)
- **Events Calendar** (</academic-affairs/calendars/index.php>)
- **Flickr Photos** (<https://www.flickr.com/photos/albanystateuniversity/>)
- **Request a Transcript** (/enrollment-management/office_of_the_registrar/transcript-information.php)
- **ASU IT Help Desk** (</technology/helpdesk/index.php>)
- **Equal Employment Opportunity** (</human-resources/equal-employment-opportunity.php>)
- **Ethics & Compliance Hotline** (</internal-audit/hotline-reporting.php>)
- **Human Trafficking Notice** (<https://gbi.georgia.gov/documents/human-trafficking-notice>)

Copyright © (<http://a.cms.omniupdate.com/10?skin=oucampus&account=asurams&site=www&action=de&path=/technology/forms-policies/password-protection-standard.pcf>) 2018 Albany State University All Rights Reserved.

Albany State University is committed to principles of equal opportunity and affirmative action.

5.11.4 Passwords

USG electronic communications systems or services must identify users and authenticate and authorize access by means of user ID, passwords, or other secure authentication processes (e.g. biometrics or Smart Cards). Password length and strength must meet the Section 5.12 Password Security. In addition, shared-access systems must enforce these standards whenever possible and appropriate and require that users change any pre-assigned passwords immediately upon initial access to the account. All default passwords for access to network accessible devices must be modified. Passwords used by system administrators for their personal access to a service or device must not be the same as those used for privileged access to any service or device.

5.11.5 Encrypted Authentication

Unencrypted device authentication mechanisms are only as secure as the network upon which they are used. Traffic across the USG network may be surreptitiously monitored, rendering these authentication mechanisms vulnerable to compromise. Therefore, all networked devices must use only encrypted authentication mechanisms unless otherwise authorized by USG Cybersecurity. In particular, historically insecure services such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.

Encryption, or equally effective measures, is required for all personal, sensitive, or confidential information, as defined in Section 5.7, that is stored on portable electronic storage media (including, but not limited to, CDs/DVDs, external/mobile storage and USB drives) and on portable computing devices (including, but not limited to laptop and notebook computers). This policy does not apply to mainframe and server tapes.

5.11.6 Physical Security

Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, devices must be configured to lock and require a user to re-authenticate if left unattended for more than twenty (20) minutes.

5.11.7 Unnecessary Services

A service(s) not necessary for the intended purpose or operation of the device shall not be running.

5.12 Password Security

5.12.1 User Access Controls

USG organizations must establish policies and procedures that ensure necessary user access controls are in place for controlling the actions, functions, applications, and operations of legitimate users. The aim is to protect the confidentiality, integrity, and availability of all USG information resources.

The guiding principles in developing these standards and procedures are:

1. Users will have access to the resources needed to accomplish their duties.
2. User access applies the principles of least privilege and resource categorization as necessary tools to achieve the desired purpose.
3. User access controls will balance security and USG mission needs.

All users, whether internal, external, or temporary, and their activity on all IT systems should be uniquely identifiable. User identification should be enabled through appropriate authentication mechanisms. User access rights to all systems and data must be in line with defined and documented business needs, and job requirements must be attached to user identification. User access rights should be requested by user management, approved by system owners, and implemented by the appropriate local security administrator. User identification and access rights should be maintained in a central repository. Each USG organization should deploy cost-effective technical and procedural measures to establish user identification, implement authentication, and enforce access rights. These measures should be reviewed periodically and kept current.

5.12.2 USG Password Authentication Standard

Purpose

Passwords are an important aspect of information and information technology security. They are often the only means for authenticating users and the front line of protection for user accounts. Failure to use a strong password or using a poorly chosen password when accessing USG information assets may result in the compromise of those assets. It is the responsibility of every USG organization to implement authentication mechanisms such as passwords to access sensitive data, and the responsibility of the user to appropriately select and protect their passwords.

Scope

This security standard applies to USG organizations. This standard also applies to all users (employees, contractors, vendors, and other parties) of USG and state information technology systems or data are expected to understand and abide by the standard.

Standard

Passwords shall be the minimum acceptable mechanism for authenticating users and controlling access to USG organizations' information systems, services and applications unless specifically designated as a public access resource.

All users (students, employees, contractors, and vendors) with access to USG information and information systems shall take the appropriate steps to select and secure their passwords.

Enforcement

Individual USG organizations are responsible for developing internal procedures to facilitate compliance with these USG security policies and standards. The standards are designed to comply with applicable laws and regulations. However, if there is a conflict, applicable laws and regulations will take precedence.

USG organizations may establish more stringent policies, standards and procedures consistent with this USG standard.

Violations of this standard could result in serious security incidents involving sensitive state, federal, sensitive or privacy data. Violators may be subject to disciplinary actions including termination and/or criminal prosecution.

The standards will guide periodic security reviews, as well as audits by USG Internal Audit & Compliance and the state Department of Audits and Accounts (DOAA).

5.12.3 USG Password Security and Composition Requirement

Purpose

This section establishes a standard for protecting passwords and the frequency of change for such passwords to mitigate compromise of sensitive information.

Scope

This security standard applies to all USG organizations. This standard also applies to all USG users, including employees, contractors, vendors, and other parties.

Guidelines

1. All passwords shall be treated as sensitive, confidential information and shall not be shared with anyone including, but not limited to, administrative assistants, system administrators and helpdesk personnel.
2. Passwords shall not be stored in clear text.
3. Users shall not write passwords down or store them anywhere in their office or publically. They shall not store passwords in a file on any computer system, including smart devices, without encryption.
4. Refresh shall:
 - a. Administrative-level passwords shall be changed every ninety (90) days.
 - b. User-level passwords shall be changed every one hundred eighty (180) days.
 - c. System-level (system-to-system or non-interactive services account) passwords shall be changed after a significant event (i.e. administrator departure, suspicion or actual compromise event.)
5. User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from other accounts held by that user.
6. Passwords shall not be inserted into email messages or other forms of electronic communication unless encrypted.
7. If an account or password is suspected of being compromised, the incident must be reported to the appropriate authorities in accordance with local incident response procedures.
8. Temporary or "first use" passwords (e.g., new accounts or guests) must be changed the first time the authorized user accesses the system, and have a limited life of inactivity before being disabled.
9. Access to all USG information systems and applications used to process, store, or transfer data with a security categorization of MODERATE or higher, as defined in Section 5.6.3 of this Manual, shall require the use of strong passwords or other strong authentication mechanisms. Strong passwords shall be constructed with the following characteristics:
 - Be at least ten characters in length
 - Must contain characters from at least two of the following four types of characters:
 - English upper case (A-Z)

- English lower case (a-z)
 - Numbers (0-9)
 - Non-alphanumeric special characters (\$, %, ^, ...)
 - Must not contain the user's name or part of the user's name
 - Must not contain easily accessible or guessable personal information about the user or user's family, such as birthdays, children's names, addresses, etc.
 - Note 1: A six-character password is acceptable if "account lockout" is enabled and set to lock or disable the account after five unsuccessful or failed login attempts. Six-character passwords must adhere to all of the characteristics noted above.
 - Note 2: Organizations may mix different characteristics regarding length and mandatory characters to obtain the same password strength. For example, a password of 11 characters containing two upper case letters, two lower case letters, two numbers, and no special characters would be permissible.
10. Password history must be enabled and configured to disallow usage of the same password for a set length of change cycles greater than four (4) times. Users and administrators must not be allowed to use the same password that has been used in the past four (4) changes. Users and administrators who have changed their user password or system password must not be allowed to change passwords immediately. This will prevent users and administrators from changing their passwords several times to get back to their old passwords.

Enforcement

Individual USG organizations are responsible for developing internal procedures to facilitate compliance with these USG security policies and standards. The standards are designed to comply with applicable laws and regulations; however, if there is a conflict, applicable laws and regulations will take precedence.

USG organizations may establish more stringent policies, standards and procedures consistent with this USG standard.

Violations of this standard could result in serious security incidents involving sensitive state, federal, sensitive or privacy data. Violators may be subject to disciplinary actions including termination and/or criminal prosecution.

The standards will guide periodic security reviews, as well as audits by USG Internal Audit & Compliance and the state Department of Audits and Accounts (DOAA).

Section 5.13 Domain Name System

Guidelines for interpretation and administration of domain name security are provided in Domain Name System (DNS) Management.

5.13.1 Domain Name System (DNS) Management

Purpose

5.12.3 USG Password Security and Composition Requirement

Purpose

This section establishes a standard for protecting passwords and the frequency of change for such passwords to mitigate compromise of sensitive information.

Scope

This security standard applies to all USG organizations. This standard also applies to all USG users, including employees, contractors, vendors, and other parties.

Guidelines

1. All passwords shall be treated as sensitive, confidential information and shall not be shared with anyone including, but not limited to, administrative assistants, system administrators and helpdesk personnel.
2. Passwords shall not be stored in clear text.
3. Users shall not write passwords down or store them anywhere in their office or publically. They shall not store passwords in a file on any computer system, including smart devices, without encryption.
4. Refresh shall:
 - a. Administrative-level passwords shall be changed every ninety (90) days.
 - b. User-level passwords shall be changed every one hundred eighty (180) days.
 - c. System-level (system-to-system or non-interactive services account) passwords shall be changed after a significant event (i.e. administrator departure, suspicion or actual compromise event.)
5. User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from other accounts held by that user.
6. Passwords shall not be inserted into email messages or other forms of electronic communication unless encrypted.
7. If an account or password is suspected of being compromised, the incident must be reported to the appropriate authorities in accordance with local incident response procedures.
8. Temporary or “first use” passwords (e.g., new accounts or guests) must be changed the first time the authorized user accesses the system, and have a limited life of inactivity before being disabled.
9. Access to all USG information systems and applications used to process, store, or transfer data with a security categorization of MODERATE or higher, as defined in Section 5.6.3 of this Manual, shall require the use of strong passwords or other strong authentication mechanisms. Strong passwords shall be constructed with the following characteristics:
 - Be at least ten characters in length
 - Must contain characters from at least two of the following four types of characters:
 - English upper case (A-Z)

- English lower case (a-z)
 - Numbers (0-9)
 - Non-alphanumeric special characters (\$, %, ^, ...)
 - Must not contain the user's name or part of the user's name
 - Must not contain easily accessible or guessable personal information about the user or user's family, such as birthdays, children's names, addresses, etc.
 - Note 1: A six-character password is acceptable if "account lockout" is enabled and set to lock or disable the account after five unsuccessful or failed login attempts. Six-character passwords must adhere to all of the characteristics noted above.
 - Note 2: Organizations may mix different characteristics regarding length and mandatory characters to obtain the same password strength. For example, a password of 11 characters containing two upper case letters, two lower case letters, two numbers, and no special characters would be permissible.
10. Password history must be enabled and configured to disallow usage of the same password for a set length of change cycles greater than four (4) times. Users and administrators must not be allowed to use the same password that has been used in the past four (4) changes. Users and administrators who have changed their user password or system password must not be allowed to change passwords immediately. This will prevent users and administrators from changing their passwords several times to get back to their old passwords.

Enforcement

Individual USG organizations are responsible for developing internal procedures to facilitate compliance with these USG security policies and standards. The standards are designed to comply with applicable laws and regulations; however, if there is a conflict, applicable laws and regulations will take precedence.

USG organizations may establish more stringent policies, standards and procedures consistent with this USG standard.

Violations of this standard could result in serious security incidents involving sensitive state, federal, sensitive or privacy data. Violators may be subject to disciplinary actions including termination and/or criminal prosecution.

The standards will guide periodic security reviews, as well as audits by USG Internal Audit & Compliance and the state Department of Audits and Accounts (DOAA).

Section 5.13 Domain Name System

Guidelines for interpretation and administration of domain name security are provided in Domain Name System (DNS) Management.

5.13.1 Domain Name System (DNS) Management

Purpose

Section Name, Section Number, Policy Number

Introduction

Offering online, partially online, and hybrid course offerings in addition to traditional face-to-face options is one way in which Albany State University strives to implement and achieve the goal of “offering flexible class times and instructional modalities” as indicated in ASU’s Guiding Principle to “Expand Access to Higher Education.”

Purpose

The purpose of this policy is to define and identify the online, partially online, and hybrid course types and to establish a process for identifying, developing or redeveloping existing course content for delivery in one of these modalities.

Scope

This policy will guide the course development/redevelopment for online, partially online, and hybrid course types for all academic colleges, as well as stipulate the procedures for accurately scheduling and promoting these course types to align with federal, state, BOR, and accrediting body standards.

Policy

The development or redevelopment of courses for the online, partially online, or hybrid mode of delivery shall be a collaborative effort between the academic colleges and the distance learning department. This collaborative effort shall include the entire course delivery process including the identification of courses for alternative delivery methods, as well as the planning, development, redevelopment, review, and scheduling of identified courses.

Each academic college should work in collaboration with distance learning to identify those courses most suited for an alternative delivery method. Once a course has been identified, to initiate the course development/redevelopment the faculty member, chair, or dean should reach out to the distance learning department to obtain an “Online/Hybrid Course Development/Redevelopment Request” form (Appendix A). Upon receipt of the completed request form, distance learning will, in collaboration with the Department Chair and Content Developer, create a timeline for the development of content, design of the course, Quality Matters Review process, and create MOUs as appropriate (See Appendix B). Courses developed/redeveloped for online, partially online, or hybrid delivery shall be required to submit to the Quality Matters certification process prior to the second semester of delivery. It is expected that the course developer will work with the course development team until the course has “met expectations” and become Quality Matters (QM) certified.

Once the course development team agrees that the course development process has been completed and the course is ready for scheduling, information specific to alternate delivery method courses must be input into Banner for the scheduled term. (See Appendix C). The course developer should be given first right of refusal to teach the alternate delivery course for the first three offerings

of the course to facilitate continuous improvement of the course design process and the QM certification process.

Definitions

Online Course: An online course is a course that is delivered using distance education technologies in which all course components, lectures, activities, exams, quizzes, etc. may be completed fully online without a requirement to attend an on-campus activity. Online courses may require students to attend synchronous sessions on specific days/times using webinar technologies.

Partially Online Course: A partially online course is a course in which the delivery of 51% of more of the content occurs using distance education technologies. Typically, partially online courses require students to attend orientations or special in-class competency assessments in a face-to-face classroom environment on-campus.

Hybrid Course: A hybrid course is a course that blends on-campus face-to-face instruction with online instruction. A hybrid course replaces up to 50% of face-to-face course instruction with online instruction using distance education technologies. Example: A course that meets for 50 minutes on Monday, Wednesday, and Friday would be considered a hybrid course if the Friday section was moved to an online environment. Additionally, a lecture/lab course would be considered hybrid if the lecture portion was moved online and the lab portion was conducted on-campus.

Procedures

To initiate developing or redeveloping a course for online or hybrid delivery the appropriate representative from the academic college should contact distance learning (asuonline@asuarams.edu or 229-317-6241) to obtain an Online/Hybrid Course Development/Redevelopment Request Packet.

Following the submission of the Online Course Development/Redevelopment Request form, the Distance Learning representative, in collaboration with the Department Chair and Course Developer, will create a timeline for the development of content, design of the course, and Quality Matters Review process and credit. The developed course should be subject to the QM certification process prior to the second semester of delivery. It is expected that the course developer will work with the course development team until the course has “met expectations” and become QM Certified.

Steps to develop or redevelop a course for online delivery:

- Contact Distance Learning to obtain an Online/Hybrid Course Development/Redevelopment Request form
- Complete Online/Hybrid Course Development/Redevelopment form and submit to Distance Learning
- If the content developer identified on the Online/Hybrid Course Development/Redevelopment Request form is not certified in Applying the Quality Matters Rubric, he or she must become certified prior to the course development process
- Distance Learning will initiate a Memorandum of Understanding (MOU) between the Distance Learning Department, the Academic College/Department developing the course, and the Content Developer. The MOU should include:
 - Course development timeline, including deadlines for course content creation, quality checks, and course review

- Standards and requirements for the course's specific discipline
- Contact information for the content matter expert (content developer), the instructional designer, and the librarian assigned to the project delineating each members role
- Intellectual property rights
- Online instructional policies unique to the specific discipline, course or program
- If applicable, how and under what conditions incentives will be paid to any or all project members
- As applicable, the distance learning department will provide professional development to the content developer in the area of distance learning theory, Bloom's Digital Taxonomy, and GaVIEW tools and resources
- Content developer should work with librarian to ascertain if appropriate open educational resources exist for the course and implement free resources, when possible, in the place of for cost materials and textbooks
- Content developer should create a course content map that contains the following information:
 - Program Level outcomes
 - Course level outcomes
 - Module level outcomes (for each module level outcomes the following should be included; an example course map is provided to the content developer)
 - Instructional Content
 - Student Activities
 - Assessment
- Distance Learning will provide a course creation template for the project within the learning management system and the Instructional Designer assigned to the project will provide support in the creation and design of the course materials. The following guidelines will be followed:
 - All materials must meet accessibility standards in compliance with Section 508 Standards as delineated by the United States Access Board
 - Universal Design Standards should be implemented to include consideration of different operating systems, access devices, learning styles, etc.
 - Engagement opportunities for instructor-student; student-student; and student-instructor should be included in the course as often as possible, but must contain at a minimum, a weekly transparent academic activity for students to engage with the content, instructor, and/or other students
 - A "Start Here" module will be included in the course template and will include:
 - Course Syllabus
 - Course Schedule
 - Information on proctored test procedures (if proctoring is required)
 - Instructions on how to navigate the course and engage with the content
 - A "Student Resources" module will be included in the course template and will include:
 - Link to Academic Calendar – with information on course start and end dates, last day to drop without academic penalty and final exam (if applicable) dates

- Information on how to access online support specialist and other support services
- Information on how to access the online writing center
- Information on how to access the online math center
- Information on using Smarthinking
- Information on Turnitin (plagiarism detection software)
- Information on Respondus Monitor and Respondus Lockdown Browser
- Information on Proctor U
- Learning Management System navigation and resource tutorials
- Upon completion of course content development, a Quality Matters team will be created composed of three members to include a Master Reviewer, a Subject Matter Expert, and a Peer Reviewer (one of which must be from outside of the institution) and all of which must be QM certified peer reviewers.
- The QM Review team works with the content developer to perform a QM review of the course and the content developer should work with the team until the course has at a minimum met 85% of QM requirements
- The course will be placed on a QM review rotation to ensure QM Certification remains current

Accountability

Academic College deans, chairs, and program coordinators will be responsible for ensuring that the procedures stated within this policy for initiating and developing an alternate delivery course are followed.

Distance learning is responsible for collaborating with the academic college stakeholders and ensuring that appropriate steps are taken to facilitate the development, redevelopment and delivery of alternate method courses.

Distance learning will be considered the policy owner, review the policy every three years and suggest edits as required.

Contacts

Renita Luck, Executive Director, Distance Learning
229-317-6732 or renita.luck@asurams.edu

Last Update

October 2017

VALUE III – ACADEMIC INTEGRITY

Section 1. Academic Dishonesty: The intentional misrepresentation of one's work to deceive for personal gain, when in fact said work is not that person's or assisting another to do the same. When the instructor has sufficient evidence of cheating or plagiarism, he or she may impose disciplinary actions such as assigning a failing grade to the student's assignment, quiz, paper, or test. If the plagiarism or cheating involves major course work such as plagiarizing a research paper or cheating on a final exam, the instructor may fail the student in the course. Academic Dishonesty includes, but is not limited to cheating, plagiarism, and fabrication.

Page | 17

- **Definition of Cheating:** Cheating can be, but is not limited to, a student using electronic technology, notes, or other written materials not permitted by the instructor; looking at other students' papers without the instructor's permission; requesting answers from other students, alteration of grades or marks by the student in an effort to change the earned grade or credit; or working with other students when independent work is required. Situations where cheating may occur are during tests, exams, quizzes, or other similar methods of evaluation.
- **Definition of Plagiarism:** Plagiarism is the appropriation of language, thoughts, or ideas of another author and claiming that as one's own. Plagiarism is work not produced by the student, or work that does not credit borrowings from the original source(s). Plagiarism can also be viewed as submitting substantially the same work to satisfy requirements for one course or academic requirement that has been submitted in satisfaction of requirements for another course or academic requirement, without permission of the instructor of the course for which the work is being submitted or supervising authority for the academic requirement.
- **Definition of fabrication:** Fabrication is the falsification of data, information, or citations in any formal academic exercise. This includes making up citations to back up arguments or inventing quotations. Some other examples of fabrication would include making up data, changing data to support your hypothesis, claiming to have consulted sources that one really did not use.

Section 2. Forgery, Dishonesty, Fraudulent Acts and/or Misrepresentation:

1. Forgery of names, signatures, documents (personal, public, and/or private) will not be tolerated.
2. Forgery, deceptive acts, misrepresentation and/or dishonest acts include, but are not limited to materials, alteration, misuse of University documents, records, or student identification cards, or documents and records belonging to another, cheating, plagiarism, or other forms of academic dishonesty; tampering with the election of any University recognized student organization; malfeasance of misuse of elective or appointive office student organization, its members, or the welfare of the University community.
3. Representing one's self as a member of a fraternity or sorority through the use of letters, paraphernalia, gestures, etc. without being a nationally initiated member who is acknowledged as an official member by documents from the national organization, including a membership card and

certificate/shingle; and fraudulently issuing worthless checks to the University. Lying, knowingly furnishing false information to the University or its officials, other forms of dishonesty in University-related affairs is also prohibited.

4. The scope includes but is not limited to the following: lying, fraudulently obtaining, altering, falsifying, transferring, loaning, selling or misusing or attempting intended misuse of ID card, validation sticker, or any University document or service, misuse of university computer systems, laboratories, equipment, or software in violation of university computer use policies.
5. Unauthorized access, distribution, alteration, or use of electronic materials including, but not limited to, information, images, text, or software; recklessly or maliciously interfering with or damaging computer or network resources or computer data, files, or other information; engaging in or attempting to engage in a denial of service; failing to comply with laws, license agreements, and contracts governing network, software and hardware use.
6. Using University computing resources for unauthorized commercial purposes or personal gain.
7. Proving use of your personal account or password to another person; using another owner's account or password with or without authorization; accessing or causing to be accessed, downloading or causing to be downloaded, pornographic or obscene materials.

Section 3. Cooperative or Collaborative Effort in Coursework: Without acknowledgement or explicit permission of the instructor (including digital media); knowingly helping or attempting to help another violate any provision of the Honor Code. Examples include, but are not limited to the following:

- a. Working together on a take-home exam;
- b. Working together on assignments without instructor permission.

Section 4. Abuse of Academic Materials: Intentionally or knowingly destroying, stealing, or making inaccessible any resource material. Examples include, but are not limited to:

- a. Stealing, destroying, or hiding any reference materials needed for common academic requirements.
- b. Stealing exams, grade books, books, papers, computer equipment and data, and laboratory materials.
- c. Destroying computer files or programs needed for academic works
- d. Damaging computer equipment (including removable media such as disks, CDs, flash drives, etc.) or laboratory equipment in order to alter or prevent evaluation of academic work, unauthorized use of another's computer password, disrupting the content or accessibility of an internet site, or impersonating another to obtain computer resources.
- e. Purchasing and/or using an instructor edition of any textbook in place of the student edition for any course.

Section 5. Submitting Work for Multiple Purposes: Submitting without prior permission, any work submitted to fulfill another academic requirement. This includes work first produced in connection with classes at either Albany State

University or other institutions attended by the student.

Section 6. Theft: Stealing, taking or obtaining in any unauthorized manner information related to any academic work. Examples include, but are not limited to: stealing exams, grade books, books, papers, computer equipment and data, and laboratory materials.

VALUE IV - PROPERTY AND THE ENVIRONMENT

Section 1. Animals (Pets):

- a. Having pets or other animals (dogs, cats, snakes, birds, hamsters, etc.) on campus and/or in campus buildings are prohibited **with the exception of service animals and comfort therapeutic animals, when accompanied by their owner**, and tropical fish in an aquarium or other approved containers in buildings, including student residences, classrooms, and offices.
- b. The feeding of stray animals in or around residential facilities is also prohibited for students' safety purposes. Stray animals are not vaccinated and may cause harm to students, faculty, staff or the campus members.

Section 2. Arson/Fire Setting: The malicious fraudulent, and/or unauthorized burning of property on the University premises. Such acts include, but are not limited to, creating fires, setting a personal fire, open flames, and/or igniting flammable materials.

Section 3. Damage to Property/Destruction of Property and/or Vandalism:

1. Damage, vandalism or destruction of property owned or leased by the University or personal property belonging to an individual. This includes, but is not limited to, car vandalism, walking on roofs of a university building, defacing structures, and facilities, littering, unauthorized biking, skating and/or skate boarding in inappropriate areas, marking, egging, keying, painting, spraying University property or the property of others.
2. Intentionally damage any property of another without consent of that other person and the damage thereto is interfering with the possession or use of the property of another person without consent of that person.
3. Damaging university property such as light fixtures, ceiling fans, walls, and pictures is prohibited.
4. A violation of this policy includes, but is not limited to:
 - a. Intentionally and maliciously breaking or damaging furnishings;
 - b. Damaging to the kitchen/living area of residence halls; or,
 - c. Damaging to your assigned room space or unit in the residence halls (i.e. ceilings, floors, carpets, door, door frame, etc.);
 - d. Damaging to other University property (i.e. University vehicles, landscaping, golf carts, etc.).

Section 4. Weapons and/or Firearms:

- a. Except where allowed by law or specifically authorized by the administration or as part of a University-sanctioned event, no student shall keep, use, possess, display, or carry any rifle, shotgun, handgun, or other lethal or dangerous device capable of launching a projectile by air, gas, explosion, or mechanical means (including BB guns, air-soft guns, and paintball guns) on any property owned, controlled, or leased by the University;
- b. No student shall use, possess, display or carry any toy weapon which

Student Confidentiality

The Family Educational Rights and Privacy Act (FERPA)

Albany State University protects students’ rights to privacy, and accords students all the rights under the federal law.

No one outside of the institution shall have access to, nor will the institution disclose any information from students’ education records, without the written consent of students, except: to authorized personnel within the institution, to officials of other institutions in which students seek to enroll, to persons or organizations providing students financial aid, to accrediting agencies carrying out their accreditation function, to persons in compliance with a judicial order and to persons in an emergency in order to protect the health or safety of students or other persons. All of these exceptions are permitted under the Act.

ASU is fully committed to ensuring the privacy and protection of personal information of all student, including those enrolled in distance learning program, and does not share personal information gathered from distance education and/or on-campus/residential students. However, in some cases, the University may be compelled by the Open Records law to release information, as outlined in the Policies and Procedures for Responding to **Open Records Requests**.

According to FERPA student rights include:

- 1. Right of Inspection of Records
- 2. Right to challenge records believed to be inaccurate
- 3. Right to consent to disclosure of personally identifiable records (with exceptions)
- 4. Right to file complaints of alleged violations of the aforementioned rights.

Students who feel that their FERPA rights have been violated may file a formal complaint with the Office of the Registrar. The complaint must be submitted in writing to the Office of the Registrar at Albany State University’s standard mailing address.

If a student feels their FERPA rights were violated by the AS&R personnel a complaint may be filed to the Office of the Provost, Academic Affairs.

To review further information, visit or contact the Office of the Registrar at Ram Central West (C Building). Or, visit the Web site of the **Department of Education FERPA**.

RETENTION OF STUDENT ACADEMIC RECORDS (COMMONLY REFERRED TO AS EDUCATION RECORDS):

The retention period for student academic records is permanent.

ASU FERPA AUTHORIZATION FORM

FERPA Authorization Form

- ▶ Class Schedules
- ▶ Commencement
- ▶ Final Exams Schedule
- ▶ Forms
- ▶ Internal Transfer Students
- ▶ Re-admission
- ▶ Registrar FAQ
- ▶ Student Academic Calendar
- ▶ Student Confidentiality
- ▶ Transfer Students
- ▶ Transcript Information
- ▶ Tuition Waivers



ASU East Campus
504 College Drive
Albany, GA 31705
Phone: (229) 500-2000

ASU West Campus
2400 Gillionville Rd
Albany, GA 31707



- Accreditation
- ASU Careers
- Maps
- Students
- Campus Safety
- ASU Foundation
- Events Calendar
- Flickr Photos
- Request a Transcript
- ASU IT Help Desk
- Equal Employment Opportunity
- Ethics & Compliance Hotline
- Human Trafficking Notice

Information Security

To protect the confidentiality, integrity, and availability of university information it is important that all Faculty, Staff and Students understand at least the basics of CyberSecurity. The Albany State University (ASU) Office of Information Technology Services (ITS) is providing you with tools and information to help you protect your information. As a member of the ASU Campus Community, it is important that you understand the institutional policies and have adequate knowledge to protect institutional and personal resources.

As a member of the University System of Georgia (USG), ASU ITS policies, standards and guidelines follow the **USG Information Technology Handbook**

. Please review the USG Information Technology Handbook and become familiar with it as ASU follows and complies with the contents.

For more information on ASU ITS guidelines and forms, you may click the menu on the left. In the meantime, please enjoy this video made available through Educause as a part of their collaboration with the Higher Education Information Security Council.



- ▶ [Getting Started for Employees](#)
- ▶ [Getting Started for Students](#)
- ▶ [Personnel](#)
- ▶ [Project Management Office](#)
- ▶ [Accessing Campus WiFi](#)
- ▶ [Enterprise Reports – Argos](#)
- ▶ [Banner Student Information System](#)
- ▶ [Card Services](#)
- ▶ [Forms & Policies](#)
- ▶ [General Use Computer Labs](#)
- ▶ [Help Desk](#)
- ▶ [Information Security](#)
 - ▶ [Information Security Awareness Training](#)
 - ▶ [Information Security News](#)
- ▶ [IT Service Catalog](#)
- ▶ [VP of Information Technology Services and CIO](#)
- ▶ [New Department Fax Numbers](#)
- ▶ [New Department Phone Numbers](#)

Information Security Policies & Forms

[ITS Appropriate Use Policy](#)
[ITS Email Policy](#)
[ITS Incident Response](#)
[Information Security Awareness Training Policy](#)
[Info-Sec Anti-Virus](#)
[Password Protection Standard](#)

ITS Email Policy

Contents

- Purpose
- Scope
- Policy
- Accountability
- Contacts
- References
- Version History

PURPOSE

The purpose of this policy is to set forth guidelines relating to the use of Albany State University's (ASU) electronic mail system ("e-mail"). It will also delineate the university's right of access to e-mail and establish rules relating to the retention and destruction of email.

SCOPE

This policy applies to all Albany State University faculty, staff, students, alumni, and affiliates (vendors, contractors, consultants, etc.).

POLICY

ASU electronic mail users must abide by the guidelines in this policy and protect e-mail documents according to the university, University System of Georgia Board of Regents (USGBOR) policies and standards as well as federal and Georgia State laws.

1. Acceptable Use

Use not consistent with this policy will be considered unauthorized use as referenced in the ASU and USGBOR Acceptable Use policies. ASU will provide the university e-mail system, and/or contracts for any Third-Party e-mail system (s), for learning activities and administrative functions supporting its business and academic missions. The e-mail system (s) primary use is for university business and academic purposes; however, modest personal use of the e-mail systems is allowed. E-mail made or received using the university e-mail system is subject to be made and/or received in the course of university employment and is subject to federal, state and local laws and regulations (including the Georgia Open Records Act), and ASU policies, including laws, regulations and policies that are specific to computers and networks. Anyone performing official university business is required to utilize their e-mail system account(s) and not personal e-mail accounts.

2. Access and Disclosure

1. Access to ASU's information technology resources, including the E-mail Systems, is a privilege. The University reserves the right to limit, restrict or remove access to its resources when policies or laws are violated and to use appropriate means to safeguard its resources, preserve network/system integrity, and ensure continued service delivery at all times.
2. E-mail may constitute University "correspondence" or "computerized records" and therefore may be considered public records subject to disclosure under the Georgia Open Records Act or other laws, or as evidence in a legal action.
3. ASU will not routinely inspect, monitor, or disclose e-mail. The university shall exercise the right with discretion, to access, retrieve, inspect and disclose the contents of e-mail for University-related purposes, which may include, but are not limited to:
 1. Maintaining system integrity
 2. Protecting health and safety
 3. Preventing interference with the academic mission
 4. Performing required internal investigations
 5. Complying with legal requests and demands

3. Privacy and Confidentiality

ASU will make reasonable efforts to maintain the integrity and effective operations of the university e-mail systems. Users should not regard e-mail as a secure medium for the communication of sensitive or confidential information. ASU cannot assure neither the privacy of an individual user's usage of the e-mail systems nor the confidentiality of their messages.

Users should exercise particular caution, so as not to send sensitive information as listed.

1. Information about the medical or mental condition of employees or students
2. Material about the evaluation, performance or discipline of ASU employees or students
3. Evidence relating to the investigation, defense, or prosecution of any pending judicial action or administrative charge in which the university, its faculty, staff or students are parties;
4. Information relating to the investigation, resolution or disposition of any complaint or charge involving faculty, staff or students, including, but not limited to, complaints and/or charges involving fair practices, grievances or alleged discrimination; and information relating to the request for or delivery of legal advice or employer/employee relations assistance) via unencrypted e-mail, and should limit any such communications (or further disclosure of any such communications) to those with a legitimate need to know.

4. Prohibited Uses

The E-mail Systems may not be used for unlawful activities or for commercial purposes that are not directly related to the university's mission or otherwise authorized. Other prohibited uses of the E-mail Systems include, but are not limited to:

1. Sending copies of documents or inclusion of the work of others into e-mail in violation of copyright laws
2. Sending junk mail or spam messages.
3. Using e-mail to harass, intimidate, defame or discriminate against others or to interfere with the ability of others to conduct university business.
4. Soliciting e-mail from any other e-mail address, other than that of the poster's account; creating or forwarding chain letters or solicitations for business schemes; using e-mail originating from within university networks for commercial purposes or personal gain.
5. Sending the same or similar non-business-related messages to large numbers of e-mail recipients such as mass-e-mailing.
6. Misrepresenting (including forgery) the identity of the sender or the source of an Electronic Communication.
7. Acquiring or attempting to acquire passwords of others.
8. Using or attempting to use the computer accounts of others.
9. Altering the content of a message originating from another person or computer with intent to deceive.
10. Deleting another person's postings without authorization.
11. Obtaining access to the files or e-mail of others without documented approval from the Office of the President or Legal Counsel
12. Attempting unauthorized access to e-mail or attempting to breach any security measures on any e-mail system, or attempting to intercept any e-mail transmissions without proper authorization.
13. Using e-mail for any purpose restricted or prohibited by law, USGBOR, or ASU policies.

5. Intellectual Property

A faculty or staff member does not lose any ownership interest he/she has in intellectual property pursuant to ASU and USGBOR policies on intellectual property, because the work is communicated through e-mail. If there is a dispute regarding ownership of the work, the University has the right, upon written notification to the faculty or staff member, to obtain access to the work (and to any e-mails in which the work is communicated) for the purpose of determining whether the University has an interest in it

6. Retention and Disposal

Employee e-mail is public record subject to disclosure under the Georgia Open Records Act. E-mail in the university e-mail system is subject to the record retention schedules established by ASU, USGBOR Records Retention policies and standards, compliance standards, and federal and state law. The university reserves the right to retain e-mails in the university e-mail System as required. Federal laws may require retaining e-mail in the university e-mail system for a specific time as defined by individual laws (e.g. FERPA, HIPAA, and PCIDSS).

1. Upon an employee's separation of employment, the employee's e-mail account shall be terminated and the university has the right to access e-mail made or received by the employee using the university e-mail systems or which is otherwise made or received in the course of employment. An employee who separates from employment shall not remove, destroy, or copy any of the business-related e-mail entrusted to his/her care or created by him/her during employment, unless otherwise permitted in writing by ASU.
2. In accordance with USGBOR Records and Retention policy, ASU Information Technology Services (ITS) must retain deans, executives, vice presidents and above employees email communication permanently. All other employees email will be archived for five years after employment has ended. If employees wish to retain e-mail in the university e-mail system beyond local server thresholds, they must transfer the information to disk. Such disks and the information they contain, constitute university property and may need to be retained based on applicable laws and policies.
3. In certain circumstances, Albany State University may issue a litigation hold requiring employees to retain electronic communications that is created, received, maintained or stored on the university e-mail system

ACCOUNTABILITY

Violation of this policy may subject the user to sanctions, including the loss of computer and/or network access privileges, disciplinary action, suspension, termination of employment, dismissal from ASU, and/or legal action.

CONTACTS

- Albany State University Chief Information Officer
- Albany State University Chief Information Security Officer

REFERENCES

- ASU ITS Security Website: <https://webdev.asurams.edu/betaram/content/information-security>
- USGBOR Handbook: http://www.usg.edu/information_technology_handbook/section5
- SANS Institute: <http://www.sans.org>

VERSION HISTORY

Date	Version	Description
July 9, 2013	1.2	First release
August 11, 2015	1.3	Removed individual names under the contact section

▶ Getting Started for Employees

▶ Getting Started for Students

▶ Personnel

▶ Project Management Office

▶ Accessing Campus WiFi

▶ Enterprise Reports – Argos

▶ Banner Student Information System

▶ Card Services

▶ Forms & Policies

▶ Info-Sec Anti-Virus

▶ Information Security Awareness Training Policy

▶ ITS Appropriate Use Policy

▶ ITS Email Policy

▶ ITS Incident Response

▶ ITS VPN Remote Access Policy

▶ Password Construction Guidelines

▶ Password Protection Standard

▶ ASK ITS Question Form

▶ General Use Computer Labs

▶ Help Desk

▶ Information Security

▶ IT Service Catalog

▶ VP of Information Technology Services and CIO

▶ New Department Fax Numbers

▶ New Department Phone Numbers

Password Protection Standard

Contents

Purpose

Scope

Standard

General

Password Creation

Password Change

Administrative Accounts

Server Administrator Passwords

Password Resets

Authority, Enforcement, Exceptions

Standard Compliance

Accountability

Contacts

References

Version History

PURPOSE

The purpose of this document is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

SCOPE

This Standard applies to all individuals associated with Albany State University (hereinafter referred to "ASU"), including faculty, staff, student assistants, and contractors. This Standard applies to anyone accessing or utilizing ASU's network or data. This use may include, but is not limited to, the following: personal computers, laptops, ASU-issued cell phones, and hand-held computing devices (e.g., iPad's, Xyboards, USB memory keys, etc.), as well as ASU electronic services, systems and servers. This Standard covers departmental resources as well as resources managed centrally.

STANDARD

General

Passwords are a primary means to control access to systems and should therefore be selected, used, and managed to protect against unauthorized discovery or usage. ASU maintains electronic information resources which are essential to performing University business. Similar to any other capital resources owned by the University, these resources are to be viewed as valuable assets over which the University has both rights and obligations to manage, protect, secure, and control. University 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 computer systems, network systems, and data.

Password Creation

All user-level and system-level passwords must conform to the **University System of Georgia Information Technology (USGITS) Handbook Section 5.12** and the ASU Password Construction Guidelines Standard. Where possible, users must not use the same password for various ASU access needs. User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines as defined in USG ITS Handbook Section 5.12 and the ASU Password Construction Guidelines Standard

Password Change

All system-level passwords (for example, root, enable, Active Directory administrators, application administration accounts, and so on) must be changed every ninety (90) days. All user-level passwords (e.g., email, web, desktop computer, etc.) shall be changed every one hundred and eighty (180) days. Password cracking or guessing may be performed on a periodic or random basis by the ASU Information Security Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the ASU Password Construction Guidelines.

Password Protection

All passwords should be treated as sensitive, confidential information. Users should not write passwords down and store them anywhere in their office. Nor should they store passwords in a file on ANY computer system (including Personal Computing Devices or similar devices) without encryption.

Passwords should not be inserted into email messages or other forms of electronic communication.

Passwords must not be revealed over the phone to anyone.

Do not reveal a password on questionnaires or security forms.

Do not hint at the format of a password (for example, "my family name").

Users should not share passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

Users should not use the "Remember Password" feature of applications (for example, web browsers).

If an account or password is suspected of being compromised, the incident should be reported to the appropriate access administrator and the user should change the password.

Users Should Not Employ Any Automatic Log-In Actions

ASU information system users should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.

Besides the authorized user, passwords should never be shared or revealed to anyone. Temporary or "first use" passwords should be changed the first time that the authorized user accesses the system. Failure to change a temporary or "first use" password leaves the authorized user liable for all actions performed under the assigned account. If users need to share computer resident data, they should use approved network services or any other mechanisms that do not infringe on any ASU or USGITS standards.

Application Development

Application developers must ensure that their programs contain the following security precautions:

Applications must support authentication of individual users, not groups.

Applications must not store passwords in clear text or in any easily reversible form.

Applications must not transmit passwords in clear text over the network.

Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

STANDARD COMPLIANCE

Compliance Measurement

The Information Security team will verify compliance to this policy through various methods, including but not limited to, periodic walk through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Information Technology Services will, whenever reasonably possible, configure accounts for automatic password expiration and set other options to encourage or remind individuals to change their passwords.

Exceptions

Exceptions must be justified in writing and accepted by the CISO of Albany State University or his/her designee. In the case of an information system managed by a third party, the University CISO can, in concurrence with the information owner, make a determination that the third party's security controls meet or exceed this standard. This exception must be based on an assessment of the third party's controls and documented in writing.

Non-Compliance

Violations of this Standard may be referred to appropriate administrative offices for disciplinary action. Violators may be subject to disciplinary outcomes as outlined in the Student Handbook and/or Employee Handbook. In addition to the other sanctions outlined in the handbooks, improper use of administrative accounts may result in immediate suspension and loss of privileges.

CONTACTS

The Chief Information Officer is charged with the responsibility to periodically review the policy and propose changes as needed.

REFERENCES

ASU IT Security Website: <https://www.asurams.edu/technology/information-security/>

USGBOR Handbook: http://www.usg.edu/information_technology_handbook/section5

National Institute for Standards and Technology: <http://www.nist.gov>

SANS Institute: <http://www.sans.org>

COBIT 5.0: <http://www.isaca.org/>

VERSION HISTORY

Date

Version

Description

June 2007

1.0

ASU ITS

October 9, 2013

1.3

ASU Information Technology Governance Committee

June 2015

2.0

Major re-write by Information Security Team

▶ Getting Started for Employees

▶ Getting Started for Students

▶ Personnel

▶ Project Management Office

▶ Accessing Campus WiFi

▶ Enterprise Reports – Argos

▶ Banner Student Information System

▶ Card Services

▶ Forms & Policies

▶ Info-Sec Anti-Virus

▶ Information Security Awareness Training Policy

▶ ITS Appropriate Use Policy

▶ ITS Email Policy

▶ ITS Incident Response

▶ ITS VPN Remote Access Policy

▶ Password Construction Guidelines

▶ Password Protection Standard

▶ ASK ITS Question Form

▶ General Use Computer Labs

▶ Help Desk

▶ Information Security

▶ IT Service Catalog

▶ VP of Information Technology Services and CIO

▶ New Department Fax Numbers

▶ New Department Phone Numbers

Albany State University

ASU East Campus

504 College Drive

Albany, GA 31705

Phone: (229) 500-2000

ASU West Campus

2400 Gillionville Rd

Albany, GA 31707

Accreditation

ASU Careers

Maps

Students

Campus Safety

ASU Foundation

Events

Calendar

Flickr Photos

Request a Transcript

ASU IT Help Desk

Equal Employment Opportunity

Ethics & Compliance Hotline

Human Trafficking Notice

f

Copyright © 2018 Albany State University All Rights Reserved.
Albany State University is committed to principles of equal opportunity and affirmative action.

Information Security Awareness Training Policy

Contents

- Purpose
- Scope
- Policy
- Accountability
- Contacts
- References
- Version History

Purpose

The purpose of the Albany State University (ASU) Information Security Awareness and Training Policy is to identify the conditions necessary to provide information technology system users with appropriate awareness of information and information systems security requirements and of their responsibilities to protect information technology resources and systems. The success of the University's awareness and training program, and the overall awareness of secure business practices, depends upon the ability of all users to work toward a common goal of protecting ASU's information, information systems and associated resources.

Scope

This policy refers to all ASU information resources whether individually controlled or shared, stand-alone or networked. It applies to all information and information systems, communication facilities owned, leased, operated, or contracted by the ASU. This includes networking devices, personal digital assistants, telephones, wireless devices, workstations, minicomputers and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.

Policy

This policy is in support of ASU security policies, standards, and procedures designed to educate users about risks to information and information systems. The ASU security training and awareness program includes security awareness presentations, security reminders, general security training, system-specific security training, security management training and professional security education for members of the workforce. Additionally, our awareness and education program will include the following:

- Annual mandatory training
- Scheduled awareness surveys.
- Periodic unscheduled awareness assessments to assure compliance with the training.
- Feedback surveys to improve our awareness training and education program.

Training completion and results will be maintained in the individuals Human Resources personnel file, as part of the permanent record.

Accountability

Violation of this policy may subject the user to sanctions, including the loss of computer and or network access privileges, disciplinary action, suspension, termination of employment, dismissal from ASU, and / or legal action.

Contacts

The Chief Information Officer is charged with the responsibility to periodically review the policy and propose changes as needed.

References

- ASU IT Security Website: <https://www.asurams.edu/technology/information-security/>
- USGBOR Handbook: http://www.usg.edu/information_technology_handbook/section5
- National Institute for Standards and Technology: <http://www.nist.gov>
- SANS Institute:Version 1.3 <http://www.sans.org>
- COBIT 5.0: <http://www.isaca.org/>

VERSION HISTORY

Date	Version	Description
October 9, 2013	1.3	ASU Information Technology Governance Committee

- ▶ Getting Started for Employees
- ▶ Getting Started for Students
- ▶ Personnel
- ▶ Project Management Office
- ▶ Accessing Campus WiFi
- ▶ Enterprise Reports – Argos
- ▶ Banner Student Information System
- ▶ Card Services
- ▶ Forms & Policies
 - ▶ Info-Sec Anti-Virus
 - ▶ Information Security Awareness Training Policy
 - ▶ ITS Appropriate Use Policy
 - ▶ ITS Email Policy
 - ▶ ITS Incident Response
 - ▶ ITS VPN Remote Access Policy
 - ▶ Password Construction Guidelines
 - ▶ Password Protection Standard
 - ▶ ASK ITS Question Form
- ▶ General Use Computer Labs
- ▶ Help Desk
- ▶ Information Security
- ▶ IT Service Catalog
- ▶ VP of Information Technology Services and CIO
- ▶ New Department Fax Numbers
- ▶ New Department Phone Numbers



ASU East Campus
504 College Drive
Albany, GA 31705
Phone: (229) 500-2000

ASU West Campus
2400 Gillionville Rd
Albany, GA 31707



- Accreditation
- ASU Careers
- Maps
- Students
- Campus Safety
- ASU Foundation
- Events Calendar
- Flickr Photos
- Request a Transcript
- ASU IT Help Desk
- Equal Employment Opportunity
- Ethics & Compliance Hotline
- Human Trafficking Notice

ITS Appropriate Use Policy

Contents

- Purpose
- Scope
- Policy
- Accountability
- Contacts
- References
- Version History

Purpose

This policy provides guidelines for the appropriate use of information resources. Use of Albany State University's (ASU) network and computer resources should support the basic missions of the University in teaching, learning and research. Users of the ASU network and computer resources are responsible for proper use, protecting information resources, and respecting the rights of others.

Scope

The policy applies to all ASU students, faculty and staff, and all others using computer and communication technologies whether personally or University owned, which accesses, transmits or stores University or student information.

Policy

- **General Policy** Users of University information resources must protect their online identity from use by another individual, the integrity of computer-based information resources, and the privacy of electronic information. In addition, users must refrain from seeking to gain unauthorized access, honor all copyrights and licenses and respect the rights of other information resources
- **Access** Users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access. Attempts to gain unauthorized access to a system or to another person's information are a violation of University policy and may also violate applicable law, potentially subjecting the user to both civil and criminal liability. However, authorized system administrators may access information resources, but only for a legitimate operational purpose and only the minimum access required to accomplish this legitimate operational purpose.
 - Prohibition against Sharing User IDs and Passwords Sharing an online identity (user ID and/or password) violates University policy.
 - Information Belonging to Others Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, passwords or other digital materials belonging to other users, without the specific permission of those other users.
 - Abuse of Computing Privileges Users of ASU information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the University.
- **Usage** Use of the University's information resources must comply with ASU policies and legal obligations (including licenses and contracts) and all federal and state laws.
 - Prohibited Use Users must not send, view or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or University policy. In particular, contributing to the creation of a hostile academic or work environment is prohibited.
 - Copyrights and Licenses Users must not violate copyright law and must respect licenses to copyrighted materials. For the avoidance of doubt, unlawful file-sharing using the University's information resources is a violation of this policy.
 - Social Media Users must respect the purpose of and abide by the terms of use of online media forums, including social networking websites, mailing lists, chat rooms and blogs.
 - Political Use University information resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws, and may be used for other political activities only when in compliance with federal, state and other laws and in compliance with applicable University policies.
 - Personal Use University information resources should not be used for activities unrelated to appropriate University functions, except in a purely incidental manner.
 - Use of University Information Users must abide by applicable data storage and transmission policies.
- **Integrity of Information Resources** Users must respect the integrity of information and information resources.
 - Modification or Removal of Information or Information Resources Without proper authorization, users must not attempt to modify or remove information or information resources that are owned or used by others.
 - Other Prohibited Activities Users must not encroach, disrupt or otherwise interfere with access or use of the University's information or information resources. For the avoidance of doubt, without express permission, users must not give away University information or send bulk unsolicited email. In addition, users must not engage in other activities that damage, vandalize or otherwise compromise the integrity of University information or information resources.
 - Academic Pursuits The University recognizes the value of legitimate research projects undertaken by faculty and students under faculty supervision. The University may restrict such activities in order to protect University and individual information and information resources, but in doing so will take into account legitimate academic pursuits.
- **Access for Legal and University Processes** Under some circumstances, as a result of investigations, subpoenas or lawsuits, the University may be required by law to provide electronic or other records, or information related to those records or relating to use of information resources, ("information records") to third parties. Additionally, the University may in its reasonable discretion review information records, e.g., for the proper functioning of the University, in connection with investigations, or to protect the safety of individuals or the ASU community. The University may also permit reasonable access to data to third-party service providers in order to provide, maintain or improve services to the University. Accordingly, users of University information resources do not have a reasonable expectation of privacy when using the University's information resources.

Accountability

- Violation of this policy may subject the user to sanctions, including the loss of computer and/or network access privileges, disciplinary action, suspension, termination of employment, dismissal from ASU, and/or legal action.

Contacts

- Albany State University Chief Information Officer
- Albany State University Chief Information Security Officer

References

- ASU ITS Security Website: <https://www.asurams.edu/technology/information-security/>
- USGBOR Handbook: http://www.usg.edu/information_technology_handbook/section5
- SANS Institute: <http://www.sans.org>

Version History

Date	Version	Description
May 14, 2015	1.2	Removed names from the positions in Contacts section

▸ Getting Started for Employees

▸ Getting Started for Students

▸ Personnel

▸ Project Management Office

▸ Accessing Campus WiFi

▸ Enterprise Reports – Argos

▸ Banner Student Information System

▸ Card Services

▸ Forms & Policies

▸ Info-Sec Anti-Virus

▸ Information Security Awareness Training Policy

▸ ITS Appropriate Use Policy

▸ ITS Email Policy

▸ ITS Incident Response

▸ ITS VPN Remote Access Policy

▸ Password Construction Guidelines

▸ Password Protection Standard

▸ ASK ITS Question Form

▸ General Use Computer Labs

▸ Help Desk

▸ Information Security

▸ IT Service Catalog

▸ VP of Information Technology Services and CIO

▸ New Department Fax Numbers

▸ New Department Phone Numbers



ASU East Campus

504 College Drive
Albany, GA 31705

Phone: (229) 500-2000

ASU West Campus

2400 Gillionville Rd
Albany, GA 31707

- Accreditation
- ASU Careers
- Maps
- Students

- Campus Safety
- ASU Foundation
- Events Calendar
- Flickr Photos

- Request a Transcript
- ASU IT Help Desk
- Equal Employment Opportunity
- Ethics & Compliance Hotline
- Human Trafficking Notice



ITS Incident Response

Contents

- Purpose
- Scope
- Policy
- Definitions
- Contacts
- References
- Version History

Purpose

Albany State University's (ASU) information, information systems, and infrastructure are critical resources for accomplishing the mission of the university. All ASU users have an interest in the security of these resources, and share in the responsibility for protecting them. Prompt and consistent reporting of and response to information technology (IT) incidents protects and preserves the confidentiality, integrity, availability, and privacy of information, information systems and associated infrastructure resources which helps the university to comply with applicable law.

Scope

This policy applies to all Albany State University faculty, staff, students, and affiliates (vendors, contractors, consultants, etc.). This policy also applies to information in any tangible form whether it is written, filmed, typed, recorded electronically or printed, and to all ASU information and technical resources.

Policy

The Albany State University IT Security Incident Response Policy and subordinate procedures define standard methods for identifying, tracking and responding to network and computer-based IT Security Incidents.

The ASU Chief Information Security Officer (CISO) is responsible for ensuring that incidents are reported promptly upon discovery, that incidents are investigated, and escalated to the University System Georgia Board of Regents (USGBOR) and local, state, and federal law enforcement agencies where applicable.

All IT system users are responsible for promptly reporting any suspected incidents to the Chief Information Security Officer through the ASU Help Desk. A preliminary investigation into all suspected incidents will be conducted to determine if the event is an actual incident requiring a coordinated incident response. The affected end user, academic and business owners and their associated Vice President and the ITS VP/CIO will be notified immediately upon discovery of an incident.

Any computing device that is involved in an incident is subject to being confiscated by ITS staff as a precautionary measure to protect the ASU networking infrastructure. The device will returned immediately once it has been tested and deemed safe to operate.

- **Identification of Incidents**
Any faculty, staff, student of ASU or outside organization may refer an activity or concern to Information Technology Services. Once identified, ITS will use standard procedures to log and track incidents, work with others as appropriate, take steps to investigate, escalate, remediate, and refer to others or otherwise address as outlined in the remainder of this policy.
- **Establishment of an IT Security Incident Response Team** The CISO is responsible for Incident interdiction and remediation of information and information systems and associated resources affected by these incidents. The CISO will consult administrators, Information Technology Services, Academic and Administrative Systems departments, USGBOR CISO, ASU Police Chief, State and Federal agencies or other units, as warranted. The CISO establishment of an IT Security Incident Response Team in response to specific incidents will be based on the level and severity of the incident.
- **Risk Assessment Classification Matrix**
The CISO will establish an internal risk assessment classification matrix. The matrix will be applied to focus the response to each Incident, and to establish the appropriate team participants to respond. This classification matrix will correspond to an "escalation" of contacts across the university, and will indicate which authorities at ASU to involve and which procedure would be applicable for each class of incident.
- **Documentation and Communication of Incidents**
The Information Technology Services will ensure that Incidents are appropriately logged and archived. Documentation of such Incidents will be catalogued and cross-reference other event databases within the university. The Help Desk, CISO and IT Security Incident Response Team representatives will be responsible for communicating the Incident to appropriate personnel and maintaining contact, for the purpose of update and instruction, for the duration of the Incident.
The CISO will maintain subordinate procedures for the response and investigation of each Incident and securing the custody of any evidence obtained in conjunction with the ASU Chief of Police in the investigation. The procedures will specify the location and method of custody for each incident, if custody of evidence is required.
- **Relationship to USGBOR, State and Federal Agencies**
A response plan or remediation defined by this policy may be preempted as required or at ASU's discretion by the intervention of USGBOR or federal and state executive officials.
- **Incident Prevention, Detection, and Correction**
ASU will undertake measures to prevent Incidents by monitoring and scanning for anomalies, and developing clear protective procedures for the configuration of its IT resources. Proactive measures are undertaken to detect information security related incidents by use of malware and antivirus tools, network monitoring tools, and logging and event monitoring. After an incident has been discovered or reported, ASU ITS will take aggressive action to resolve the incident as deemed appropriate by the IT Security Incident Response Team.
- **Modifications and Adjustments**
This procedural documentation will be reviewed periodically to adjust processes, identify new risks and remediation.

Definitions

Sensitive Information

Sensitive Information is information that is not to be publicly disclosed. The disclosure, use, or destruction of Sensitive Information can have adverse effects on ASU and possibly carry significant civil, fiscal, or criminal liability. This designation is used for highly sensitive information such as open legal investigations, sealed bids, research activity, social security numbers, etc., whose access is restricted to selected, authorized employees

Academic or Business data owner

The individual who has ultimate responsibility and ownership for a particular set of data (e.g. a department head, dean, or V.P.)

Forensic Analysis

The process of making a duplicate of the computer system hard drive(s) using some form of hardware write protection, such as a hardware write blocker, to ensure no writes are made to the original drive.

Information Security Incident Response Team (ISIRT)

The role of the ASU ISIRT is to coordinate the University response to breaches of security involving confidential or private information. The responsibilities of the ISIRT include, but are not limited to:

- Notifying affected constituents of the incident
- Coordinating responses to public inquiries
- Making the decision to involve law enforcement agencies and computer forensic experts
- Discussing, reviewing, and documenting any lessons learned from incidents

IT Incident

An activity or event that results in damage to, misuse of, or loss of, an IT resource. Incidents include but are not limited to: •

- Loss of a computing device (misplaced, stolen, vandalized)
- Detection of a malicious program, such as a virus, worm, Trojan horse, keystroke logger, rootkit, remote control bot, etc.
- Detection of unauthorized users, or users with unauthorized escalated privileges.
- Detection of a critical or widespread vulnerability or misconfiguration that might lead to a compromise affecting the confidentiality, integrity, or availability of university systems or data.

IT Resource

A computing asset provided by ASU to further its mission. Examples include, but are not limited to, network bandwidth, networking equipment, workstations, computer systems, data, databases, servers, and printers.

Local Support Provider

An individual or group with principal responsibility for the installation, configuration, security, and maintenance of an IT resource. When there is no formally identified local support provider (e.g., a personally owned computer used from home to connect to the ASU network), the user is the local support provider.

Major Incident

- Involves a device or system containing private (see definition) or confidential data
- Threatens the business continuity of college, department, or university
- Affects multiple systems or servers
- Affects multiple systems or servers

Private Information

Private Information includes information that ASU is under legal or contractual obligation to protect such as FERPA, HIPAA or GLBA data. Examples would include Employee ID numbers, birth dates, location of assets, donors, gender, etc.

Security Incident Response Team (SIRT)

The ASU SIRT consists of individuals from various departments within ITS including Network Services, Server Administration, and IT Security. The SIRT reports to the VP of Information Technology Services who assigns the team to respond to an incident:

- Which requires coordination across multiple departments
- When a single department lacks the resources to respond
- When the local support provider requests assistance
- When the ISIRT determines involvement is necessary

Security Threat Profile

A threat profile is a straightforward and repeatable way to identify, organize, document and prioritize threats to your organization. A threat profile provides a way to map threats with the source of the event or events that are evidence of specific behavior.

Accountability

Failure to abide by the requirements of this policy and / or any procedures that are developed to implement this policy may result in disciplinary action. Some violations may constitute criminal offenses under local, state, and federal laws. Albany State University will carry out its responsibility to report such violations to the appropriate authorities.

Contacts

- Albany State University Chief Information Officer
- Albany State University Chief Information Security Officer

References

- ASU ITS Security Website: <https://www.asurams.edu/technology/information-security/>
- USGBOR Handbook: http://www.usg.edu/information_technology_handbook/section5
- SANS Institute: <http://www.sans.org>

Version History

Date	Version	Description
July 8, 2013	2.3	
August 11, 2015	2.4	Removed names from the positions in Contacts section

▶ Getting Started for Employees

▶ Getting Started for Students

▶ Personnel

▶ Project Management Office

▶ Accessing Campus WiFi

▶ Enterprise Reports – Argos

▶ Banner Student Information System

▶ Card Services

▶ Forms & Policies

▶ Info-Sec Anti-Virus

▶ Information Security Awareness Training Policy

▶ ITS Appropriate Use Policy

▶ ITS Email Policy

▶ ITS Incident Response

▶ ITS VPN Remote Access Policy

▶ Password Construction Guidelines

▶ Password Protection Standard

▶ ASK ITS Question Form

▶ General Use Computer Labs

▶ Help Desk

▶ Information Security

▶ IT Service Catalog

▶ VP of Information Technology Services and CIO

▶ New Department Fax Numbers

▶ New Department Phone Numbers



ASU East Campus

504 College Drive
Albany, GA 31705

Phone: (229) 500-2000

ASU West Campus

2400 Gillionville Rd
Albany, GA 31707



- Accreditation
- ASU Careers
- Maps
- Students

- Campus Safety
- ASU Foundation
- Events
- Calendar
- Flickr Photos

- Request a Transcript
- ASU IT Help Desk
- Equal Employment Opportunity
- Ethics & Compliance Hotline
- Human Trafficking Notice

Info-Sec Anti-Virus

Contents

- Purpose
- Scope
- Terms
- Policy
- Introduction
- Standards
- Compliance
- Accountability
- Contacts
- References
- Version History

Purpose

To provide guideline for the use of Anti-Virus Software at Albany State University (ASU)

Scope

This policy applies to all students, faculty, and staff who have desktop, workstations and laptops/notebooks which are either physically or remotely connected to the Albany State University network. This policy also applies to contractors and temporary staff whose personal laptops will connect to the Albany State University network (if applicable).

Terms

Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software by examining (scanning) files to look for known viruses matching definitions in a virus dictionary and/or identifying suspicious behavior from any computer program which might indicate infection.

Policy

All student, faculty, and staff desktops, workstations and laptops/notebooks, running Windows or Macintosh operating systems, and which are either physically or remotely connected to the Albany State University network will have a passive anti-virus detection and removal application installed and active on those desktops, workstations and laptops/notebooks.

Introduction

The internal computers systems, networks and data repositories of Albany State University are critical resources of the University and must be protected against unauthorized access, malicious access, and disruption of service. Active measures are necessary to lessen the opportunity for such incidents. Rising frequency of security incidents involving network-attached devices significantly increases the probability of major disruptions to the internal computer systems of the University. Statistics indicate that a very large percentage of potentially damaging incidents can be avoided by the use of existing anti-virus detection and elimination procedures. Establishing policy centrally and issuing standards and utilities from a central authority allows for rapid incident response and continuous update of protection methods. In order to reduce the opportunity for introduction of viruses and Trojan Horses, all student, faculty, and staff desktops, workstations and laptops/notebooks, running Windows or Macintosh operating systems, and which are either physically or remotely connected to the Albany State University network will have a passive anti-virus detection and removal application installed and active on those desktops, workstations and laptops/notebooks. Users are responsible for ensuring that anti-virus files are kept up to date.

Standards

Faculty and Staff Employees: The University provides a site-wide license) Anti-Virus, which is available to all faculty and staff members. This application, when installed using OIT-provided instructions, allows for the least amount of interruption or activity required from end users. Installation should be configured for automatic scanning and automatic updates. Users who know of or expect interference between the anti-virus software and another application running on their workstations or laptops must contact the University Security Officer to evaluate and agree to a work around.

Individual users (including but not limited to students, guests, contractors, and temporary employees): Individual users must procure their own anti-virus software for use on a personal computer which will be connected to the ASU network. It is the responsibility of the individual user, in conjunction with their respective supervisor, to ensure that all University-owned computers on which they work have up-to-date anti-virus installed and configures.

Compliance

Faculty and Staff Employees:Vice-Presidents, Administrative Unit Directors, and Deans are responsible for monitoring compliance by their respective users with this policy and associated standards by:

- Directing administrators of Windows® and Macintosh® machines in their respective organizations that are provided by the University and connected to the University network to install approved anti-virus software
- Directing reviews of and action on, reports on compliance with this policy that are generated by Office of Information Technology

Individual users (including but not limited to students, guests, contractors, and temporary employees): Individual users must procure their own anti-virus software for use on a personal computer which will be connected to the ASU network. It is the responsibility of the individual user, in conjunction with their respective supervisor, to ensure that all University-owned computers on which they work have up-to-date anti-virus installed and configures.

Accountability

Violation of this policy may subject the user to sanctions, including the loss of computer and/or network access privileges, disciplinary action, suspension, termination of employment, dismissal from ASU, and/or legal action.

Contacts

- Albany State University Chief Information Officer
- Albany State University Chief Information Security Officer

References

- ASU ITS Security Website: <https://www.asurams.edu/information-security>
- USGBOR Handbook: http://www.usg.edu/information_technology_handbook/section5
- SANS Institute: <http://www.sans.org>

Version History

College and Departmental IT contacts will provide recommendations to ASU ITS for the development and revision of standards. ITS will forward recommendations for changes and rationales for the changes to the Campus Technology Committee for consideration of future funding. Instruction and assistance on installation and maintenance of anti-virus software will be developed and offered by College and Departmental IT contacts in coordination with ITS.

Date	Version	Description
April 14, 2007	1.0	First release
August 11, 2015	1.2	Removed vendor name for anti virus, was Symantec (Norton)

- ▶ Getting Started for Employees
- ▶ Getting Started for Students
- ▶ Personnel
- ▶ Project Management Office
- ▶ Accessing Campus WiFi
- ▶ Enterprise Reports – Argos
- ▶ Banner Student Information System
- ▶ Card Services
- ▶ Forms & Policies
 - ▶ Info-Sec Anti-Virus
 - ▶ Information Security Awareness Training Policy
 - ▶ ITS Appropriate Use Policy
 - ▶ ITS Email Policy
 - ▶ ITS Incident Response
 - ▶ ITS VPN Remote Access Policy
 - ▶ Password Construction Guidelines
 - ▶ Password Protection Standard
 - ▶ ASK ITS Question Form
- ▶ General Use Computer Labs
- ▶ Help Desk
- ▶ Information Security
- ▶ IT Service Catalog
- ▶ VP of Information Technology Services and CIO
- ▶ New Department Fax Numbers
- ▶ New Department Phone Numbers



ASU East Campus

504 College Drive
Albany, GA 31705
Phone: (229) 500-2000

ASU West Campus

2400 Gillionville Rd
Albany, GA 31707

- Accreditation
- ASU Careers
- Maps
- Students

- Campus Safety
- ASU Foundation
- Events Calendar
- Flickr Photos

- Request a Transcript
- ASU IT Help Desk
- Equal Employment Opportunity
- Ethics & Compliance Hotline
- Human Trafficking Notice





CONFIDENTIALITY AND SECURITY ACCESS AGREEMENT

Albany State University has a legal and ethical responsibility to safeguard and to protect all confidential information. Confidential information includes employee information, student records, business information, financial information and other information relating to Albany State University. In the course of my employment and/or association with Albany State University, I understand that I will come into contact with confidential information. Confidential information may be spoken, written or electronic. The purpose of this agreement is to clarify my duties regarding confidential information. By signing this document I understand and agree to comply with Albany State University Policies & Procedures on Confidentiality and Security Access and the GA Computer Systems Protection Act, copies of which I have received for my records. In addition:

1. I agree not to disclose confidential information to others who do not have a need-to-know. Need-to-know is defined as that which is necessary for one to adequately perform one's specific job responsibilities as they relate to Albany State University.
2. I agree not to access or attempt to access any information, or utilize equipment, other than that which is required to do my job.
3. I agree not to discuss confidential information where others can overhear the conversation, e.g., in hallways, on elevators, in the cafeterias, at restaurants, at social events. I understand that it is not acceptable to discuss any confidential information inside or outside the organization, while on or off duty, even if specific names are not used, other than as permitted in this agreement.
4. I agree not to access any confidential information for any person who does not have a need-to-know.
5. I understand that my user name and password are the equivalent of my signature and that I am accountable for all entries and actions recorded during their use.
6. I agree that I will not disclose my user name and password to any person for any reason.
7. I agree not to access any confidential information using someone else's user name and password.
8. I agree not to send or take any confidential information outside Albany State University in any form (including PDAs) without authorization.
9. I agree not to make any additions, modifications or deletions to any confidential information without authorization.
10. I agree to respect the limitations and usage of the information system network and not to interfere unreasonably with the activity usage of other authorized persons.
11. I understand that my access to all computer systems may be monitored and audited without notice to me.
12. I agree to log out of any computer session opened under my user name and password prior to leaving any computer or terminal unattended.
13. I understand that if authorized to use Internet and/or email, I will use it only for authorized job responsibilities. Any misuse or abuse (e.g., pornographic material, chain letters, etc.) of these privileges could be grounds for disciplinary action.
14. I understand that I must participate in periodic training, as determined by Albany State University.
15. I agree to respect the ownership of proprietary software (e.g., I will not operate any unauthorized software on Albany State University computers or make unauthorized copies of any software for my own use).
16. I understand that confidential papers should be picked up as soon as possible from copiers, mail boxes, fax machines, printers and other publicly accessible locations. Confidential papers, reports, and computer printouts should be kept in a secure place. When they are no longer needed, confidential papers should be deposited in the document destruction bins to be destroyed.
17. I understand that my obligation under this agreement will continue after my termination of employment and/or association with Albany State University and that my privileges are subject to periodic review, revision, renewal and termination.
18. I agree to notify my supervisor or the Department of Human Resources immediately of any unauthorized access or use of confidential information or of violation by anyone of any of the rules above.

I understand that violation of this agreement may result in the following: Denial of access to University computer systems; Disciplinary action as stated in University Policies and Procedures up to and including termination; Penalties under State and Federal laws and regulations; Denial of entry into University facilities; Notification to State and/or national professional licensing departments or organizations; any combination of the above.

Full Name: _____ Signature: _____ Date: _____

Student Resources
Student Confidentiality
System Checker
GaVIEW FAQ's
Course Listings
Book Store
Web Registration Process
Contact Support Specialist

Use your official ASU username and password to log in to GaVIEW. (example: jsmit999). [Click here to reset your password.](#)

Preferred browsers for GaVIEW: [Chrome](#), [Firefox](#), Safari, Edge

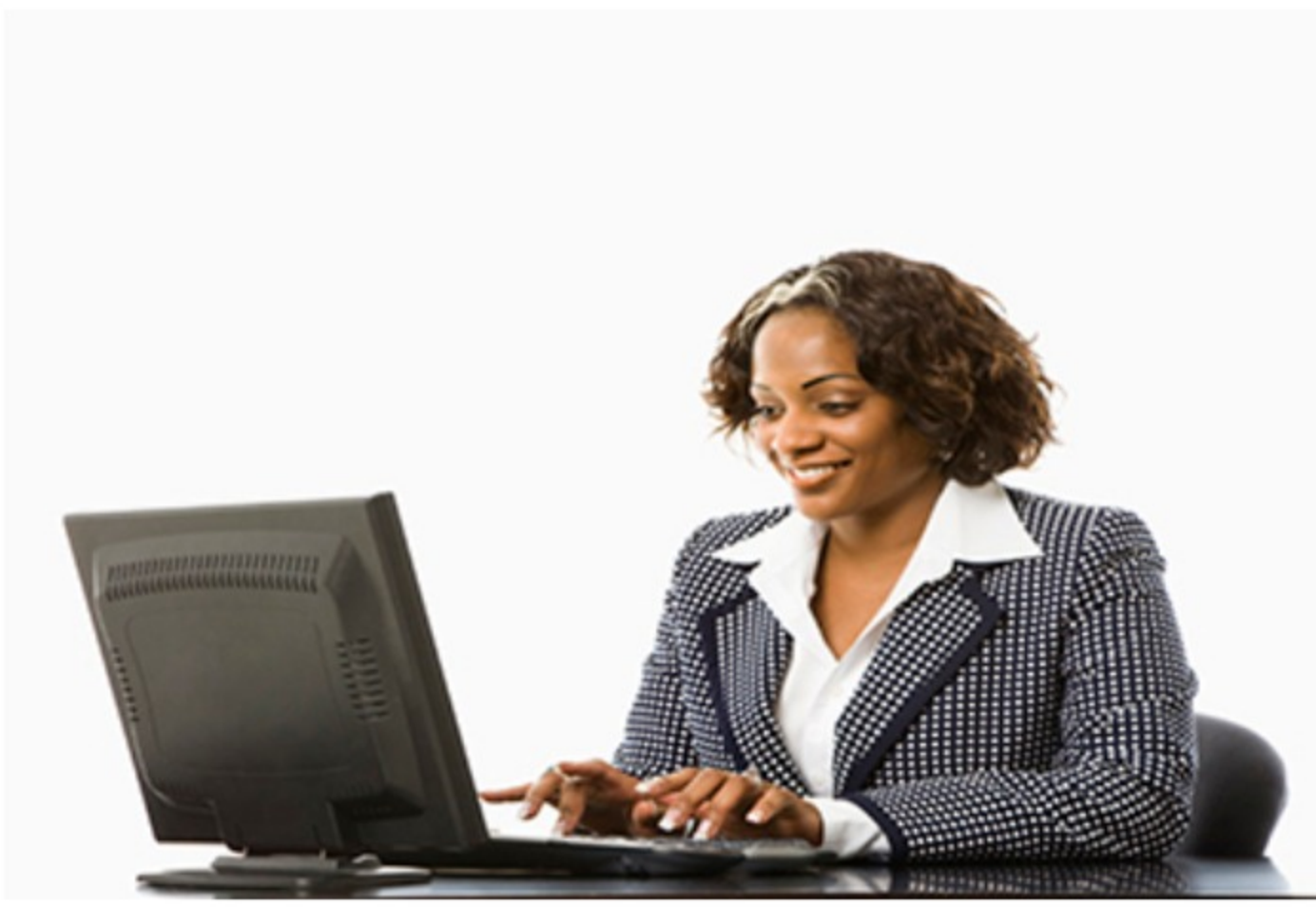
You are encouraged to upload a profile picture within the GaVIEW environment. [Please review the profile guidelines for pictures.](#)

[Click here to log in to eCore/eMajor classes](#)

Username *

Password *

Log In





Search...

Student Confidentiality

The Family Educational Rights and Privacy Act (FERPA)

Albany State University protects students' rights to privacy, and accords students all the rights under the federal law.

No one outside of the institution shall have access to, nor will the institution disclose any information from students' education records, without the written consent of students, except: to authorized personnel within the institution, to officials of other institutions in which students seek to enroll, to persons or organizations providing students financial aid, to accrediting agencies carrying out their accreditation function, to persons in compliance with a judicial order and to persons in an emergency in order to protect the health or safety of students or other persons. All of these exceptions are permitted under the Act.

ASU is fully committed to ensuring the privacy and protection of personal information of all student, including those enrolled in distance learning program, and does not share personal information gathered from distance education and/or on-campus/residential students. However, in some cases, the University may be compelled by the Open Records law to release information, as outlined in the Policies and Procedures for Responding to **Open Records Requests**.

According to FERPA student rights include:

1. Right of Inspection of Records
2. Right to challenge records believed to be inaccurate
3. Right to consent to disclosure of personally identifiable records (with exceptions)
4. Right to file complaints of alleged violations of the aforementioned rights.

Students who feel that their FERPA rights have been violated may file a formal complaint with the Office of the Registrar. The complaint must be submitted in writing to the Office of the Registrar at Albany State University's standard mailing address.

If a student feels their FERPA rights were violated by the AS&R personnel a complaint may be filed to the Office of the Provost, Academic Affairs.

To review further information, visit or contact the Office of the Registrar at Ram Central West (C Building). Or, visit the Web site of the **Department of Education FERPA**.

RETENTION OF STUDENT ACADEMIC RECORDS (COMMONLY REFERRED TO AS EDUCATION RECORDS):

The retention period for student academic records is permanent.

ASU FERPA AUTHORIZATION FORM

FERPA Authorization Form

▸ Class Schedules

▸ Commencement

▸ Final Exams Schedule

▸ Forms

▸ Internal Transfer Students

▸ Re-admission

▸ Registrar FAQ

▸ Student Academic Calendar

▸ Student Confidentiality

▸ Transfer Students

▸ Transcript Information

▸ Tuition Waivers



ASU East Campus
504 College Drive
Albany, GA 31705
Phone: (229) 500-2000

ASU West Campus
2400 Gillionville Rd
Albany, GA 31707



- Accreditation
- ASU Careers
- Maps
- Students

- Campus Safety
- ASU Foundation
- Events Calendar
- Flickr Photos

- Request a Transcript
- ASU IT Help Desk
- Equal Employment Opportunity
- Ethics & Compliance Hotline
- Human Trafficking Notice

Courses

Distance Learning Courses

Categories

Select a Subject:

ACCT

Accounting

ALHE

Allied Health

ANTH

Anthropology

ARTS

College of Arts & Humanities

ASU

ASU First Year Experience/Foundations of College Success

BIOL

Biology

BUSA

Business Administration

CHEM

Chemistry

COMM

Communications

COPR

- ACCT 2101 - Principles of Accounting I
- ACCT 2102 - Principles of Accounting II
- ACCT 4111 - Auditing I and Assurance Services
- ACCT 6101 - Accounting Analysis for Decision Making
- ACCT 6102 - Mangerial/Cost Accounting
- ACCT 6112 - Advance Auditing I
- ACCT 6131 - Advanced Accounting I
- ACCT 6141 - Municipal Accounting



ASU East Campus

504 College Drive

Albany, GA 31705

Phone: (229) 500-2000

ASU West Campus

2400 Gillionville Rd

Albany, GA 31707



- Accreditation
 - ASU Careers
 - Maps
 - Students
- Campus Safety
 - ASU Foundation
 - Events Calendar
 - Flickr Photos
- Request a Transcript
 - ASU IT Help Desk
 - Equal Employment Opportunity
 - Ethics & Compliance Hotline
 - Human Trafficking Notice

Hines, Domonique R.

Subject: Ga/View/ Email AM
Location: ASU Online

Start: Mon 7/29/2019 9:00 AM
End: Mon 7/29/2019 9:30 AM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Williams, Denata N.
Required Attendees: Hines, Domonique R.

Communication: GaView/Email Access

Subject: Albany State University Orientation Quiz Fall 2019 Information- IMPORTANT PLEASE REVIEW ENTIRE EMAIL

Don't forget to SCROLL to see all of the important information!

Good morning!

We are excited that you have registered for Fall term courses with Albany State University. To ensure that you are ready for the first day of class – **Monday, August 19, 2019** – please make sure that you have completed the following:

1. Ensure that you have access to your Office 365 ASU email. To do that please follow the directions found here: [Getting Started for Students](#)

Please remember:

If you are a **CONTINUING STUDENT**: You may need to reset your Office 365 email password and then use that to log into GaVIEW. Be sure to log out of Office 365 entirely and then click “use a different login” – enter your new ASU username and be sure to include the @students.asurams.edu. (When entering your username for GaVIEW it is simply the username without the @students.)

If you are a **NEW STUDENT**: You need to set up your Office 365 email for your ASU rams email account. Remember that when entering your username for email you include the @students.asurams.edu – when entering your username for GaVIEW it is simply the username without the @students.... Once you have set up your email or reset your password, go to the GaVIEW log in page <https://albanystate.view.usg.edu/d2l/login> and enter your username (remember DO NOT add @students.asurams.edu) and the password that you use to access the ASU email in Office 365.

If you have followed all of the above instructions and still cannot access your email, please contact helpdesk@asurams.edu or call 229-500-4357

2. **Once you have successfully accessed your ASU Office 365 email**, you will be ready to access GaVIEW, Albany State's learning system for online courses and face-to-face support content. To access GaVIEW, go to www.asurams.edu, click Students, click “online courses GaVIEW – Distance Learning” – If you cannot access the GaVIEW system, please contact asuonline@asurams.edu – but remember **if you are a NEW STUDENT – YOUR ACCESS WILL NOT BE AVAILABLE UNTIL 12:01 A.M. August 19, 2019.** When

sending the email you MUST include your complete name, student ID number, and good contact information for priority service. Once you have successfully logged in complete the Orientation Completion Quiz (if you have not done so previously).

3. Still having issues accessing GaVIEW? Email asuonline@asurams.edu from your Office 365 email. If you cannot access your Office 365 email, please email helpdesk@asurams.edu or call 229-500-4357, remember in the email to include your complete name, student ID number, and good contact information.
4. Don't forget, as an online student you have access to student support services such as the [online writing center](#), [online math center](#), Smarthinking tutoring services and more – check out the [Distance Learning website](#) for more information and to find the contact information for your [Distance Learning Support Specialist](#).

See you Online!

The ASU Distance Learning Team
asuonline@asurams.edu or 229-500-2907 or
<https://www.asurams.edu/Academics/asuonline/>



Search...


[HOME](#) [ABOUT ▾](#) [ACADEMICS ▾](#) [ADMINISTRATION ▾](#) [APPLY](#) [STUDENT LIFE](#) [STUDENTS](#) [DONATE](#)
[ATHLETICS](#)
[HOME](#) > [FISCAL AFFAIRS HOME](#) > [STUDENT ACCOUNTS](#) > [TUITION & FEES PAYMENT](#) > [TUITION & FEES SCHEDULES](#)

Tuition & Fees Schedules

Payment Information

[2017-2018 Tuition and Fees Schedule](#)
[2018-2019 Tuition and Fees Schedule](#)
[2019-2020 In State Tuition and Fees Schedule](#)
[2019-2020 Out of State Tuition and Fees Schedule](#)
[▶ Tuition & Fees Schedules](#)
[▶ Payment Information](#)
[▶ Nelnet Payment Plan](#)
[▶ International Fees](#)
[▶ Frequently Asked Questions](#)


ASU East Campus

504 College Drive
Albany, GA 31705

Phone: (229) 500-2000

ASU West Campus

2400 Gillionville Rd
Albany, GA 31707

- [Accreditation](#)
- [ASU Careers](#)
- [Maps](#)
- [Students](#)

- [Campus Safety](#)
- [ASU Foundation](#)
- [Events Calendar](#)
- [Flickr Photos](#)

- [Request a Transcript](#)
- [ASU IT Help Desk](#)
- [Equal Employment Opportunity](#)
- [Ethics & Compliance Hotline](#)
- [Human Trafficking Notice](#)



Effective Fall Semester 2019

*Unused Dining Dollars greater than the incentive amount for each plan are refundable at end of semester/term.

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
 College of Arts & Humanities
 ASU First Year
 Experience/Foundations of College Success
 Biology
 Business Administration
 Chemistry
 Communications
 Computer Processing
 Computer Science
 Computed Tomography
 Economics
 Education
 English
 eCore Class
 eCore Class
 French
 Geology
 Health Care Administration

[Print All Fees](#)

ASU 1101

First Year Experience/Pathway to Success

Some instructors may require one proctor exam for this course. Proctored Tests – This course requires 1 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
 College of Arts & Humanities
 ASU First Year
 Experience/Foundations of College Success
 Biology
 Business Administration
 Chemistry
 Communications
 Computer Processing
 Computer Science
 Computed Tomography
 Economics
 Education
 English
 eCore Class
 eCore Class
 French
 Geology
 Health Care Administration

[Print All Fees](#)

ACCT 2101 Principles of Accounting I

Proctored Tests – this course requires **4** proctored tests. Students living in the Albany/Cordele area may test at the testing center at Albany State University (East, West or Cordele campuses)– students who live outside the Albany area must arrange with their instructor for an approved proctoring site – off-site proctor approval forms are found within your course. Albany State University's off-site proctor policy will be found in the course. **(Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)**

Instructor Bagley Classes: Extensive use of EXCEL spreadsheets and formulas.

ACCT 2102 Principles of Accounting II

Proctored Tests – this course requires **4** proctored tests. Students living in the Albany/Cordele area may test at the testing center at Albany State University (East, West or Cordele campuses)– students who live outside the Albany area must arrange with their instructor for an approved proctoring site – off-site proctor approval forms are found within your course. Albany State University's off-site proctor policy will be found in the course as well. **(Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)**

Instructor Bagley Classes: Extensive use of EXCEL spreadsheets and formulas.

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

BIOL 1100K Human Anatomy and Physiology for the Health Care Professional

Proctored Tests – This course requires **5** proctored tests. Students may test at Albany State University's testing centers (East, West, or Cordele Campuses) or online through Proctor U. Testing through Proctor U requires a computer (not a mobile device) with a webcam and microphone.

There is an additional \$40 Science Fee associated with this course.

BIOL 1110K Introduction to Environmental Biology

Proctored Tests – This course requires 1 proctored tests. Students may test at Albany State's Albany or Cordele campuses or online through Proctor U. Testing through Proctor U requires a computer (not a mobile device) with a webcam and microphone.

BIOL 2107K Principles of Biology I

Proctored Tests – this course requires **5** proctored tests. Students living in the Albany/Cordele area may test at the testing center at Albany State University (East, West or Cordele campuses) – students who live outside the Albany area must arrange with their instructor for an approved proctoring site – off-site proctor approval forms are found within your course. Albany State University's off-site proctor policy may be found in the course. This course has more stringent standards than Albany State University's minimum requirements. Libraries, K-12 schools, and administrators are routinely denied. **(Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)**

Biology LabPak: BK-2A w/lab manual purchased at LabPak online at www.athomescience.com/index.htm (\$199.00 – double check website for price variance)

Access to 600X microscope – may also be purchased at LabPak online at www.athomescience.com/index.htm (\$112.00 double check website for price variance)

There is an additional \$20 Lab Science Fee associated with this course.

BIOL 2108K Principles of Biology II

Proctored Tests – this course requires **5** proctored tests. Students living in the Albany/Cordele area may test at the testing center at Albany State University (East, West or Cordele Campuses) – students who live outside the Albany area must arrange with their instructor for an approved proctoring site – off-site proctor approval forms are found within your course. Albany State University's off-site proctor policy may be found in the course. This course has more stringent standards than Albany State University's minimum requirements. Libraries, K-12 schools, and administrators are routinely denied. **(Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)**

Biology LabPak: BK-2B w/lab manual purchased at LabPak online at www.athomescience.com/index.htm (\$219.00 – double check website for price variance)

Access to 600X microscope – may also be purchased at LabPak online at www.athomescience.com/index.htm (\$112.00– double check website for price variance)

There is an additional \$20 Lab Science Fee associated with this course.

BIOL 2411K Human Anatomy and Physiology I

Proctored Tests – This course requires **5** proctored tests. Students may test at Albany State University's testing centers (East, West, or Cordele Campuses) or online through Proctor U. Testing through Proctor U requires a computer (not a mobile device) with a webcam and microphone.

There is an additional \$40 Science Fee associated with this course.

BIOL 2412K Human Anatomy and Physiology II

Proctored Tests – This course requires **5** proctored tests. Students may test at Albany State University's testing centers (East, West, or Cordele Campuses) or online through Proctor U. Testing through Proctor U requires a computer (not a mobile device) with a webcam and microphone.

There is an additional \$40 Science Fee associated with this course.

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
 College of Arts & Humanities
 ASU First Year
 Experience/Foundations of College Success
 Biology
 Business Administration
 Chemistry
 Communications
 Computer Processing
 Computer Science
 Computed Tomography
 Economics
 Education
 English
 eCore Class
 eCore Class
 French
 Geology
 Health Care Administration

[Print All Fees](#)

BUSA 1105 Introduction to Business

Instructor YATES: Proctored Tests – This course requires 1 proctored tests. Students may test at Albany State's Albany or Cordele campuses or online through Proctor U. Testing through Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
 College of Arts & Humanities
 ASU First Year
 Experience/Foundations of College Success
 Biology
 Business Administration
 Chemistry
 Communications
 Computer Processing
 Computer Science
 Computed Tomography
 Economics
 Education
 English
 eCore Class
 eCore Class
 French
 Geology
 Health Care Administration

[Print All Fees](#)

CHEM 1211K Principles of Chemistry I

Proctored Tests – **Instructor Mutisya requires 4 proctor exams other instructors require 2**. This course requires 4 - 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Chemistry LabPak: *First Semester Chemistry for Science Majors* online at <http://holscience.com/orders/> (\$225.00 – please check website for possible price variances)

CHEM 1212K Principles of Chemistry II

Proctored Tests – **Instructor Mutisya requires 4 proctor exams other instructors require 2**. This course requires 4 - 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Chemistry LabPak: *Second Semester Chemistry II for Science Majors* online at <http://holscience.com/orders/> (\$260.00 – please check website for possible price variances)

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting

College of Arts & Humanities

ASU First Year

Experience/Foundations of College Success

Biology

Business Administration

Chemistry

Communications

Computer Processing

Computer Science

Computed Tomography

Economics

Education

English

eCore Class

eCore Class

French

Geology

Health Care Administration

Print All Fees

ARTS 1100

Art Appreciation

• Instructor Carter Only: This course requires students to visit in person (not virtually) an art/history museum or art exhibit in the student's local area.

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

COMM 1000 Cultural Diversity in Communication

- JAVA, Chrome Browser (preferred)
- Audacity software (a free voice-recording program)
- Digital video recording device (i.e.: webcam - NO Mobile Devices)
- Computer microphone
- Microsoft PowerPoint
- A computer with Microsoft Word and PowerPoint
- This class requires up to two one-hour synchronous meetings which will be conducted via web technologies. These meetings will allow you to present up to two live speeches. Your instructor will post optional times for each speech at the start of the term.

COMM 1100 Human Communications

- JAVA, Chrome Browser (preferred)
- Audacity software (a free voice-recording program)
- Digital video recording device (i.e.: webcam - NO Mobile Devices)
- Computer microphone
- Microsoft PowerPoint
- A computer with Microsoft Word and PowerPoint
- This class requires up to two one-hour synchronous meetings which will be conducted via web technologies. These meetings will allow you to present up to two live speeches. Your instructor will post optional times for each speech at the start of the term.

COMM 1110 Public Speaking

- JAVA, Chrome Browser (preferred)
- Audacity software (a free voice-recording program)
- Digital video recording device (i.e.: webcam - NO Mobile Devices)
- Computer microphone
- Microsoft PowerPoint
- A computer with Microsoft Word and PowerPoint
- This class requires up to two one-hour synchronous meetings which will be conducted via web technologies. These meetings will allow you to present up to two live speeches. Your instructor will post optional times for each speech at the start of the term.

COMM 1111 Issues in Argumentation and Advocacy

- JAVA, Chrome Browser (preferred)
- Audacity software (a free voice-recording program)
- Digital video recording device (i.e.: webcam - NO Mobile Devices)
- Computer microphone
- Microsoft PowerPoint
- A computer with Microsoft Word and PowerPoint
- This class requires up to two one-hour synchronous meetings which will be conducted via web technologies. These meetings will allow you to present up to two live speeches. Your instructor will post optional times for each speech at the start of the term.

COMM 2105 Introduction to Interpersonal Communication Online

- JAVA, Chrome Browser (preferred)
- Audacity software (a free voice-recording program)
- Digital video recording device (i.e.: webcam - NO Mobile Devices)
- Computer microphone
- Microsoft PowerPoint
- A computer with Microsoft Word and PowerPoint
- This class requires up to two one-hour synchronous meetings which will be conducted via web technologies. These meetings will allow you to present up to two live speeches. Your instructor will post optional times for each speech at the start of the term.

COMM 2220 Introduction to Small Group Communication

- JAVA, Chrome Browser (preferred)
- Audacity software (a free voice-recording program)
- Digital video recording device (i.e.: webcam - NO Mobile Devices)
- Computer microphone
- Microsoft PowerPoint
- A computer with Microsoft Word and PowerPoint
- This class requires up to two one-hour synchronous meetings which will be conducted via web technologies. These meetings will allow you to present up to two live speeches. Your

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting

College of Arts & Humanities

ASU First Year

Experience/Foundations of College Success

Biology

Business Administration

Chemistry

Communications

Computer Processing

Computer Science

Computed Tomography

Economics

Education

English

eCore Class

eCore Class

French

Geology

Health Care Administration

Print All Fees

CTCP 2140	<div>Clinical Applications I</div> <div>DCHP Background Check Fee: \$50.00</div> <div>Computed Tomography Insurance Fee: \$18.00</div>
-----------	--

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting

College of Arts & Humanities

ASU First Year

Experience/Foundations of College Success

Biology

Business Administration

Chemistry

Communications

Computer Processing

Computer Science

Computed Tomography

Economics

Education

English

eCore Class

eCore Class

French

Geology

Health Care Administration

Print All Fees

COPR 1122	Introduction to Instructional Technology Requires at least one synchronous class meeting.
-----------	--

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
 College of Arts & Humanities
 ASU First Year
 Experience/Foundations of College Success
 Biology
 Business Administration
 Chemistry
 Communications
 Computer Processing
 Computer Science
 Computed Tomography
 Economics
 Education
 English
 eCore Class
 eCore Class
 French
 Geology
 Health Care Administration

[Print All Fees](#)

CSCI 2500

Discrete Structures

Proctored Tests – This course requires 3 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Courses with Additional Costs

Course with Additional Costs

Course Areas
Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

ECON 2105 Principles of Macroeconomics

Instructor AARON JOHNSON: Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele), online through Proctor U, or by arranging with the instructor to find a local proctor site. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

ECON 2106 Principles of Microeconomics

Instructor AARON JOHNSON: Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele), online through Proctor U, or by arranging with the instructor to find a local proctor site. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Courses with Additional Costs

Course with Additional Costs

Course Areas
Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

Print All Fees

EDUC 2110	Invest Critical/Contemporary Issues This course requires the completion of 10 hours of field experience, which is obtained through classroom observation of state-certified teachers during the semester the course is taken.
EDUC 2120	Exploring Socio-Cultural Perspective This course requires the completion of 10 hours of field experience, which is obtained through classroom observation of state-certified teachers during the semester the course is taken.
EDUC 2130	Exploring Teaching and Learning This course requires the completion of 10 hours of field experience, which is obtained through classroom observation of state-certified teachers during the semester the course is taken.

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

Print All Fees

ENGL 3405	Professional and Technical Writing - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
-----------	--

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
 College of Arts & Humanities
 ASU First Year
 Experience/Foundations of College Success
 Biology
 Business Administration
 Chemistry
 Communications
 Computer Processing
 Computer Science
 Computed Tomography
 Economics
 Education
 English
 eCore Class
 eCore Class
 French
 Geology
 Health Care Administration

[Print All Fees](#)

FREN 1001 Elementary French I

Proctored Tests – this course requires **2** proctored tests. Students living in the Albany area may test at the testing center at Albany State University – students who live outside the Albany area must arrange with their instructor for an approved proctoring site – off-site proctor approval forms are found within your course. **(Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)**

FREN 1002 Elementary French II

Proctored Tests – this course requires **2** proctored tests. Students living in the Albany area may test at the testing center at Albany State University – students who live outside the Albany area must arrange with their instructor for an approved proctoring site – off-site proctor approval forms are found within your course. **(Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)**

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting

College of Arts & Humanities

ASU First Year

Experience/Foundations of College Success

Biology

Business Administration

Chemistry

Communications

Computer Processing

Computer Science

Computed Tomography

Economics

Education

English

eCore Class

eCore Class

French

Geology

Health Care Administration

Print All Fees

GEOL 1011K	Introductory Geosciences I This is an eCore course - tuition is \$169 per credit hour.
------------	---



ASU East Campus
 504 College Drive
 Albany, GA 31705
 Phone: (229) 500-2000

ASU West Campus
 2400 Gillionville Rd
 Albany, GA 31707



- Accreditation
 - ASU Careers
 - Maps
 - Students
 - Campus Safety
 - ASU Foundation
 - Events Calendar
 - Flickr Photos
 - Request a Transcript
 - ASU IT Help Desk
 - Equal Employment Opportunity
 - Ethics & Compliance Hotline
 - Human Trafficking Notice

Courses with Additional Costs

Course with Additional Costs

Course Areas
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration
Health and Human Performance
History
Health Information Technology
Human Services Technology
Integrated Science
Japanese

[Print All Fees](#)

HITE 2150	Coding I Proctored Tests – this course requires 1 proctored tests. Students living in the Albany area may test at the testing center at Albany State University – students who live outside the Albany area must arrange with their instructor for an approved proctoring site – off-site proctor approval forms are found within your course. (Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)
HITE 2160	Coding II Insurance Fee \$18.00
HITE 2170	Advance Coding and Reimbursement • DCHP Background Check: \$50.00
HITE 2600	Professional Practice I Insurance Fee: \$18.00
HITE 2745	Abstracting Principles I Allied Health Background Check: \$49.50
HITE 2746	Abstracting Principles II Health Information Tech Insurance: \$17.50

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

HEDP 1163 Personal Health

Proctored tests required for the following instructors only: Nancy Abraham and Jane Kelly

Proctored Tests – This course may require 1 proctored test online with Proctor U. Testing through Proctor U requires **a computer (not a mobile device) with a webcam and microphone.**

(Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)

HEDP 1164 Stress Management

Proctored tests required for the following instructors only: Nancy Abraham

Proctored Tests – This course requires 1 proctored test online with Proctor U. Testing through Proctor U requires **a computer (not a mobile device) with a webcam and microphone.**

(Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)

HEDP 1165 Mental Health

Proctored tests required for the following instructors only: Nancy Abraham

Proctored Tests – This course requires 1 proctored test online with Proctor U. Testing through Proctor U requires **a computer (not a mobile device) with a webcam and microphone.**

(Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)

Courses with Additional Costs

Course with Additional Costs

Course Areas
Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

HADM 3301	Health Care Organizations - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
HADM 3302	Health Care Economics - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
HADM 3303	US Health Care Systems - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
HADM 3304	Health Care Communication - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
HADM 4301	Healthcare Administration - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
HADM 4401	Health Care Compliance - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
HADM 4402	Health Information Management - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

HIST 1111 Survey of World History I

Instructor Sharon Sewell Only: Proctored Tests – This course requires 4 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

HIST 1112 Survey of World History II

Instructor Sharon Sewell and Mcdermott Only: Proctored Tests – This course requires 4 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

HIST 2111 U.S. History Through 1877

Instructor McDermott Requires: Proctored Tests – This course requires 3 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

HIST 2112 History after 1877

Instructor McDermott: Proctored Tests – This course requires 3 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

HIST 3511 Modern Europe I

Instructor Sharon Sewell Only-Proctored Tests – This course requires 4 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

HUST 1110 Families and Other Systems

Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

HUST 2000 Group Theory and Process

- Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

HUST 2650 Applied Community Health

Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

HUST 2700 Understanding and Treating Addictions

Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone..

HUST 2750 Current Trends in Addiction and Mental Health

Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Natural Sciences (ISCI)

2019-2020 Catalog

Q Search Catalog

Graduate Catalog

Undergraduate Catalog

Introduction

History of Albany State University

Campus Resources

Facilities

Tobacco Policy

Institution Accreditations

The Albany State University Alumni Association

University Police Department

Admissions

Financial Aid

Academic Advising

Financial Information

Academic Affairs, Requirements/Regulations & Support Services

Academic Information

Student Affairs and Services

Student Complaint Procedures

Special Programs

Core Curriculum

Degree Programs

College of Arts and Sciences

College of Professional Studies

Darton College of Health Professions

Course Descriptions

Accounting (ACCT)

Allied Health (ALHE)

Elementary Arabic I (ARAB)

Art (ARTS)

Biology (BIOL)

Business Administration (BUSA)

Chemistry (CHEM)

Computed Tomography (CTCP)

Computer Info Systems Mgt (CISM)

Computer Processing (COPR)

Computer Science (CSCI)

Criminal Justice (CRJU)

Curriculum and Instruction (EDUC)

Dance (DANC)

Dental Hygiene (DHYG)

Diagnostic Medical Sonography (DMSP)

Early Childhood Education (ECEC)

Economics (ECON)

Educational Technology (ETEC)

Emergency Medical Services (EMTP)

Engineering (ENGR)

English (ENGL)

Environmental Science (ENVS)

Ethics (ETHI)

Finance (FINC)

Forensic Science (FOSC)

French (FREN)

Geography (GEOG)

German (GRMN)

Health (HLTH)

Health and Human Performance (HHUP)

Health and Physical Education (HEDP)

Health Information Technology (HITE)

Health Professions (COHP)

Healthcare Administration (HADM)

History (HIST)

Human Services Technology (HUST)

Japanese (JAPN)

Latin (LATN)

Leadership Development (LEAD)

Management (MGMT)

Management Health Care (MGHC)

Marketing (MKTG)

Mass Communications/ Public Speaking (COMM)

Mathematics (MATH)

Medical Laboratory Technology (MLTS)

Mgmt Information Systems Tech (MIST)

Middle Grades Education (MGED)

Military Science (MILS)

Modern Languages (MDLG)

Modern Languages (YORB)

Music (MUSC)

Mythology (MYTH)

Natural Sciences (ISCI)

Nursing (NURS)

Occupational Therapy Assistant (OTAS)

Office Admin Technology Conc (OATC)

Organizational Leadership (ORGL)

Paralegal (PARA)

Philosophy (PHIL)

Phlebotomy (PHLE)

Physical Education (PEDH)

Physical Science (PHSC)

Physical Therapist Assistant (PTAS)

Physics (PHYS)

Political Science (POLS)

Psychology (PSYC)

Public Administration (PADM)

Radiologic Technology (RADS)

Recreation (RECD)

Respiratory Care (RESP)

Science (SCIE)

Social Science (SSCI)

Social Work (SOWK)

Sociology (SOCI)

Spanish (SPAN)

Special Education (SPED)

Speech/Theatre (THEA)

Supply Chain & Logistics Mgmt (LOGM)

University Courses (ASU)

Wellness (WELL)

Faculty & Administrative Officers

Print Options

ISCI 2001. Life/Earth Science. (3 Credits)

An integrated overview of the core Life and Earth Science content covered in the K-5 Georgia Performance Standards. Topics include the Solar System, Earth Processes, Characteristics of Living Organisms, Biodiversity and the Natural History of Georgia. Students will gain conceptual understanding through Inquiry-Oriented, Activity-Based pedagogical strategies in order to have experience learning science content in the ways they will be expected to teach in the future.

ISCI 2002. Physical Science. (3 Credits)

COURSE DESCRIPTION: [ISCI 2002](#) – Physical Science... Activity – based Physical Science for Early Childhood Education Performance majors. Course addresses content covered by Standards (GPS) for K-5 grades. Georgia Performance. Prerequisite: Teacher Education major status.

ISCI 3002. Integrated Earth and Space Sci. (4 Credits)

The content in this course focuses on developing the earth science content that supports middle grades science standards-based content. The course incorporates inquiry, nature of science, characteristics of science and reading in the content area. Additional topics include a study of meteorology, oceanography, earth materials, the solar system, scientific views of the universe, the earth-sun-moon relationships, earth processes, and geologic time. The lab gives experiences which will include activities that further develop each of the topic areas. Candidates must earn a minimum grade of C to receive credit for this course in the program of study. Offered: Spring.

ISCI 3003. Integrated Concepts in Phy Sci. (4 Credits)

The content in this course focuses on developing the physical science content that supports middle grades science content standards. The topics include scientific inquiry, the nature of science, characteristics of science, the nature of matter, forms and transformations of energy, motion, gravity, waves, light, sound, electricity, magnetism, and relationship between force/mass/motion of objects. Candidates must earn a minimum grade of C to receive credit for this course in the program of study.

ISCI 3109. Integrated Concept in Biol Sci. (4 Credits)

The content in this course focuses on developing the life science content that supports middle grades science content standards. The topics covered include: characteristics of science, nature of science, inquiry, cells, cell structures, cell functions, composition and structure of DNA and RNA, asexual and sexual cellular reproduction, application of Mendel's laws, passing of genetic traits to successive generations, characteristics of single- and multi-celled organisms, adaptations, evolution, and ecosystems. Candidates must earn a minimum grade of C to receive credit for this course in the program of study.

Courses with Additional Costs

Course with Additional Costs

Course Areas
Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

JAPN 1001	Elementary Japanese I <ul style="list-style-type: none"> Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele).
JAPN 1002	Elementary Japanese II <p>Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele).</p>
JAPN 2002	Intermediate Japanese II <p>Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele).</p>

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

MATH 0987 Foundations for Quantitative Reasoning

Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

MATH 0989 Foundations for College Algebra

Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

MATH 1001 Quantitative Skills and Reasoning

Graphing calculator- TI-83 or TI84

Proctored Tests – This course requires 4 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

MATH 1111 College Algebra

Proctored Tests – This course requires 5 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Graphing calculator- TI-83 or TI84

MATH 1211 Calculus I

Proctored Tests – This course requires 5 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

MATH 1401 Intro to Statistics

- This is an eCore course - tuition is \$169 per credit hour
- Students must take the eCore Orientation quiz prior to registering for this class.
- All eCore classes require one-two proctored exams.
- This course requires a TI 83/84 calculator.

MATH 1501 Calculus

- This is an eCore course - tuition is \$169 per credit hour
- Students must take the eCore Orientation quiz prior to registering for this class.
- All eCore classes require one-two proctored exams.
- This course requires a TI 83/84 calculator.

MATH 2008 Foundations of Numbers and Operations

Proctored Tests – This course requires 4 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone..

Graphing Calculator- TI-83, 84, 85, or 86

MATH 2411 Introduction to Statistics

Proctored Tests – This course requires 5 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

MLTS 1161W Medical Lab Technology II
Allied Health Background Check Fee: \$49.50

MLTS 1182 Parasitology, Mycology and Virology
Proctored Tests –
Instructor Mary Hays: This course requires 5 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

MLTS 1340 Histology IV Clinical Rotation
Medical Lab Tech Insurance: \$18.50
Background Fee \$50.00

MLTS 1360 Histology VI
Medical Lab Tech Test Fee: \$215.00

MLTS 2010L Medical Laboratory Technology III LAB
Proctored Tests – this course requires **4** proctored tests. Students living in the Albany area may test at the testing center at Albany State University – students who live outside the Albany area must arrange with their instructor for an approved proctoring site – off-site proctor approval forms are found within your course. **(Proctored testing prices vary greatly from site to site; please check your local area for proctored costs for this course.)**

MLTS 2010W Medical Lab Technology III
Proctored Tests – This course requires **4** proctored tests. Students may test at Albany State University's testing centers (East, West, or Cordele Campuses) or online through Proctor U. Testing through Proctor U requires a computer (not a mobile device) with a webcam and microphone.

MLTS 2670 Seminars in Medical Laboratory Science
Medical Lab Tech Test Fee: \$185.00

Courses with Additional Costs

Course with Additional Costs

Course Areas
Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

Print All Fees

NURS 2111	Nursing Care of Women and Children (ASN)
	Insurance Fee \$18.00
	ATI Fee \$340.00

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
 College of Arts & Humanities
 ASU First Year
 Experience/Foundations of College Success
 Biology
 Business Administration
 Chemistry
 Communications
 Computer Processing
 Computer Science
 Computed Tomography
 Economics
 Education
 English
 eCore Class
 eCore Class
 French
 Geology
 Health Care Administration

[Print All Fees](#)

OATC 3150	Computer Operating Systems - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
OATC 3610	Web Design and Multimedia - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
OATC 3700	Desktop Publishing - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
OATC 4020	Virtual Office Technology - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
OATC 4160	Administrative Office Procedures - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
OATC 4810	Contemporary Skills - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.

Courses with Additional Costs

Course with Additional Costs

Course Areas
Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

ORGL 1100	Leadership in a Global Society This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 1500	Profiles of Leaders This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 2050	Communications for the Workplace - eMajor Only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 2100	Writing for Leadership This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 2601	Introduction to Public Administration This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 2800	Ethics and Leadership This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 2900	Program and Policy Evaluation for Leaders This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 3000	Reflective Seminar 1: Self as Learner - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 3050	Reflective Seminar II: Self in Context - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 3200	Introduction to Organizational Development - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 3400	Technology for Organizations - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 4000	Reflective Seminar III: Transforming Self - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 4690	Capstone Seminar in Organizational Leadership - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
ORGL 4900	Organizational Internship - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.


ASU East Campus

 504 College Drive
Albany, GA 31705

Phone: (229) 500-2000

ASU West Campus

 2400 Gillionville Rd
Albany, GA 31707

- [Accreditation](#)
- [ASU Careers](#)
- [Maps](#)
- [Students](#)

- [Campus Safety](#)
- [ASU Foundation](#)
- [Events Calendar](#)
- [Flickr Photos](#)

- [Request a Transcript](#)
- [ASU IT Help Desk](#)
- [Equal Employment Opportunity](#)
- [Ethics & Compliance Hotline](#)
- [Human Trafficking Notice](#)



Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
 College of Arts & Humanities
 ASU First Year
 Experience/Foundations of College Success
 Biology
 Business Administration
 Chemistry
 Communications
 Computer Processing
 Computer Science
 Computed Tomography
 Economics
 Education
 English
 eCore Class
 eCore Class
 French
 Geology
 Health Care Administration

[Print All Fees](#)

PHIL 4120

Professional Ethics - eMajor Only

This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.

Courses with Additional Costs

Course with Additional Costs

Course Areas
Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

PHSC 1011K Physical Science I

Lab Science Fee: \$20.00

Students may have to purchase sundry items. However, most students should have most of the items in their pantry or garage.

Instructor Mutisya: Proctored Tests – This course requires 4 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

PHSC 1012K Physical Science II

Instructor Mutisya: Proctored Tests – This course requires 4 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Courses with Additional Costs

Course with Additional Costs

Course Areas
Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

POLS 1101	American Government <ul style="list-style-type: none"> This course uses Open Educational Resources - no textbook purchase is required.
POLS 3201	Public Policy - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
POLS 4200	Principles of Public Administration - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
POLS 4202	Inter-organizational Behavior - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
POLS 4204	Public Finance - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.0.
POLS 4210	Modern Public Management - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
POLS 4215	Management of Non-Profit Organizations - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
POLS 4217	Grant Writing for Non-Profit Organizations - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
POLS 4218	Project Management in the Public Sector - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
POLS 4219	Human Resource Management - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
POLS 4220	Administrative Law and Government This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.
POLS 4221	Government Organization and Administrative Theory - eMajor only This course is part of the eMajor collaborate program degree. The tuition for this course is at the current eMajor rate.


ASU East Campus

 504 College Drive
Albany, GA 31705

ASU West Campus

 2400 Gillionville Rd
Albany, GA 31707

Phone: (229) 500-2000



- [Accreditation](#)
- [ASU Careers](#)
- [Maps](#)
- [Students](#)

- [Campus Safety](#)
- [ASU Foundation](#)
- [Events Calendar](#)
- [Flickr Photos](#)

- [Request a Transcript](#)
- [ASU IT Help Desk](#)
- [Equal Employment Opportunity](#)
- [Ethics & Compliance Hotline](#)
- [Human Trafficking Notice](#)

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
 College of Arts & Humanities
 ASU First Year
 Experience/Foundations of College Success
 Biology
 Business Administration
 Chemistry
 Communications
 Computer Processing
 Computer Science
 Computed Tomography
 Economics
 Education
 English
 eCore Class
 eCore Class
 French
 Geology
 Health Care Administration

[Print All Fees](#)

PSYC 1101 General Psychology

Instructor Reba Goodin Only: Proctored Tests – This course requires 1 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

PSYC 2225 Introduction to Abnormal Psychology

Proctored Tests – This course requires 1 proctored tests. Students may test at Albany State University's Albany or Cordele campuses or online through Proctor U. Testing through Proctor U requires a computer (not a mobile device) with a webcam and microphone.



ASU East Campus

504 College Drive
 Albany, GA 31705

Phone: (229) 500-2000

ASU West Campus

2400 Gillionville Rd
 Albany, GA 31707



- [Accreditation](#)
- [ASU Careers](#)
- [Maps](#)
- [Students](#)

- [Campus Safety](#)
- [ASU Foundation](#)
- [Events Calendar](#)
- [Flickr Photos](#)

- [Request a Transcript](#)
- [ASU IT Help Desk](#)
- [Equal Employment Opportunity](#)
- [Ethics & Compliance Hotline](#)
- [Human Trafficking Notice](#)

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

[Print All Fees](#)

SPAN 1001 Elementary Spanish I

- Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

SPAN 1002 Elementary Spanish II

- Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

SPAN 1050 Spanish for Health Care Professionals I

- Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

SPAN 1054 Spanish for Health Care Professionals II

- Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

SPAN 2001 Intermediate Spanish I

- Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

SPAN 2002 Intermediate Spanish II

- Proctored Tests – This course requires 2 proctored tests. Students may test at Albany State University campuses (East, West or Cordele) or online through Proctor U. Further information regarding proctored tests (including pricing structures for Proctor U) can be found within the course. Proctor U requires a computer (not a mobile device) with a webcam and microphone.

Courses with Additional Costs

Course with Additional Costs

Course Areas
Accounting
College of Arts & Humanities
ASU First Year
Experience/Foundations of College Success
Biology
Business Administration
Chemistry
Communications
Computer Processing
Computer Science
Computed Tomography
Economics
Education
English
eCore Class
eCore Class
French
Geology
Health Care Administration

Print All Fees

ETEC 1101	Electronic Technology in the Educational Environment
	This is an eCore class - tuition is at \$169 per credit hour.

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting

College of Arts & Humanities

ASU First Year

Experience/Foundations of College Success

Biology

Business Administration

Chemistry

Communications

Computer Processing

Computer Science

Computed Tomography

Economics

Education

English

eCore Class

eCore Class

French

Geology

Health Care Administration

Print All Fees

ENVS 2202	<div>Environmental Science</div> <div>This is an eCore class - tuition is \$169 per credit hour.</div>
-----------	--



ASU East Campus

504 College Drive

Albany, GA 31705

Phone: (229) 500-2000

ASU West Campus

2400 Gillionville Rd

Albany, GA 31707



- Accreditation

• ASU Careers

• Maps

• Students

• Campus Safety

• ASU Foundation

• Events Calendar

• Flickr Photos

• Request a Transcript

• ASU IT Help Desk

• Equal Employment Opportunity

• Ethics & Compliance Hotline

• Human Trafficking Notice

Courses with Additional Costs

Course with Additional Costs

Course Areas

Accounting

College of Arts & Humanities

ASU First Year

Experience/Foundations of College Success

Biology

Business Administration

Chemistry

Communications

Computer Processing

Computer Science

Computed Tomography

Economics

Education

English

eCore Class

eCore Class

French

Geology

Health Care Administration

Print All Fees

- ISCI 2002
- Physical Science
- Scientific calculator - suggested: Texas Instruments TI-30Xa
 - Materials for laboratory exercises (common household items, ruler, glue, etc. – and some grocery items, eggs, cabbage, etc.)
 - A small kitchen/diet scale that has “gram” measurements on it (<\$15)
 - A model rocket kit and Launchpad/controller (<\$25)
 - A computer with Microsoft Word and appropriate plug ins to successfully run GeorgiaView, See <https://albanystate.view.usg.edu/d2l/login> – click *System Checker*