# INFORMATION SECURITY POLICY

Information security is the protection of Angelina College's information resources, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

Definitions:
Information technology resources: Include, but are not limited to, the members of the IT department, software, hardware, systems, services, tools, budget, data, and documentation.

Information Owners: "A person(s) with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal", as defined in Texas Administrative Code 202.72 (TAC 202.72).

Information Custodian: "A department, agency, or third-party service provider responsible for implementing the information owner-defined controls and access to an information resource", as defined in Texas Administrative Code 202.72 (TAC 202.72).

Angelina College establishes the minimum standards and procedures for information security in accordance with the state's Information Security Standards for Institutions of Higher Education found in Title 1, Chapter 202, Texas Administrative Code (TAC 202). The Texas Department of Information Resources (DIR) has adopted a select number of controls that align with the NIST SP 800-53 control family catalog. Each Angelina College standard and procedure references the appropriate NIST SP 800-53/TCF control identifier.

## SECTION ONE: ACCESS CONTROL

Angelina College (AC) controls access to AC information technology resources by the implementation of an appropriate access control regulation to manage accounts and define the processes of authentication, authorization, administration, identification, monitoring, and termination of access rights.

**1.01** AC shall require an approval process prior to granting access to an information resource.

**1.02** Each person must be assigned a unique logon ID for the associated account for accountability purposes. Each logon ID will be granted permissions based on the least amount of privilege and job duties. Guest, visitor, contractors, or any other role-based accounts are to be used in very limited situations, must provide a designee for individual accountability, submitted to the IT Helpdesk, and be approved by IT Administrators.

> **1.02.1** Individuals are not permitted to use account credentials for which they are not the designated user; and

**1.02.2** Sharing user account credentials is prohibited.

**1.02.3** Any suspected unauthorized access of a user account should be reported immediately to the IT Helpdesk.

**1.03** Access authorization permissions shall be appropriately modified as an account holder's employment or job responsibilities change.

**1.04** User credentials that are associated with individuals who are no longer employed by, or associated with Angelina College must have their accounts disabled. If there is a need for the account to stay active, the information owner(s) or department head(s) must provide reasonable justification in writing to the IT Helpdesk. The request must be reviewed and approved by the AC IT Department.

**1.05** All new logon IDs that have not been accessed within a reasonable period of time from the date of creation will be disabled. The period of time is determined by risk management decisions established by Angelina College information owners and IT leadership.

**1.06** AC information owners shall:

**1.06.1** Make decisions regarding access to the AC data under their control. Account setup and modification require the approval of the requestor's supervisor and the relevant information owners(s).

**1.06.2** The Office of Information Technology (IT) is responsible for the activation of accounts, and in consultation with each user's supervisor and relevant information owners, the application of appropriate security classes under the principle of "least privileged access" to perform each user's business function.

**1.07** AC information custodians shall:

**1.07.1** Have a documented process for removing user accounts who are no longer authorized to have access to AC information resources.

**1.07.3** Have a documented process for modifying user accounts to accommodate situations such as name, accounting, and permission changes.

**1.07.4** Periodically review existing accounts for account management compliance.

**1.08** Confident between one state agency to another or from or between a state agency to a contractor or other third party shall be protected in accordance with the conditions imposed by the providing state agency at a minimum.

Document History:
Adopted: 02/2021
Reviewed: 08/2023

**1.09** Passwords

**1.09.1** The identity of users must be verified before providing them with account and password details. Face-to-Face authentication must be used for those accounts with privileged access.

**1.09.2** Users are provided an initial secure password for new accounts that must be changed at first login. Passwords will be communicated through an approved secure method during the onboarding and enrollment process.

**1.09.3** Regardless of the circumstances, an account's password must never be shared or revealed to anyone other than the authorized user of the account.

**1.09.4** The authorized user of each account is responsible for actions any other individual takes with that account's access through a shared or revealed password.

**1.09.5** All users are responsible for both the protection of their user account passwords and the data stored through their user account.

**1.09.6** Passwords must never be written down and left in a location easily accessible or visible to others.

**1.09.7** Individuals must never leave themselves logged into an application or system where someone else can unknowingly use their account.

**1.09.8** Passwords must meet the requirements outlined in the AC IT Standard Operating Procedures.

**1.10** Disabling/Revoking/Deleting Accounts

**1.10.1** Any account may be disabled, revoked, or deleted if it is determined the account has been compromised or misused, and an account disabled, revoked, or deleted pursuant to this section may only be reinstated at the direction of the Chief Information Officer (CIO), Information Security Officer (ISO), IT leadership, HR, or Vice President of Business Affairs and Internal Counsel.

**1.11** Remote Access

**1.11.1** Remote Access will not be granted until the user has requested and been granted authorization by the Vice President of Business Affairs & General Counsel of the College and has a completed and signed Remote Work Agreement with HR. Remote access will only be granted to Angelina College employees who need remote access for legitimate

business purposes. Faculty, agency, student, and part-time employees will not be granted remote access without special permission from the Vice President of Business Affairs & Internal Counsel.

**1.12** Network Access

Angelina College network provides wired and wireless access to information resources for devices.

**1.12.1** Prohibited Activities

Unauthorized use of the AC network is strictly prohibited. This includes, but is not limited to:

**1.12.1.1** Unauthorized access to network resources or attempts to bypass network security measures.

**1.12.1.2** Use of the network for any illegal activities.

**1.12.1.3** Unauthorized sharing or distribution of sensitive or confidential information.

**1.12.1.4** Deliberate introduction of malicious software or engaging in hacking activities.

**1.12.1.5** Interfering with the network infrastructure or disrupting network services.

**1.12.1.6** Use of the network for personal or non-work-related activities that consume excessive bandwidth or degrade network performance.

**1.12.1.7** Any other activities that violate applicable laws, regulations, or company policies.

**1.12.1.8** Any personal devices or hardware connected to the AC network that violates the Prohibited Activities outlined in this section will be confiscated and/or revoke access to the AC Network.

**1.13** Mobile Devices

**1.13.1** Mobile computing devices that access Angelina College information resources should be encrypted, patched/updated, and protected with antivirus software, and if appropriate, a personal firewall enabled.

**1.13.2** Angelina College may install remote wipe software on college owned devices.

**1.13.3** Angelina College data created and/or stored on personal devices or other non-College databases should be transferred to AC information resources as soon as feasible through an encrypted connection, such as Virtual Private Network (VPN), Wi-Fi Protected Access (WPA), or other secure encryption protocols.

**1.13.4** Angelina College data created and/or stored on a user's personal device or in databases that are not part of Angelina College information resources may be subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to AC Information Resources.

**1.13.5** Unattended mobile computing or storage devices containing Angelina College data, shall be kept physically secured.

**1.13.6** Personal owned user devices may be subject to Angelina College hardware and software compliance checks when accessing College information resources. Compliance checks may consist of, but are not limited to, minimum operating system, Antivirus, browser, security patches, firewall, and various software version requirements.

**1.13.7** Any protected or confidential data stored on mobile computing or storage devices shall be encrypted with an appropriate encryption algorithm.

**1.13.8** Mobile computing and storage devices containing Protected or Confidential data must be protected from unauthorized access by the use of passwords and/or multifactor authentication methods.

## SECTION TWO: INFORMATION TECHNOLOGY RESOURCES AND ACQUISITIONS

**2.01** Acquisition of information technology resources should be planned in advance. Justification for resources should be based on the mission, goals, and objectives of the College District and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

**2.02** All College District employees desiring to acquire information technology resources or to upgrade existing resources must complete and submit a technology request form to their respective supervisor. Small items should be ordered through the department/school's purchasing personnel. An updated list of small items can be requested from the IT Helpdesk.

**2.03** Each form submitted should be carefully reviewed for completeness and consistency with divisional goals and objectives before it is approved and signed by the submitter's supervisor. The completed and signed form can then be forwarded to the IT Helpdesk by the supervisor.

Document History:
Adopted: 02/2021
Reviewed: 08/2023

**2.03.01** All documentation for installation, maintenance, security information/certificates, or any kind of operation of the information technology resource must be submitted by the requester before processing of the request.

**2.03.02** Company contacts for support, maintenance, and billing must accompany the request.

**2.03.03** Requests that do not meet state, federal, or college security requirements will not be approved.

**2.04** IT should carefully review technology resources requested to determine compatibility with existing campus-wide information technology resources before forwarding the request for budget consideration and if required Board approval.

**2.05** All information technology resource requests will be prioritized based on the mission, goals, and operational needs of the college.

**2.06** Equipment checkout is available from the library. Equipment availability is limited and will be on a first come first serve basis.

**SECTION THREE: ACCEPTABLE USE OF RESOURCES**

**3.01** This policy governs the use of information technology resources by its students, faculty, staff, visitors, and contractors. This policy outlines the acceptable and prohibited uses of these resources and the consequences for violating this policy.

**3.01.1** Use information technology resources only for authorized purposes. College information technology resources must be used in a manner that complies with AC IT Standard Operating Procedures and State and Federal laws and regulations.

**3.01.2** Protect their user credentials from unauthorized use. Users are responsible for all activities associated with their user credentials or that originate from their computer/system.

**3.01.3** Use of Angelina College's computing and networking infrastructure by Angelina College employees unrelated to their Angelina College positions must be limited in both time and resources, and must not interfere in any way with Angelina College functions or employee duties.

**3.01.4** All software must be authorized by Angelina College IT prior to use. Users must not download, install, or run any software on systems except those installed and authorized by the Angelina College IT Department. Unauthorized software is subject to removal upon discovery.

**3.01.5** Uses that interfere with the proper functioning or the ability of others to make use of Angelina College's networks, computer systems, applications, and data resources are not permitted.

**3.01.6** Use of Angelina College computer resources for personal profit is not permitted.

**3.01.7** Files, images, emails, or documents which may cause legal action against or embarrassment to Angelina College, may not be sent, received, accessed in any format (i.e. auditory, verbal, or visual), downloaded, or stored on Angelina College information resources.

**3.01.8** All personal or Angelina College-owned messages, files, and documents, located on Angelina College information resources are owned by Angelina College, and may be subject to open records requests, and may be accessed in accordance with this standard.

**3.01.9** Use of network sniffers is prohibited. Exceptions shall be restricted to system administrators who must use such tools to solve network problems. Network sniffers may also be used by auditors or security officers in the performance of their duties.

**3.01.10** Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations.

**3.01.11** Anyone with disabilities that prevent them from using information resources should seek advice or help from the office of Student Support Services.

**3.01.12** Use of the College's wireless connection is entirely at the risk of the user, and Angelina College is not responsible for any loss of any information that may arise from the use of the wireless connection, nor is AC responsible for any loss, injury, or damages resulting from the use of the wireless connection.

**3.01.13** Anyone using AC information technology resources, including the network, is forewarned that there can be no expectation of privacy.

**3.01.14** Use of Angelina College's wireless network is governed by this Acceptable Use of Resources Policy and AC IT Standard Operating Procedures.

**3.01.15** The web page (angelina.edu), The Angelina College App, and any Angelina College social media sites are managed by the Marketing Department and reflect the mission, goals, and values of the college. Employees, students, and student organizations launching social media sites identified with Angelina College or intended primarily for use by A.C. students should receive prior approval from the Marketing Department.

Document History:
Adopted: 02/2021
Reviewed: 08/2023

## SECTION FOUR: ACCOUNTABILITY, AUDIT, AND RISK

The Angelina College ISO or designee, in coordination with information owners and custodians, shall develop, document, and disseminate a set of procedures that addresses the Audit and Accountability of information resources. These procedures should include purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

## SECTION FIVE: SECURITY AWARENESS AND TRAINING

All Angelina College personnel who use information resources must acknowledge they have read, understand, and will comply with the college's requirements regarding computer security standards and procedures.

**5.01** Security Awareness and Training

**5.01.1** All new personnel who use a college-owned computer for at least 25 percent of their required duties must complete an approved security awareness training prior to, or at least within 30 days of, being granted access to any Angelina College information resource.

**5.01.2** All Angelina College personnel who use a college-owned computer for at least 25 percent of their required duties must complete the college's security awareness training on an annual basis.

**5.01.3** Additional incidental training and acknowledgement may be required as determined by the Information Security Officer, or designee.

**5.01.4** Angelina College IT Department shall develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest as approved by the Information Security Officer (ISO), or designee.

**5.01.5** All consultants and contractors who access AC information systems shall be provided with sufficient training and supporting reference materials to allow them to properly protect Angelina College information resources.

## SECTION SIX: CONFIGURATION MANAGEMENT

Angelina College IT Department establishes the procedures for controlling modifications to hardware, software, firmware, and documentation to ensure the information resources are protected against improper modification before, during and after system implementation.

## SECTION SEVEN: CONTINGENCY PLANNING

Document History:
Adopted: 02/2021
Reviewed: 08/2023

Angelina College shall maintain a written Continuity of Operations Plan (COOP) that addresses information resources so that the effects of a disaster will be minimized, and the college will be able either to maintain or quickly resume mission-critical functions.

The Information Security Officer (ISO), and/or designee, in coordination with information resource owners, shall develop, document, and disseminate a set of controls that addresses the Contingency Planning of information resources. These controls should include purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

## SECTION EIGHT: IDENTIFICATION AND AUTHENTICATION

Angelina College establishes procedures for verifying the identity of a user, process, or device, as a prerequisite for granting access to AC information resources.

Unique identifiers will be assigned for each individual who has a business or educational need to access AC information resources. A standardized naming convention maintained by the Information Technology Department will ensure each user's identifier is unique. A method of authenticating the user's identifier will be enabled on each information resource.

Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, smartphone authenticator applications, or in the case of multifactor authentication, some combination thereof.

## SECTION NINE: INCIDENT RESPONSE

This policy describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of information resources. AC develops, disseminates, and periodically reviews/updates formal, documented procedures to facilitate the implementation of the Incident Response Policy.

**9.01** Incident Reporting

> **9.01.1** Requires personnel to report suspected security, privacy, and supply chain incidents to the IT Help Desk immediately (ithelpdesk@angelina.edu or (936)633-5208)); and
>
> **9.01.2** Reports security, privacy, and supply chain incident information to the Information Security Officer (ISO).

## SECTION TEN: MEDIA PROTECTION

The Information Security Officer (ISO), or designee, in coordination with information resource owners, shall, develop, document and disseminate a Media Protection Policy that:

**10.01** Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

**10.02** Is reviewed and updated periodically by the ISO, or designee.

## SECTION ELEVEN: PERSONNEL SECURITY

Angelina College ISO, or designee:

**11.01** Develops, documents, and disseminates to information owners and custodians:

> **11.01.1** A personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
>
> **11.01.2** Procedures to facilitate the implementation of the personnel security policy and associated personnel security controls; and

**11.02** Reviews and updates the current:

> **11.02.1** Personnel security policy biennially; and
>
> **11.02.2** Personnel security procedures annually.

## SECTION TWELVE: PHYSICAL AND ENVIRONMENTAL PROTECTION

Angelina College develops, documents, and disseminates procedures to facilitate the implementation of the Physical and Environmental Protection and associated controls.

In coordination with the Police and Maintenance departments, the IT department's physical spaces that contain AC information systems shall have controls in place to restrict physical access to only authorized personnel.

## SECTION THIRTEEN: PROGRAM MANAGEMENT

Angelina College develops, documents, and disseminates procedures to facilitate the implementation of the Program Management and associated controls.

**13.01** Develops and disseminates an organization-wide information security program plan that:

> **13.01.1** Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;

**13.01.2** Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;

**13.01.3** Reflects coordination among organizational entities responsible for the different aspects of information security (i.e., technical, physical, personnel); and

**13.01.4** Is approved by the Information Security Officer (ISO) with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations, and

**13.02** Reviews the organization-wide information security program annually;

**13.03** Updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and

**13.04** Protects the information security program plan from unauthorized disclosure and modification.

**SECTION FOURTEEN: RISK ASSESSMENT**

Angelina College develops, disseminates, and periodically reviews/updates formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

**14.01** Develop, document, and disseminate to information owners and custodians:

**14.01.1** A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

**14.01.2** Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls; and

**14.02** Review and update the Risk Assessment controls and procedures as necessary.

**SECTION FIFTEEN: SECURITY ASSESSMENT AND AUTHORIZATION**

Angelina College develops, documents, and disseminates procedures to facilitate the implementation of the Security Assessment and Authorization and associated controls.

**15.01** The Angelina College ISO or designee, in coordination with information resource owners and custodians, shall develop, document, and disseminate a set of procedures that addresses the Security Assessment and Authorization for information resources. These procedures should

include purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

**15.02** The ISO, or designee, shall review and update the Security Assessment and Authorization controls and procedures as necessary.

## SECTION SIXTEEN: SECURITY PLANNING

Angelina College develops, disseminates, and periodically reviews/updates formal, documented procedures to facilitate the implementation of the Planning Control policy and associated controls.

As specified in Texas Administrative Code §§ 202.23(a) and 202.73(a), the Angelina College Information Security Officer (ISO) shall directly report to the College President, at least annually, on the adequacy and effectiveness of information security policies, procedures, practices, and compliance with the requirements of Texas Administrative Code, Chapter 202, and

**16.01** Effectiveness of current information security program and status of key initiatives;

**16.02** Residual risks identified by Angelina College risk management process; and

**16.03** Angelina College information security requirements and requests.

## SECTION SEVENTEEN: SUPPLY CHAIN RISK MANAGEMENT

The scope of this policy applies to all information resources and systems that support the operations and assets of Angelina College, including those provided or managed by another agency, contractor, or other source. Services include, but are not limited to, those hosted by the college, outsourced, and cloud-based solutions. All information owners, custodians, users, contractors, and external service providers are responsible for adhering to these regulations and procedures. Information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures.

**17.01** Angelina College shall develop, document, and disseminate to all AC personnel, contractors, and users authorized to access AC information resource systems, or systems operated or maintained on behalf of the college, a supply chain risk management policy that:

> **17.01.1** Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
>
> **17.01.2** Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines;

**17.01.3** Authorizes the Information Security Officer (ISO) to manage the development, documentation, and dissemination of the IT supply chain management policy.

## SECTION EIGHTEEN: SYSTEM AND COMMUNICATION PROTECTION

This policy applies to all information owners and custodians, supervisors, managers, and others who are responsible for ensuring that all requirements of this control are satisfied.

**18.01** Develops, documents, and disseminates to information owners and custodians:

**18.01.1** A System and Communication Protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

**18.01.2** Procedures to facilitate the implementation of the System and Communication Protection policy and associated controls; and

**18.02** Reviews and updates the System and Communication Protection controls as necessary.

## SECTION NINETEEN: SYSTEM AND INFORMATION INTEGRITY

Angelina College develops, disseminates, and periodically reviews/updates formal, documented procedures to facilitate the implementation of the System and Information Integrity policy and associated controls.

The scope of this policy applies to all information resources owned or operated by Angelina College. All information resource owners, custodians, and users are responsible for adhering to these regulations and procedures. Information regarding roles, responsibilities, management commitment, and coordination among organizational entities are embedded within these procedures.

**19.01** The college Information Security Officer (ISO), or designee, in coordination with information resource owners, shall develop, document, and disseminate to the college a set of controls that addresses the System and Information Integrity of information resources.

**19.02** The ISO shall review and update the System and Information Integrity controls as necessary

## SECTION TWENTY: SYSTEM MAINTENANCE

The Information Security Officer (ISO), or designee, in coordination with information resource owners, shall, develop, document and disseminate a System Maintenance Policy that:

**20.01** Addresses purpose, scope, roles, responsibilities, management commitment, coordination among Angelina College entities, and compliance; and

**20.02** Is reviewed and updated periodically by the ISO, or designee.

## SECTION TWENTY ONE: VIOLATIONS

**22.01** Violations of this Regulation will be addressed in accordance with relevant college policies, including Regulation DHA-Discipline and Dismissal of Employees. The appropriate level of disciplinary action will be determined on an individual case-by-case basis by the appropriate executive or designee, with sanctions up to and including termination or expulsion depending upon the severity of the offense.

## RELATED DOCUMENTS

Texas Administrative Code (TAC) §202

NIST 800.53 Security and Privacy Controls for Information Systems and Organizations

Angelina College IT Standard Operating Procedures

The Vice President of Business Affairs is responsible for reviewing and updating this regulation. Policy reviews are made in accordance with the Office of Institutional Effectiveness Policy Tracking document.

Document History:
Adopted: 02/2021
Reviewed: 08/2023