Arkansas State University

Interim Policy On Information Technology Management, Security, and Privacy

4 March 2011

ARKANSAS STATE UNIVERSITY

ITERIM POLICY ON INFORMATION TECHNOLOGY MANAGEMENT, SECURITY, AND PRIVACY

EFFECTIVE DATE MARCH 4, 2011

This Information Security Manual applies to all personnel, students, agents, vendors, contractors, and other individuals or entities utilizing information technology, communications systems/networks, and data owned or operated by Arkansas State University.

Table of Contents

Policy Background 1

Impact Analysis 2

Policy Development Process 5

- General Policy 6
- Information Security Council 8
- Electronic Communications Privacy Act 9
- Data Protection and Classification 10
- Data Access Control 14
- Physical Security 16
- The Deployment and Use of Wireless Networks 18
- The Deployment and Use of Communication Networks 19
- Mobile Information Security 20
- Incident Reporting and Response 21
- Application Development and Management 22
- System Security 25

Definitions 27

Arkansas State University

Information Technology Management, Security, & Privacy

Policy Background

Information Technology Policies serve a number of purposes for the university community. These policies further the university's missions, educate the community about best practices in information technology, promote university-wide operational efficiencies, and reduce institutional risks. They also guide community members to help ensure compliance with applicable laws and regulations.

In July of 2009, Arkansas State University engaged a private audit firm to audit the general security posture of the university in regard to security/privacy policy and procedure. The policies set forth are proposed as a result of the findings and recommendations of the audit firm, at the request of the University System Office to update technology policies, and at the request of State of Arkansas Legislative Audit.

General Information Technology Policy is often found implicitly in the general policies of the university as well as in the university's statements and actions. However it is often helpful to have specific Information Technology Policies formally developed, approved, maintained and distributed in a consistent and timely manner. This practice helps to assure the success of university strategic initiatives, compliance with policy objectives, and establishes the accountability of operating units and individuals affected by each policy.

Specific Information Technology Policies should have broad applicability throughout the university. The Chief Information Officer (CIO) is responsible for University Information Technology Policies. The need for a new policy may become apparent or compelling in a number of ways. For example, the availability of new technology or changes in the ways campus community members work could drive the need. Any member of the university community may contact the Office of the CIO to discuss policy issues, suggest a need for a new policy, or comment on existing policy.

Specific policies are developed through a broadly based campus-wide consultative process, and in coordination with university Legal Counsel. Final policies are approved by the at the campus level by the Executive Council, after which the approved proposals are provided to the University System Office for Board of Trustee approval. Once approved, they are then maintained in the Information Technology Policy Repository.

Impact Analysis
For Proposed Policy
Information Technology Security & Privacy

Drafted: 14 October 2009
Revised: 14 May 2010
9 Dec 2010
Responsible Executive(s) (Dean or Vice Chancellor): Vice Chancellor, Finance & Administration
Responsible Office(s): Chief Information Officer

A. Background

1. General Information Technology policy and manual to replace Appropriate Use Policy.
2. Will serve as Board Approved, overarching policy to sanction specific computing and technology standards outlined in the manual at Arkansas State University.
3. The university must preserve its information technology resources and data, comply with applicable laws and regulations, and comply with other university policy regarding protection and preservation of data.

B. Policy Statement

1. ASU expects all individuals using information technology to take appropriate measures to protect institutional data.
2. Institutional data *(information)* is either A) an information asset entrusted to the Board of Trustees or B) an information asset that is the property of the Board of Trustees.
3. Policy statement should read:

"The Board of Trustees of Arkansas State University hereby approves this policy, known as the "General Policy on Information Security" in an effort to ensure use of owned and entrusted information resources and data assets, to minimize the liability and risks associated with these resources and assets, and to establish appropriate information management environment within Arkansas State University.

Hereby, Arkansas State University expects all information stewards, custodians, and persons who have access to and/or responsibilities for information resources and data assets of the institution to manage it according to the rules and policies regarding storage, disclosure, access, classification, and standards set forth in subsequent information security policies.

Hereby, Arkansas State University will adhere to the following attached, Information Technology Management, Security and Privacy Policy"

C. Reason for Policy

1. The security policy will build a framework that guides users and departments in specific procedures and technologies that address risks.
2. Each section of the manual address specific groups of vulnerabilities and areas of liability to the university.
3. In order to implement accepted best-practices and improve the financial audit report of the institution, it is necessary to implement certain policy constructs throughout the university.
4. Many statutory requirements call for agencies to have Board-approved policies in place that address areas of vulnerabilities.

D. Overview of Policy Content

1. The sections of the manual will each have a "bulletin". The bulletin will be the campus-specific information applicable to particular technologies and procedures to comply with the approved policy.
2. The Information Security Council will periodically recommend updates to technology bulletins. These updates will be approved by campus executive leadership on each campus.
3. The General Security Policy establishes the principle that every information technology device and data element is either an asset or entrusted asset of the institution (ultimately, the Board of Trustees).
4. The General Security Policy establishes the principle that every data asset aside from intellectual property is an asset of Arkansas State University and therefore subject to all security policies.
5. The General Security Policy establishes the principle that intellectual property and certain personal data are assets not belonging to, but rather entrusted to, Arkansas State University.
6. The General Security Policy requires all persons and units with access to information technology and data assets of the University to comply with institutional policy on it respective handling, treatment, and use.
7. The General Security Policy creates the categories of individuals, each with specific obligations regarding the security, use, privacy, and handling of information technology resources and data assets.

E. Consistency with University's Mission and Goals, Other Policies, and Related External Documents

1. Fair and Accurate Credit Transactions Act of 2003
2. Electronic Communications Privacy Act of 1986
3. Arkansas Freedom of Information Act
4. Health Insurance Privacy Policy of 1996
5. Family Education Rights and Privacy Act

F. Entities, Offices, and Other ASU Community Members Affected By This Policy

1. All connected persons and assets of Arkansas State University.
2. State all entities that apply:
    a. All entities of Arkansas State University
    b. All points of delivery and service of Arkansas State University

G. Impact on the University

1. Classification of all institutional data and information.
2. Certain protection mechanisms for data and respective systems and environments, depending on data classification.
3. Certain network systems will require replacement. This will be accomplished in the course of regular replacement and renewal.
4. Certain computer systems will require changes in security parameters.
5. Personnel training efforts must be assumed.
6. Certain protection mechanisms surrounding intellectual property and their respective environments will need to be implemented and/or reconfigured.
7. Acquisition of data security technology. Already underway.

H. Stakeholders Who Will Be Consulted in Developing This Policy

1. Legislative Audit
2. University Legal Counsel
3. Executive Counsel
4. University Business Owners Group
5. Faculty and Staff Senates
6. Shared Governance Bodies (as directed by EC)
7. Academic Dean's Council
8. Office of Human Resources
9. Subject Matter/Industry Experts (as needed)

I. System Changes Required

1. Network authentication from end-to-end. That is, the ability to know "who accesses what".
2. Role-based security. That is, rather than location-based security.
3. Some computer systems will require changes to security parameters and operating constructs.

J. Communications and Training Activities That Will Be Conducted To Build Awareness and Enable Implementation

1. Faculty, Staff will be required to engage in information security and privacy awareness training.
2. Regular promotional activities and communication efforts will be implemented to increase and maintain awareness of information privacy and security matters.

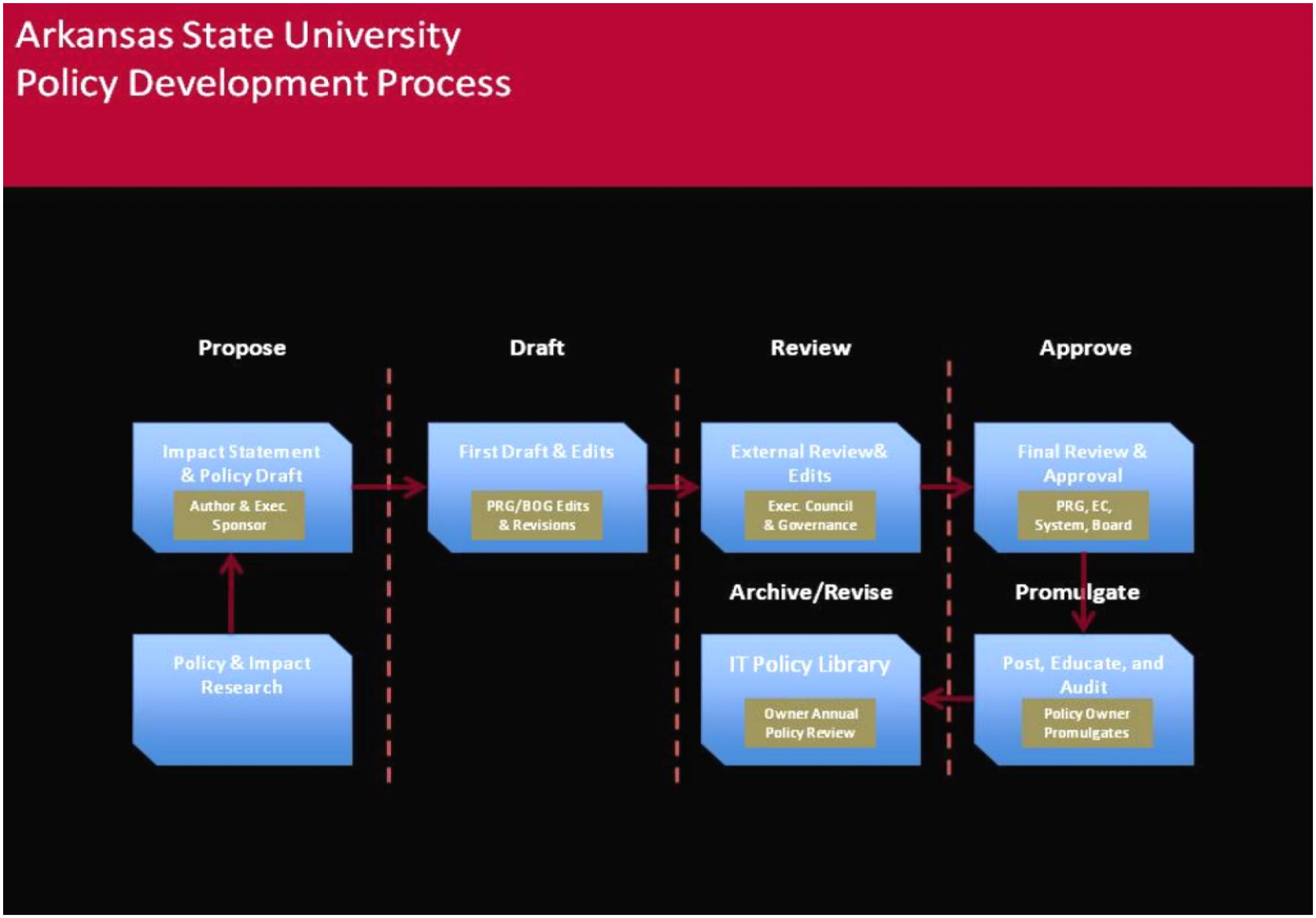
K. Compliance Mechanisms Existing or To Be Created

1. Policy will utilize existing faculty, staff, and student disciplinary procedures and mechanisms.

L. Timing Requirements for This Policy

1. Some aspects of this policy must be implemented in coordination with the institutional budgeting process.
2. Policy should be fully implemented by December 2011

Arkansas State University
Policy Development Process



GENERAL POLICY ON INFORMATION SECURITY [###.000]

This policy applies to all Faculty, Staff, Students, agents, vendors, contractors, and other individuals utilizing information technology, communications systems/networks, and data owned, operated by, or entrusted to Arkansas State University.

A. Policy Statement on General Information Security

The Board of Trustees of Arkansas State University hereby approves this policy, known as the "General Policy on Information Security" in an effort to ensure best use of entrusted information resources and data assets, to minimize the liability and risks associated with these resources and assets, and to establish an appropriate information management environment within all entities of Arkansas State University.

Hereby, Arkansas State University expects all information stewards, custodians, and persons who have access to and/or responsibilities for information resources and data assets of the institution to manage it according to the rules and policies regarding storage, disclosure, access, classification, and standards set forth in subsequent information security policies.

Hereby, Arkansas State University will adhere to the following attached, Information Technology Policies:

1. Information Security Council Policy [###.001]
2. Electronic Communications Privacy Act [###.002]
3. Data Protection and Classification [###.003]
4. Password Requirements [###.004]
5. Access Control Policy [###.005]
6. Physical Security Policy [###.006]
7. Wireless Security Policy [###.007]
8. Communications Network Security Policy [###.008]
9. Mobile Security Policy [###.009]
10. Incident Reporting & Response Policy [###.010]
11. Application Development Policy [###.011)
12. System Security Policy [###.013]

B. Policy Details

In order to manage information technology security comprehensively, this policy serves five major purposes.

1. It establishes the principle that every information technology device and data element is either an asset or entrusted asset of the institution, and subsequently under the authority of the Board of Trustees.
2. It establishes the principle that every data asset aside from intellectual property is an asset of Arkansas State University and therefore subject to all security policies.
3. It establishes the principle that intellectual property and certain personal data are assets not belonging to, but rather entrusted to, Arkansas State University.
4. It requires all persons and units with access to information technology and data assets of the University to comply with institutional policy on its respective handling, treatment, and use.
5. It creates the categories of individuals, each with specific obligations regarding the security, use, privacy, and handling of information technology resources and data assets.

The general information security policy establishes the framework for the information security program. The information security program is comprised of 11 policies, which address specific areas of vulnerabilities and substantial risk exposure to the institution. The Security Council will oversee the creation "Policy Bulletins" that will document specific procedures and technologies used to achieve policy compliance.

C. Responsibilities

Chief Information Officer	Administer and coordinate the overall security policy and program, which include the following: 1. Propose policy constructs and framework. 2. Draft policy and bulletins. 3. Facilitate Review 4. Manage approval process of necessary and recommended policy. 5. Promulgate through publishing, educating, and auditing of policy. 6. Maintain policy in IT policy library.
Security Council	Acts as advisory body to CIO and IT management through: 1. Advising officers of the institution about issues related to the security of information, systems, and/or data. 2. Ensure that Information Technology Policy bulletins are relevant and useful. 3. Recommends policy changes to relevant University policies on information security. 4. Reviews proposed policy changes. 5. Champions information security program.
Employees	Remain aware of, and practice, appropriate handling and use of technology resources and institutional data through: 1. Following appropriate university procedures and information security policies. 2. Complete relevant and/or necessary training regarding information technology and data security.

INFORMATION SECURITY COUNCIL [###.001]

A. Members of the Information Security Council

The Information Security Council (ISC) should include Data Stewards and administrative personnel who are responsible for lines of business within the University.

B. Purpose of the Information Security Council

The purpose of the Information Security Council is to recommend and assist in the development and maintenance of the information security program at Arkansas State University.

C. Functions of the Information Security Council

The Information Security Council will serve as the review and recommendation body of the Information Security Program. The council will be chaired by the CIO or designee. Although most of the responsibility of creating and maintaining the information security program falls to the Information Technology leadership, the council has the following primary functions:

1. Review all Information Technology bulletins annually and recommend modification to executive leadership;
2. Recommend manual modification through executive leadership;
3. Review and approve information reclassification requests under direction of the Data Stewards.
4. Hold the technology organization accountable for auditing and enforcing information security policy.
5. Sponsor/conduct relevant user education and information initiative regarding information security.
6. Champion and sponsor the information security program within each organizational entity.
7. Sponsor and review the annual audit of policies conducted by the information technology organization.
8. Provide accountability for the Information Technology organization in managing and administering the information security program.

D. ISC Bulletin

ASU will establish an Information Security Council Bulletin. The ISC Bulletin will be updated annually in the regular committee appointment process. The bulletin will:

1. Identify ISC members by title and position.
2. Establish regular meeting schedule.
3. Outline critical success factors for the committee.

E. Reporting

The Information Security Council will produce an annual summary of committee activities and report this information to Executive Council.

ELECTRONIC COMMUNICATIONS PRIVACY ACT [###.002]

A. Application of the Electronic Communications Privacy Act

The Electronic Communications Privacy Act applies to any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnet, photo electronic or photo optical system. All electronic communications sent or received on Arkansas State University equipment or through Arkansas State University technology systems are presumed to be controlled by the Electronic Communications Privacy Act[i].

B. Interception of Electronic Communications

As the entity providing electronic communications service, Arkansas State University has the authority to intercept electronic communications without the consent of the person sending or receiving the communication to ensure compliance with federal and state laws or university policy. Arkansas State University will not engage in random monitoring except for mechanical or service quality control checks.

C. Disclosure of Stored Electronic Communications

As the entity providing electronic communication services, Arkansas State University has the authority to read and disclose the contents of stored electronic communications without the consent of the person sending or receiving the communication. State Freedom of Information Act requests may require the disclosure of electronic communications without the consent of the person sending or receiving the communication. All Freedom of Information Act requests are required to be forwarded to University Counsel before any records are disclosed.

D. No Expectation of Privacy in Electronic Communications

Because all electronic communications maintained in public offices, or by public employees within the scope of their employment, are presumed to be public records under Arkansas law[ii], no person utilizing Arkansas State University equipment to send or receive electronic communications has an expectation of privacy in those communications. Public records include electronic communications which constitute a record of the performance or lack of performance of official functions which are or should be carried out by a public official or employee, a governmental agency, or any other agency wholly or partially supported by public funds or expending public funds.

A. DATA CLASSIFICATION

Data Stewards will assign each data element under their purview to one of three categories: *Public*, *Limited Access*, or *Restricted*. Data stewards will then be responsible for reviewing these data classifications as required and recommending classification changes to the Information Security Council.

This manual defines information as an asset belonging to, or entrusted to, Arkansas State University. The manual addresses the areas of data classification, data labeling, data storage, and data retention.

By default, all institutional data not specifically classified in this manual as *Restricted Data* will be designated as *Limited Access data* for use in the conduct of university business or to satisfy external reporting requirements.

B. Public Data

Public data is information available to the general public.
Examples: High-level Enrollment Statistics, Course Catalog, Current Funds Budget, Financial Statements, and data on web sites intended for the general public.

C. Limited Access Data

Limited Access data is available internally but is not available to the general public unless required to be disclosed by law. Users must obtain specific authorization to access limited access data since the data's unauthorized disclosure, alteration, or destruction may cause damage to the university, students, faculty, affiliates, or staff.
Examples: Date of Birth, Ethnicity, and Purchasing Data

D. Restricted Data

Restricted data is for internal use only and is never available to the public unless by court action or consent. Where required, data stewards may identify institutional data elements as **restricted**, for which the highest levels of protection should apply, both internally and externally, due to the risk or harm that may result from disclosure or inappropriate use. This includes information protected by law or regulation whose improper use or disclosure could:

1. Adversely affect the ability of the university to accomplish its mission.
2. Pose a potential threat to the health and/or safety of faculty, staff, students, and constituents of the institution.
3. Lead to the possibility of identity theft by release of personally identifiable information of university constituents.
4. Place the university into a state of non-compliance with state and federal regulations.
5. Place the university into a state of non-compliance with contractual obligations such as payment card industry data security standards.

Restricted Data Declaration

The following data are classified as “Restricted”:

1. *Social Security Number* of any employee, student, or constituent of the institution.
2. *Banking and Financial information* of any employee, student, or constituent of the institution.
3. *Academic history and earned grade information* of any student/former student of the institution.
4. *Medical and health information* of any employee, student, or constituent of the institution.
5. *System and Network Configuration, Log Files, and security breach attempts* of any system with authorized access to an ASU network.

Statement on Classification of All Other Data

All other data will be classified as Limited Access Data and University employees will have access to these data for use in the conduct of university business on a need-to-know basis. These data, while available within the university, are not designated as open to the general public unless otherwise required by law.

The specification of data as protected should include reference to the legal or externally imposed constraint that requires this restriction, the categories of users typically given access to the data, and under what conditions or restrictions access is typically given.

Data stewards are responsible for identifying and requesting safeguards for data. If the applicable laws and regulations or the General Security Manual does not specify how to adequately safeguard the restricted data, the Data Steward is responsible for requesting appropriate safeguards in cooperation with the Office of the CIO and Legal Affairs. In some cases, multiple data stewards may collect and maintain the same restricted data element. In these cases, these data stewards and the technology organization must work together to implement a common set of safeguards. The Information Security Council should review these safeguards annually.

Data stewards are responsible for communicating and providing education on the required minimum safeguards for protected data to authorized end users and data custodians.

Examples: Social Security Numbers, Personal Financial Data protected by GLBA, Credit Card Information protected by contractual obligations under PCI standards, security data, and any data exempt from disclosure under Arkansas statutes pertaining to public records unless the exemption is waived by the university.

E. Data Classification Bulletin

A *Data Classification Bulletin* will be maintained by the university, reviewed, and updated annually by the Information Security Council. All data belonging to the institution will be identified and classified in the *Data Classification Bulletin*.

The Data Stewards are designated in the *Data Classification Bulletin* along with the data elements assigned to each Data Steward according in the *Data Classification Bulletin.* The Data Steward should be the functional business owner or intellectual property creator within the entity who assumes responsibility for owned or entrusted data elements. The Data Steward must approve release of non-public data.

Data Stewards may assign non-default Public or Restricted classifications to data based on the needs of the university as well as applicable laws and regulations. The Data Steward will bring these classification recommendations to the Information Security Council.

F. Records Retention Bulletin

The university will maintain a *Records Retention Bulletin*.

The Information Security Council of each entity will annually review the *Records Retention Bulletin* and recommend changes, additions, or modifications. The *Records Retention Bulletin* will define for each data element:

1. Data Classification.
2. Data Storage Location for onsite and offsite storage.
3. Data Retention Period.
4. Data Disposal Method.
5. Data Steward
6. Responsible Executive

G. Data Storage

All data will be stored according to its classification, meeting the following minimum requirements:

1. All data classified as *Public Data* may be stored de-centrally.
2. There are no authentication requirements for *Public Data* access.
3. A clear source of record should be identified in the *Data Classification Bulletin*.
4. All data classified as *Limited Access Data* must be stored centrally in the central data center with protected storage with high-level encryption.
    a. Exceptions to central storage of Limited Access Data are extended to:
        i. Those data identified as Intellectual Property
        ii. Academic course work of students.
5. All data classified as *Restricted Data* must be stored centrally in the central data center and must remain fully encrypted in transit and at rest.
    a. Access to such data must be fully authenticated.

H. Intellectual Property

Intellectual Property is that data which is created in support of the teaching and research activities of the institution.

A. Intellectual Property that is partially or wholly funded by external sources is by default labeled as Limited Access data and subject to this manual.
B. Any intellectual property containing data that is classified by the Data Classification Manual as “Restricted” assumes Restricted status whether or not external funding applies.
C. Intellectual Property that does not meet the Restricted Use definition is classified as Limited Use data.

In the event that this policy conflicts with the Arkansas State University Policy on Intellectual Policy, the Policy on Intellectual Policy will prevail except for the reclassification of any data that is deemed “Restricted Access Data” under the conditions in this policy.

I. Disclosure and Release

It is frequently necessary to share data from various classes of information with agencies, vendors, or service providers to the University in order to fulfill the mission of the institution. In such cases where Limited Access Data or Restricted Data is provided, the agency(ies), vendor(s), or service provider(s) must complete and return a properly-executed Non-Disclosure Agreement. The completed Non-Disclosure Agreement will remain on file in the central data center for the life of the data sharing agreement.

J. Compliance

Any unit or person using, distributing, or accessing any class of data in a manner that does not appear to be compliant with this manual will be notified by the data steward so that the use may be brought into compliance. Any access or use posing an immediate threat or risk to the University or its constituents will be disabled by any technical means possible. Use remaining non-compliant will be denied access to any University information resource until the issue is resolved through appropriate university management and disciplinary procedures.

In a perceived emergency situation, the central IT organization may take immediate steps including fully or partially blocking access, to ensure the integrity and/or confidentiality of institutional data, to protect the health and safety of the University community members and property, and/or protect the university from liability.

All decisions, notifications, or measures taken may be appealed to the Office of the CIO. If resolution or compromise is unable to be reached, the appeal may be referred to the Information Security Council for final decision.

K. Statement on Physical Security

All institutional data will meet the requirements as outlined in the Statement on Physical Security.

A. Access Control

Appropriate access control policies reduce the exposure and risk of all data that belongs to, or is entrusted to, Arkansas State University. This manual outlines minimum requirements for data access control.

The Information Security Council will annually review an information access control report to assure compliance with this manual. This report will be provided by the central IT organization to the Information Security Council.

Request procedures must take into account the risks associated with the specific data and/or system being accessed and the need-to-know reason for the request. The following minimum standards must be incorporated into the individual data access technical policies and procedures for systems and facilities containing Restricted and Limited Access data:

1. Any person with access to Restricted or Limited Access institutional data shall have unique and individual user credentials such as a user id and password.
2. Any person with access to Restricted or Limited Access data will use a complex password of at least 8 alphanumeric characters containing at least one number 0-9 and one letter A-Z.
3. Access shall be deactivated after a period of inactivity not to exceed 90 days.
4. Access shall be deactivated after 3 failed access attempts, requiring a system administrator to reset access after identity verification or automatic reactivation after 30 minutes of no access attempts.
5. Terminated employees shall lose access to data as of their termination date.
6. The data access request process for all systems shall be formalized, electronic, and auditable. The request process must include:
    a. Approvals of the requestor's supervisor.
    b. Approval of the Data Steward.
    c. Description of the specific data access requested.
    d. Level of access requested as read, write, modify or delete.
    e. Purpose for accessing the data.
7. Data access requests should be maintained in order to support the need to audit data access permissions throughout the complete data access lifecycle.
8. An automated monitoring and maintenance process against user authentication must protect limited Access and Restricted data.
9. Any facility housing systems with Restricted data must meet the following criteria:
    a. Two-levels of access control to the site.
    b. A method by which the identity of persons entering the site is logged and archived.
    c. A monitoring system to monitor all activity while in the facility.
10. Data access processes, procedures, and authorizations must be reviewed on an annual basis by each data steward to ensure that access management and control technologies and procedures are appropriate.

III. Statement on General Account Access

Under various circumstances, access to institutional data may be terminated, but it remains necessary to leave the general user account in place. Such instances include courtesy accounts for email access/forwarding, guest accounts for research partners, retiring employees, technical policy owner accounts, etc….

Under such circumstances, accounts will be assigned to an Account Sponsor. Under such circumstances, the following applies:

A. The Account Sponsor must be a full-time employee of Arkansas State University.
B. The Account Sponsor is the institutional owner of all data under sponsored account ownership.
C. The Account Sponsor becomes the owner of the sponsored account.
D. The Account Sponsor is liable for all activity and access by the sponsored account.
E. The Account Sponsor must periodically review activities and information associated with the account.
F. The sponsored account will have an automated termination date not to exceed 12 months if a renewal request is not received from the Account Sponsor.

V. Enforcement

A. The central technology organization or respective data steward will notify any unit or individual determined to be out of compliance with this manual. Efforts should be made to bring the access control procedures into compliance with this manual. Any access posing an immediate threat or risk to the university or its constituents will be disabled. Use remaining non-compliant will be resolved through appropriate university management procedures.
B. Central IT is responsible for administering and enforcing this manual.
C. All decisions, notifications, or measures taken under this manual should first be appealed to the central IT organization. If mutual arrangements cannot be made, the decision should be appealed to the appropriate Vice Chancellor.

PHYSICAL SECURITY
[###.005]

Statement Details

Physical control to information reduces the exposure of the institution by controlling access to hardware, software, networks, and data belonging to, or entrusted to, Arkansas State University.

A. Minimum Standards for Physical Access to Data

Arkansas State University will maintain appropriate physical access control procedures that meet the following minimum standards:

1. Any site containing systems or media within which Limited Access data is present must have access control in place when unattended. Most commonly, this will include locked doors.
2. Any site containing systems or storage media housing Restricted data must meet the following minimum requirements:
   a. Two levels of access control to the site.
   b. A method by which the identity of persons entering the site is logged and archived.
   c. A monitoring system to monitor all activity while in the facility.

B. Minimum Standards for Network Access

Arkansas State University will adhere to the following Network Access standards:

1. The university will maintain a system to control access of devices and persons to the network. The system must ensure current vulnerability updates, security releases, and role-based security of the connecting client.
2. The access control system must authenticate all users at all network entry points, both terrestrial and wireless.
3. All facilities containing attached network equipment (routers, switches, etc) must be single-use, secured (usually via key or card access) facilities.
4. Access control and traffic logs will be retained for 6 months, and included in the Records Retention Schedule.
5. ASU will establish and maintain a network activity monitoring system that alerts network administrators in the event of unlawful or breach attempt activity.

C. Physical Access Control Bulletin

Arkansas State University will develop and maintain a Physical Access Control Bulletin. This bulletin will outline the following:

1. Access Control systems that are utilized to achieve manual compliance and to protect physical access to data, systems, and networks.
2. Names and contact information of individuals responsible for monitoring and managing the physical layer of information access.

D. Reporting

The IT organization will provide an annual report to its respective Information Security Council to review physical access-related incidents and follow-up procedures.

THE DEPLOYMENT AND USE OF WIRELESS NETWORKS [###.006]

Deployment and use of wireless networks

Wireless networks are layered on all wired networks at Arkansas State University. Any device utilizing or appropriating wireless access to the University network infrastructure is subject to the following:

A. All use of wireless access points and devices must comply with applicable laws, regulations, and university policies including FCC regulations and the university's provisions on Acceptable Use.
B. Deployment and use of wireless network access points and devices connected to the university infrastructure must be registered and approved with the university device registration & management system at the designated URL.
C. Only centrally managed, university-owned wireless access points may be attached to any Arkansas State University network.
D. All wireless devices connected to the University network infrastructure must use wireless spectrums officially recognized by the FCC as production data networks.
E. As with all ASU wired network access, access through wireless access points and devices must be automatically logged. Logs must be retained for at least 30 days and should include the identity of the user or equivalent information, the date and time of access, and the IP address assigned for the session.
F. Any wireless access point and device providing access to data identified as "Restricted" in the data classification manual must support data encryption of identified data while in transit and must not retain said data in any manner.
G. Any wireless access point or device must utilize IP address space as assigned by network management via static or dynamic address assignment.

Enforcement

The central IT organization will notify personnel operating a wireless access point or device that does not appear to be compliant with this manual so that it may be removed from the network. Wireless access points not brought into compliance will be denied network access.

In a perceived emergency situation, the central IT organization may take immediate steps, including denial of access, to ensure the integrity of the university data network and systems, safeguard the health and safety of the university community members and property, or protect the university from liability.

DEPLOYMENT AND USE OF COMMUNICATION NETWORKS [###.007]

A. Deployment and use of Communications Networks

Data communications networks support the operations and the health/human safety of all constituents. To ensure the optimal and reliable operation of this critical university resource, all communication networks are subject to the following:

1. Use of any network facility must be consistent with the provisions on Acceptable Use.
2. ASU will develop a Network Operating Requirements Bulletin. The bulletin will outline communications protocols supported by ASU, operational and security requirements that exceed the minimum requirements of this manual, and device standards for network-attached devices.
3. ASU will maintain, at minimum, a neutral network (commonly referred to as a DMZ), an academic network, a residential network, and a restricted network.
4. Systems and servers hosting or processing data classified as "Restricted" will be configured to reside in a Restricted Network on the local area network.
5. All network-attached devices will be registered (by MAC-level address) and authenticated before being granted network access.
6. Technical, operational, security guidelines and standards will be available in the Network Operating Requirements Bulletin. All units and personnel using any network resource as well as devices connected directly or indirectly to wired and wireless networks must comply with the requirements of the bulletin.
7. Network address space, domain naming spaces, network connections, and video services will be maintained and managed by the central IT organization.
8. The central IT organization will collaboratively (with the ISC) update the Network Operating Requirements Bulletin to continually meet changing requirements.
9. To appropriately manage traffic to local, state, and global networks, all network access and traffic must be authenticated and logged. Log files will be retained for a minimum of 180 days.
10. All units, personnel, students, and connected users will be notified that normal operation and maintenance of the network requires the central IT organization to routinely engage in backup and caching, logging activities, and monitoring of usage patterns, and security activities. However, use of information gathered in this manner is subject to the university's provisions on Acceptable Use.
11. The central IT organization will work with all units to ensure use and compliance with this policy and with the operating requirements. In the event of a conflict, central IT will work to negotiate acceptable arrangements. If a resolution cannot be reached, the CIO will specify a resolution to be approved by executive leadership.
12. The Deployment and Use of Communications Networks will be audited annually by central IT, results of which will be reviewed by the Information Security Council.

I. Responsibilities

Central IT	Manage daily operations of local and wide-area networks. Ensure performance and service expectations are met. Audit network performance/security, provide summary report to ISC. Conduct annual capacity/use analysis, provide summary report to ISC.
Information Security Council	Review compliance summary report. Review traffic and capacity management plan.

MOBILE INFORMATION SECURITY [###.008]

Mobile Information Security

Any device connecting to a university network or accessing/storing university-owned Restricted or Limited Use data is subject to the following provisions:

1. University-owned Devices
   ASU will maintain minimum security standards of mobile computing devices that are not cellular phones, to include:
   a. Fully encrypted internal storage use whole-disk encryption.
   b. Asset tracking & recovery capability.
   c. Password protecting for access. A minimum password length of no less than 8 characters.

2. University-owned Cellular Phones
   All university owned cellular phones must:
   a. Be procured through the central IT organization.
   b. Be registered in the institutional asset management system.
   c. Be capable of being remotely disabled or “wiped”.

3. Personally-owned Devices
   a. The device must be password protected at all times, with a password length of no less than 8 characters.
   b. The device must support data encryption.
   c. Any university data stored on the device must remain encrypted.

4. All Mobile Devices
   a. No Restricted data may be stored on the device unless it is encrypted and prior approval has been obtained from the Data Steward.
   b. No mobile computing device may connect to terrestrial or wireless networks without authentication and scanning for vulnerabilities.
   c. By connecting personally-owned mobile devices to the Arkansas State University network, and/or by storing university-owned information on personally-owned mobile devices, the user of said device recognizes that the data is subject to all provisions of this manual and consents to allow Arkansas State University to remotely erase devise in the instance of terminated employment or device loss.
   d. The owner of a personally owned device that has stored university-owned Limited Use or Restricted data consents to liability for protection of stored data.

   In the event that the device cannot be brought into compliance, Limited Use or Restricted data belonging to Arkansas State University will be removed by necessary steps to protect the interest of the University or its constituents.

INCIDENT REPORTING AND RESPONSE [###.009]

A. Incident Reporting

Information security incidents shall be reported to the security address with the central IT organization utilizing the Security Incident Report.

B. Incident Response

Upon receipt of a Security Incident Report, the central IT organization shall conduct an investigation and ensure that in all incidents:

1. Are documented and thoroughly and expertly investigated;
2. Are handled in a consistent manner and in accordance with data disclosure notification laws.
3. That evidence is preserved so as not to corrupt forensic efforts;
4. That harmful effects are mitigated; and
5. That measures to prevent recurrence are identified and implemented.
6. To avoid inadvertent violations of state or federal law, neither individuals nor departments may release University information, electronic devices or electronic media to any outside entity, including law enforcement organizations, before making the notifications required by this manual.

C. Incident Reporting Bulletin

ASU will develop an Incident Reporting Bulletin on how its respective constituents should report information security incidents.

ASU will prepare an annual incident summary report to be reviewed by the Information Security Council.

APPLICATION DEVELOPMENT AND MANAGEMENT [###.010]

A. Application Development and Management

ASU and its authorized personnel will adhere to the Application Development guidelines and Application Management guidelines below:

1. Application Development Guidelines

AD Guideline	Practice	Req/Rec
a	Classify the university data handled or managed by the application (see Data Classification Standard).	Required
b	Prominently display a Confidential Record banner to the screen or interface in use by the application, depending on the type of data being accessed.	Required
c	Ensure applications validate input properly and restrictively, allowing only those types of input that are known to be correct. Examples include, but are not limited to, such possibilities as cross-site scripting, buffer overflow errors, and injection flaws.	Required
d	Ensure applications execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system.	Required
e	Ensure applications processing data properly authenticate users through central authentication systems.	Recommended
f	Establish authorizations for applications by affiliation or institutional role, rather than by individual identity.	Recommended
g	If individual authorizations are used, these should expire and require renewal on a periodic (at least annually) basis.	Required
h	Provide automated review of authorizations where possible.	Recommended
i	Use central authorization tools where possible, and if additional functionality is needed, coordinate development with Information Technology Services (ITS).	Recommended

j	Ensure applications make use of centralized secure storage for university data.	Required
k	Services or applications running on systems manipulating Restricted data should implement secure (encrypted communications).	Required
l	Implement the use of application logs to the extent practical, given the limitations of certain systems to store large amounts of log data. When logging access to university data, store logs of all users and times of access for at least 14 days.	Required
m	Conduct code-level security reviews with professionally trained peers for all new or significantly modified applications; particularly, those that affect the collection, use, and/or display of confidential Restricted data, documenting the actions that were taken.	Required
n	Conduct annual security tests of Internet applications. Request annual security scans of Internet applications.	Recommended
o	Ensure that obsolete applications, or portions of applications, are removed from any possible execution environment.	Required
p	Implement and maintain a change management process for changes to existing software applications.	Required
q	Third parties, for example, vendors, providing software and/or receiving university data must enter into written agreements with the university to secure systems and data.	Required

2. Application Management Guidelines

AM Guideline	Practice	Rec/Req
a	Maintain a full inventory of all applications with descriptions of authentication and authorization systems, along with the data classification and level of criticality for each application. Ensure a custodian(s) is assigned to each application.	Required
b	Document clear rules and processes for vetting and granting authorizations.	Required

c	On at least a semi-annual basis, review and remove all authorizations for individuals who have left the university, transferred to another department, or assumed new job duties within the department.	Required

B. Application Development Bulletin

ASU will maintain an Application Development Bulletin in support of this manual. Exceptions to the application development standards will be documented, including the exception that was made and the reasoning for the exception.

C. Application Management Bulletin

ASU will maintain an Application Management Bulletin in support of this manual. Exceptions to the application management standards will be documented, including the exception that was made and the reasoning for the exception.

D. Compliance

The central IT organization will provide annual compliance and testing reports to the respective Information Security Council. Exceptions and non-compliance will be addressed through the appropriate Vice Chancellor for the functional business owner.

ARKANSAS STATE UNIVERSITY JONESBORO

SYSTEM SECURITY [###.011]

A. System Security

All non-university systems, owned equipment and servers connected to university owned equipment, systems, and servers must be owned by a full-time faculty or staff member who is responsible for system administration.

B. Central Registry

The central IT organization on the respective will monitor compliance of all network-attached systems and will implement a bulletin outlining specific configuration requirements and exceptions granted to these requirements.

C. Configuration Guidelines

Approved server configuration guidelines that meet the minimum requirements of this manual are as follows:

1. ASU will maintain a centralized registry of installed servers on the campus or attached to the university network. At a minimum, the following information is required to be listed in the registry for each server:
    a. Server contact and backup contact
    b. Server location
    c. Hardware and Operating System versions
    d. Indication as to whether the server contains virtual machines
    e. IP Addressing information
    f. Primary functions and applications.
2. Information in the central registry should be kept up to date. Ideally, registration of the server should be complete prior to granting network access to the server.
3. Any system that stores or processes data classified as “Restricted” according to the Data Classification Manual may not be classified as a Research System.
4. Servers and systems supporting only research (Research System) should be connected to the network through a DMZ. Once in the DMZ, research systems are exempt from the guidelines outlined in Section II.

D. Configuration Requirement Bulletin

Operating system configurations should meet configuration requirement bulletins. Exceptions that are made should be documented and attached to the server configuration bulletin. At a minimum, each bulletin must require that:

1. Services and applications on the system that will not be used must be disabled where practical.
2. Access to services should be logged and/or protected through access control methods such as TCP wrappers, if possible.
3. The most recent security patches must be installed on the system as soon as practical.
4. Server-class systems must be located in an access-controlled environment.
5. Network-attached server-class systems are specifically prohibited from operating in non-access-controlled areas.

E. Monitoring

1. All security-related events must be logged and audit trails saved.
2. All security related logs should be kept online for a minimum of 7 days.
3. Daily incremental backups must be retained for at least 30 days.
4. Weekly full backup of logs must be retained for at least 30 days.
5. Monthly full backups must be retained for a minimum of 2 years.
6. Security-related events will be reported to the central IT organization, which will review log files and prescribe corrective measures as needed. Security-related events include, but are not limited to:
    a. Port-scanning activity
    b. Evidence of unauthorized access to privileged accounts
    c. Anomalous occurrences that are not related to specific applications on the host.

F. Compliance

1. Audits of compliance will be performed annually by the central IT organization. The compliance report should include every system in the registry, along with documented scans to identify network-attached systems that are not registered.
2. The central IT organization will provide the Information Security Council with a compliance report of all systems in the central registry.
3. Every effort should be made to prevent audits from causing operational interruptions or failures.

DEFINITIONS

Administrative Network
Generally virtual local area networks that are intended for routing information/data/communications between business support systems.

Academic Network
Generally those networks, physical or virtual local area networks that are intended for routing information/data/communications between academic systems/instruments.

Access-controlled Environment
Physical environments, usually rooms, buildings, and facilities into which general access is prohibited. Such environments usually are restricted by key, lock, or other access control system (cards, bio-metric, etc).

Arkansas State University System
All entities under the jurisdiction of the Arkansas State University Board of Trustees.

Arkansas State University
Any organized under the ASU Board of Trustees, usually within the purview of a Chancellor.

Buffer Overflow Errors
Occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.

Central IT
The organization that manages and operates technology resources for the institution as a whole.

Critical Success Factors
Those factors defined as essential for success in technology operations.

Cross Site Scripting
A security exploit in which the attacker inserts malicious coding into a link that appears to be from a trustworthy source.

Data Encryption
Conversion of data, based on industry standards, into a form that cannot be easily accessed or understood by unauthorized persons.

Data Stewards
Personnel responsible for data use and maintenance.

DMZ
Generally, a virtual local area network with more unrestricted access to systems within it.

Dynamic IP
Internet Protocol address that is temporarily assigned to a device for the duration of a session.

Executive Leadership
Generally, those personnel who report to the Chancellor.

Incident Reporting Site
Specific website where users can anonymously report suspected security breaches.

Information Security Incident
Suspected breach of information security.

Information Security Program
All policies, guidelines, management, and audit related activities which are intended to reduce exposure and risk in regard to information privacy and security.

Lines of Business
Academic and Business activities within Arkansas State University. Generally reporting back through mid-management to a Vice Chancellor.

MAC-level Address
Unique identifier assigned to network adapters in devices that connect to a network or the Internet.

Mobile Device
A computing or communications device that is designed for portability.

Non-Access-Controlled Environment
General areas that are accessible without restrictive measures to prevent unauthorized intrusion.

Non-Commercial Use
Use that is intended for purposes that do not generate profit.

Neutral Network
A network that passes packets without analysis, prioritizing, or shaping those packets.

Personally-Owned Device
Generally, a stationary or mobile computing/communications device that is owned by an individual.

Port-Scanning Activity
Generally, software that is designed to probe a network for open/vulnerable ports.

Research System
Generally, a system or instrument that processes or stores information collected for research purposes.

Restricted Network
Local or Wide Area Networks that are restricted either by role or data type.

Security Patch
Generally, a software release that is designed to address specific security vulnerabilities.

Server-Class Systems
Hardware and software systems that are designed to host many simultaneous users and process.

Source of Record
Original record.

Static IP
Internet Protocol address that is permanently assigned to a device for use through multiple sessions.

TCP Wrappers

IP packet filtering system based on token attached to a packet.

University-Owned Device

Generally, stationary and mobile computing/communications devices purchased with public or foundation funds and assigned to Arkansas State University Board of Trustees.

Wireless Access Point

Wireless communications device that broadcasts a signal and accepts connections from devices.

---

[i] 20 U.S.C. § 1277

[ii] A.C.A. § 25-19-101