Information & Technology Services Management & Security Principles & Procedures

Executive Summary Contact: Henry Torres, (870) 972-3033

Background:

The Security Task Force began a review of all procedures related to the integrity and security of ASU technology assets. In an effort to accurately document and reflect the current environment and create the framework for future security improvements, the following statement of Information & Technology Services Management & Security Principles & Procedures has been drafted.

Summary:

The following provides the framework for privacy and security of data on the ASU campus.

- There is no expectation of privacy in University electronic communications
- Data that contains personally identifiable information or information protected by FERPA must be safeguarded
- Unauthorized use of the University network or electronic assets is prohibited
- Any incident involving any of the above should be reported immediately to ITS

Consequences:

- Failure to observe the procedures and recommendations can result in exposure of private data, damage to University and its assets and compromise of personal information.

- Knowing and willful disregard for these procedures may result in may result in disciplinary action and/or termination of employment.

Information & Technology Services Management & Security Principles & Procedures

The following document enumerates the principles and procedures pertaining to Technology Management and Security at ASU-J.

I. Privacy

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.

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.

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.

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, 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.

II. Data Access

Data Classification

The University has established Data Stewards by Division (see attachment) with ownership and responsibility for the access to and integrity of the data elements assigned to them. Data Stewards will assign each data element under their purview to one of three categories: *Public*, *Limited Access*, or *Restricted*. By default, all institutional data not specifically classified as *Restricted Data* will be designated as *Limited Access data* for use in the conduct of university business or to satisfy external reporting requirements.

- **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.*
- **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*

- **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.

The following list of data elements are classified as "Restricted" but should not be considered exhaustive:

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

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.

III. Data Retention

The university will maintain a *Records Retention Schedule* which defines for University records:
1. Type of record.
2. Description of record.
3. Data Retention period.
4. Data Retention location.
5. Custodian.
6. Disposal method.

IV. 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. *Restricted Data* must be in a university-owned or leased data center that meets the criteria set forth in this policy.
4. All data classified as *Restricted Data* must remain fully encrypted in transit and access to such data must be fully authenticated.

V. Data 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.

VI. Compliance

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.

VII. Physical Security

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 or last day of work.
6. The data access request process for all systems shall include:
    - Approvals of the requestor's supervisor.
    - Approval of the Data Steward or his/her authorized delegate.
    - Description of the specific data access requested.
    - Level of access requested as read, write, modify or delete.
7. Data access requests will be maintained in order to support the need to audit data access permissions throughout the complete data access lifecycle.
8. 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.

VIII. Minimum Standards for Network Access

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

1. The university is implementing and 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 will be configured to authenticate all users at all network entry points, both terrestrial and wireless.
3. All facilities containing attached network equipment (routers, switches, etc) must be secured (usually via key or card access) facilities.
4. Access control and traffic logs will be retained for a minimum of 90 days, and included in the Records Retention Schedule.

IX. Deployment and use of wireless networks

Any device utilizing or appropriating wireless access to the University network infrastructure is subject to the following:
A. Only centrally managed, university-owned wireless access points may be attached to any Arkansas State University network.
B. All wireless devices connected to the University network infrastructure must use wireless spectrums officially recognized by the FCC as production data networks.
C. 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.

In a perceived emergency situation where the integrity of the university data network and systems, the health and safety of the university community members and property, or substantial risk to the University exists, the central IT organization may take immediate steps, including denial of access, to protect the above. The situation will be reported immediately to the CIO and appropriate University management for further action.

X. Incident Reporting

Information security incidents shall be reported to the CIO immediately including the loss or theft of a University owned device.
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 notification to the CIO.

For further steps regarding an incident involving loss or theft, see Operating Procedure 05-31 on the Finance website at http://www.astate.edu/dotAsset/bb4a2846-36fc-4360-9bd4-960526e9b2d3.pdf

Attachment

Data Stewards as of 10/10/2013

Terry Finney, Financial Aid
Tracy Finch, Registrar & Admissions
Carol Byrd, Student Accounts
Vacant, Payroll
Lori Winn, HR
Holly Van Wagener, Advancement
Russ Hannah, Finance