Data Classification

Purpose
ASMSA uses cyber systems to perform education, research, and all other business functions by collecting, storing, and processing data. State, federal, and international laws and regulations require protection of data. Each of these laws prescribes the types of security and privacy controls required for protecting the confidentiality, availability, and integrity of the data. Consistency and reliability of controls and clarity of responsibility are achieved by developing a schema, which can be applied to any data type.

The purpose of this policy is to define a data classification schema and hence define the most effective, efficient, and economically reasonable controls to protect the data.

Scope
This policy applies to all school-owned data collected by school business units and departments, stored on school owned devices and systems, transferred between school owned devices and systems or between school owned devices/systems and all other devices and systems owned and operated by third parties who are storing and processing ASMSA data.

Policy

Data Classification
ASMSA has developed the following three main classification categories. Every data collected, stored, processed, and transferred should be categorized and labelled properly.
Everybody, including but not limited to faculty, staff, students, and any third-party service provider collecting, processing, or storing ASMSA data excluding federal, state, and legal institutions (e.g.: IPEDS, ADHE, DOE, DOJ, UA System Office) should implement the security controls defined in this policy.

Highly Sensitive
Highly sensitive data that, if disclosed to unauthorized persons, would be a violation of federal or state laws, ASMSA policy, or ASMSA contracts. Any file or data that contains personally identifiable information of a trustee, officer, agent, faculty, staff, retiree, student, graduate, donor, or vendor may also qualify as highly sensitive data unless the data is already disclosed by the ASMSA or classified as public and published on the web sites or public documents, including the directory data as defined by the Arkansas Freedom of Information Act. Highly Sensitive includes all data defined by the state Data and System security standard classifications of Level C (Very Sensitive) and Level D (Extremely Sensitive). By way of illustration only, some examples of Highly Sensitive data include, but are not limited to:

- Health information, also known as protected health information (PHI), which includes health records combined in any way with personal information.

- Names.
- Addresses.
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, and date of death.
- Any phone numbers, fax numbers, email addresses not listed in the ASMSA directory and can be used to uniquely identify any individual.
- Social Security Numbers.
- ASMSA identification numbers.
- Medical record numbers.
- Diploma/certificate/license numbers.
- Vehicle identifiers and serial numbers, including license plate numbers.
- Device identifiers and serial numbers.
- Biometric identifiers, including finger and voice prints.
- Full face photographic images and any comparable images not publicly available.
- Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual.
- Health Information as further defined by the Health Insurance Portability and Accountability Act (HIPAA) or the Health Information Technology for Economic and Clinical Health Act (HITECH Act) of 2009.
- Student records (except for that information designated by the ASMSA as directory information under the Family Educational Rights and Privacy Act) and other non-public student data.
- Payment Card Information (PCI), including cardholder name, service code, expiration date, CVC2, CVV2, or CID value, PIN, and contents of credit card's magnetic stripe.
- Certain personnel records, such as benefits records, health insurance information, retirement documents and/or payroll records.
- Any data identified by state or federal law or government regulation, or by order of a court of competent jurisdiction to be treated as confidential or sealed by order of a court of competent jurisdiction.
- Any law enforcement investigative records and communication systems.
- Authentication verifiers, including passwords, shared secrets, and cryptographic private keys.
- GLBA covered financial information, including employee payroll and tax data.
- Student financial aid information.
- IT security information (such as privileged credentials, incident information, and device configurations).
- Information covered by GDPR.
- Intellectual property; and
- Unpublished research data.

Internal

Internal data is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission,

storage, or other use. This classification applies even though there may not be any law or other regulation requiring this protection.

Internal data is information that is restricted to personnel designated by the ASMSA who have a legitimate business purpose for accessing such data. Legitimate business processes include any business process required to perform education and research activities in the ASMSA and other supporting activities enabling education and research functions. Much of this data includes any information that is made available through open records requests or other formal or legal processes. Internal data includes all information that is made available under the Arkansas Freedom of Information Act. Internal data includes all data defined by the state Data and System Security standard classification of Level B (Sensitive). By way of illustration only, some examples of internal data include, but are not limited to:

- Employment data.
- Business partner information where no more restrictive confidentiality agreements exist.
- Internal directories and organization charts.
- Planning documents.
- Network-System information.
- Contracts.
- Building plans and associated information.
- Export controlled information; and
- Telecommunications systems information.

Public

Public data is information to which the general public may be granted access in accordance with ASMSA of Arkansas policy or standards. Public includes all data defined by the state Data and System Security standard classification of Level A (Unrestricted). By way of illustration only, some examples of public data include, but are not limited to:

- Publicly posted press releases.
- Publicly posted schedules of classes.
- Posted interactive ASMSA maps, newsletters, newspapers, and magazines.
- Information posted on the ASMSA's public website, including the website for
- Institutional Research and Analytics; and
- Student records are designated by the ASMSA as directory information under the Family Educational Rights and Privacy Act.

Data Protection Controls

General Statements

It is the responsibility of everyone with access to highly sensitive data resources to use these resources in an appropriate manner and to comply with all applicable federal, state, and local statutes. Additionally, it is the responsibility of everyone with access to highly sensitive data resources to safeguard these resources.

It is the responsibility of everyone to determine if they have highly sensitive data on their individual-use device(s) and media and, if so, to ensure compliance with this policy. Failure to comply with the requirements of this policy will result in loss of access to the data. The IT Manager enforces this policy at the direction of the Director.

Sensitive Data Handling

Methods of safeguarding highly sensitive data include:

- Highly sensitive data should not be stored on any unencrypted personal desktop or laptop computers.
- Highly sensitive data should not be stored on individual-use, removable media, including but not limited to external hard drives, magnetic tapes, diskettes, CDs, DVDs, and USB storage devices.
- If it is necessary to use external storage systems to transfer highly sensitive data between the systems in order to complete a legitimate business process, highly sensitive data may be stored on external storage systems temporarily.
- Any highly sensitive data must be deleted from external storage devices after data is transferred to another system.
- If it is not possible to delete the data, the storage device must be destroyed.
- Access to computers that are logged into central servers storing highly sensitive data should be restricted (i.e., authenticated logins and screensavers, locked offices, etc.).
- Access to highly sensitive data resources stored on central servers should be restricted to those individuals with an official need to access the data.
- All servers containing sensitive data must be housed in a secure location and operated only by authorized personnel.
- All servers containing sensitive data must be protected by appropriate firewall rules and must undergo a regular vulnerability assessment.
- All servers containing sensitive data must maintain authentication, security, and similar system logs for no shorter than 120 days.
- For all information system resources which contain, or access data classified as “sensitive” per the data classification standard, processes must be in place to ensure the access and activity is recorded and reviewed.
- Copies of highly sensitive data resources should be limited to as few central servers as possible.
- Highly sensitive data should be transmitted across the network in a secure manner (i.e., to secure web servers using data encryption with passwords transmitted via secure socket layer, etc.).

Sensitive Data Storage

- All individuals must routinely inventory their respective electronic devices for highly sensitive data using processes or procedures recommended by Information Technology Services.
- Highly sensitive data must be securely encrypted on the electronic device or media, according to encryption methods recommended by Information Technology Services.

- A log-in password must be enabled for the electronic device and, if available, the electronic media. The password must meet or exceed appropriate complexity levels. The password should not be shared with anyone.
- A password-protected screen saver, if available, must be enabled on the electronic device and set to activate after a maximum of ten minutes of user inactivity. The password must meet or exceed appropriate complexity levels. The password must not be shared with anyone.
- At a minimum, the electronic device must employ the basic security requirements described in the "Securing Electronic Devices" process and procedures published by Information Technology Services.
- The data must be deleted from the individual-use device or media as soon as they are no longer required using secure methods according to the Electronic Data Removal section of this policy and the Records Retention and Disposition Policy.
- Management of the electronic device may not be outsourced to any party external to the ASMSA without written approval from the data owner and the Associate Vice Chancellor for Information Technology Services. This written request and approval/disapproval must be filed in a secure location for subsequent audit purposes.

Electronic Data Removal

All software and data files must be removed by ASMSA-approved procedures from electronic devices and electronic media that are surpluses, returned to a leasing company, or transferred from one ASMSA employee to another employee having different software and data access privileges. When electronic devices are sent outside the ASMSA for repair, all data must be either encrypted or removed to the extent possible.

All electronic devices must be routinely scanned for highly sensitive data (as defined in the Data Classification Policy) that is not stored on ASMSA-approved secured servers and storage. Any data found must be reported to the IT Manager. This data must be moved to a secured location or removed according to ASMSA-approved procedures.

Data Breach Reporting

Any accidental disclosure or suspected misuse of highly sensitive data must be reported immediately to the appropriate ASMSA officials. The appropriate ASMSA officials include the data owner, the IT Manager, and the school Director.

Compensating Control and Exception Request

It is imperative that ASMSA faculty, staff, and students comply with this policy and any related procedures or guidelines. However, there are circumstances that fall outside the ability to comply with and/or conform to the standard. In such instances, an exception must be documented and approved by Internal Audit and Information Technology Services.

Requests for exception must include:

- a valid business justification
- a risk analysis

- compensating controls to manage risk.
- technical reasons for exception.

Requests for exceptions that create significant risks without compensating controls will not be approved.

Requests for exceptions are reviewed frequently to ensure that assumptions or business conditions have not changed and for validity. Exception requests and renewals are not automatically approved.