Data and System Classification Grid Guidelines

State Security Office

The purpose of the data and system classification exercise is for agencies to examine the data in their information systems, determine its sensitivity or criticality to the agency's functions, and then determine the appropriate level of security to apply to the information technology systems. Various security standards promulgated by the State Security Office directly reference the classification level of agency data and systems. To see the state security standards, please visit: http://www.techarch.state.ar.us/indexes/standards.htm .

Agencies are not expected to take a complete inventory of their data and systems, but to look at their data and systems in general terms. The data and system classification process should not take a substantial amount of time. Typically, the process can be completed by a small group of people familiar with the agency's information technology resources or a person with comprehensive knowledge of agency data, such as the agency chief information officer, information technology manager, or database administrator.

Step 1. Identification of data and systems

Identify the major databases and systems controlled by your agency's IT provider, whether the provider is internal or external (such as the Department of Information Systems). Even though DIS may house an agency's information, each agency is responsible for determining the criticality and sensitivity of the information. Control is defined as the responsibility for the design and/or maintenance of the hardware and software housing the databases or the security of the database or system.

There are some databases over which an agency has control of some of the records, such as AASIS or federal databases to which the state supplies data, but over which the agency has no control or input with regard to security or maintenance. *It is not necessary to classify these databases.*

There may be several databases throughout an agency that are not considered significant or are not under centralized control. However, some of the less significant databases may contain sensitive or critical information and should be classified.

In addition to databases, systems such as phone networks, websites, email systems, and networks should be considered for inclusion in the grid.

Step 2. Classification of agency data and systems

The Data and System Classification Grid contains descriptions that will lead your organization to appropriately classify agency data and systems. See Appendix A for more descriptive information regarding the levels of classification.

In performing the classification, keep in mind that data sensitivity refers to the most sensitive component of the database. For instance, an otherwise innocuous database may contain social security numbers, so the database would be classified as Very Sensitive. This concept also applies to the level of criticality.

Classifying Standard Databases

Many databases are readily identified as a single source of data. Examples of standard databases might be permit tracking, license holders, and fleet records databases. A database of license holders might be considered critical for agency operation, and the presence of social security numbers in the database would classify the data as Very Sensitive. Therefore, the database would be classified as 2C, being Critical and Very Sensitive.

Classifying Grouped Data

Agencies can group types of data in their classification grid. Your agency may control a particular type of data maintained in a variety of media, such as databases, spreadsheets, and word documents. You can refer to this data as a whole in your classification. For example, an agency may group all of its legal proceeding information together in a single entry in the classification grid, but it may exist in different electronic forms throughout the agency.

Classifying Systems

Systems should be also be classified. For example, your agency’s phone system might not carry sensitive information, yet it is critical for your agency to function. In contrast, an emergency communications network would not only carry sensitive information, but also be considered extremely critical for the functioning of state government, so these two systems would be classified differently.

Another example would be a public website versus an email system. Both are transmitting data and are combinations of hardware and software, but the email system usually transports more sensitive information and is probably more important for the daily operations of your organization.

Appendix A

Sensitivity Levels

LEVEL A - UNRESTRICTED

Unrestricted data is characterized as being open public data with no distribution limitations and to which anonymous access is allowed.

These data elements form information that is actively made publicly available by state government. It is published and distributed freely, without restriction. It is available in the form of physical documents such as brochures, formal statements, press releases, reports that are made freely available, and in electronic form such as internet web pages and bulletin boards accessible with anonymous access.

The greatest security threat to this data is from unauthorized or unintentional alteration, distortion, or destruction of this data. Security efforts appropriate to the criticality of the system containing this data must be taken to maintain its integrity.

Examples of data at this sensitivity level include many agency public websites.

LEVEL B - SENSITIVE

These data elements are the information that is made available through open records requests or other formal or legal processes. This category includes the majority of the data contained within the state government electronic databases. Direct access to this data is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties.

Security threats to this data include unauthorized access, alteration and destruction concerns.

Examples:

Most data elements in state personnel records
Driver history records
Employment & training program data
Firearm permits data
Real estate appraisal data
Personnel data

Building code violations data
Collective bargaining data
Federal contracts data
Historical records repository data
Occupational licensing data

LEVEL C - VERY SENSITIVE

Data classified as being very sensitive is only available to internal authorized users and may be protected by federal and state regulations. Very sensitive data is intended for use only by individuals who require the information in the course of performing job functions.

These data elements include those protected by federal and state statute or regulation.

Access to these data elements is restricted to authenticated and authorized individuals who require access to that information in the course of performing their duties.   These are the data elements removed from responses to information requests for reasons of privacy.

Security threats to this data include violation of privacy statutes and regulations in addition to unauthorized alteration or destruction. If this data were accessed by unauthorized persons, it could cause financial loss or allow identity theft. Unauthorized disclosure could provide significant gain to a vendor's competitors.

Examples:

Social Security numbers
Most home addresses
Attorneys' files
Comprehensive law enforcement data
Domestic abuse data
Educational records
Foster care data
Health and medical data
Library borrower's records
Signature imaging data
Welfare records/data

Credit card numbers
Competitive bids
Civil investigative data
Criminal history data
Economic development assistance data
Food assistance programs data
Head Start data
Juvenile delinquent data
Counselors' data
Trade secrets data

LEVEL D - EXTREMELY SENSITIVE

Data classified as being extremely sensitive is data whose disclosure or corruption could be hazardous to life or health.

These data elements are the most sensitive to integrity and confidentiality risks. Access is tightly restricted with the most stringent security safeguards at the system as well as the user level. Failure to maintain the integrity and confidentiality could have severe financial, health or safety repercussions. Very strict rules must be adhered to in the usage of this data.

Examples of this data include the contents of state law enforcement investigative records and communications systems.

Criticality Levels

LEVEL 1 – NOT CRITICAL

These data and systems are necessary to state government but short-term interruption or unavailability is acceptable. They do not play any role in the scheme of the health, security, or safety of Arkansas' citizens.

LEVEL 2 – CRITICAL

These data and systems are required in order to administer functions within state government that need to be performed. Business continuity planning allows state government to continue operations in these areas within a certain period of time until the data and systems can be restored.

LEVEL 3 – EXTREMELY CRITICAL

These data and systems are critical to public health or safety and must be protected by a vital plan that would allow resumption of operations within a very short timeframe. These data and systems also require restoration of the original facilities to be able to resume business.