



INFORMATION SECURITY AND PRIVACY POLICY DATA CLASSIFICATION

IT POLICY NUMBER: 2100-04

EFFECTIVE DATE: 12/05/2012

APPROVED BY:

A handwritten signature in black ink, appearing to read "Robert Blair", written over a horizontal line.

Robert Blair, Director
Department of Administrative Services

1.0 PURPOSE

This policy provides the data classification methodology and requirements for the Department of Administrative Services (DAS) for the purpose of properly identifying and labeling data and information assets according to their levels of confidentiality and criticality. Classification of data and information assets provides a basis for deploying appropriate levels of security relevant to the use, management, and control of data and information assets.

2.0 SCOPE

The scope of this IT policy includes computer and telecommunications systems owned or operated by DAS, the information residing on these systems and the managers of DAS business units and IT systems who use or administer such systems.

DAS customers are responsible for classification of their information. DAS is responsible for classification of information internal to or used by DAS.

All data that is either stored or shared via any method on or by any DAS IT resource falls within the scope of this policy. This includes electronic information, information on paper, and information shared orally or visually (e.g. telephone or video conferencing).

3.0 BACKGROUND

Increased connectivity of computers and databases makes more data available to individuals, businesses and agencies. As a result, the potential for unauthorized disclosure, modification or destruction of personal, financial, business and other data also has increased. Data classification is a process that identifies what information needs to be protected against unauthorized access, use or abuse, and the extent of that protection.

4.0 REFERENCES

- 4.1. **Ohio IT Standard; ITS-SEC-02; Security Controls Framework:** This state IT standard specifies the minimum requirements for information security in all **agencies** and identifies the National Institute of Standards and Technology (NIST) Special Publication 800-53, revision 3 (NIST 800-53) as the framework for information security controls implementation for the state.
- 4.2. **NIST Special Publication 800-53 (Rev 3), Recommended Security Controls for Federal Information Systems and Organizations,** provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.
- 4.3. **Federal Information Processing Standard (FIPS) 199 “Standards for Security Categorization of Federal Information and Information Systems”** provides guidance for assigning security categories to information systems.
- 4.4. **Ohio IT Bulletin; ITB-2007.02; Data Encryption and Securing Sensitive Data:** This IT Bulletin provides guidance to agencies on protecting sensitive data.
- 4.5. **DAS Policy; 2100-02; Mobile Computing:** This DAS policy addresses remote access and the use of portable computing devices.
- 4.6. **DAS Policy; 700-01; IT Resource Usage:** This DAS policy addresses use of DAS IT resources.
- 4.7. A glossary of terms found in this policy is included in Section **9.0 – Definitions**.

5.0 POLICY

DAS is issuing this policy to ensure compliance with related state policies and to protect DAS’ IT resources. More detailed security standards and procedures supporting the implementation of this policy will be maintained separately.

DAS manages a great deal of information in support of its business objectives. DAS serves as a classification authority for the data and information that it collects or maintains in satisfaction of its mission. DAS customers are responsible for classifying their data.

- 5.1 **Data Classification Labels.** The classification of data is an important tool in defining and implementing the correct level of protection for DAS information assets. DAS shall label data for both confidentiality and criticality.

Classification labels shall be:

5.1.1 Confidentiality. The confidentiality label identifies how sensitive the data is with regard to unauthorized disclosure.

5.1.1.1 Data shall be assigned one of three labels for confidentiality:

- Public. The “public” label includes information that must be released under Ohio public records law or instances where an agency unconditionally waives an exception to the public records law.
- Limited Access. The “limited-access” label applies to information that an agency may release if it chooses to waive an exception to the public records law and places conditions or limitations on such a release.
- Restricted. The “restricted” label applies to information, the release of which is prohibited by state or federal law. This label also applies to records that an agency has authority to release under public records law exceptions but has chosen to treat the information as highly confidential and not release the information in all or most circumstances. The “restricted” label also specifically applies to sensitive data as defined in Ohio IT Bulletin; ITB-2007.02, “Data Encryption and Securing Sensitive Data.”

5.1.2 Criticality. The criticality label identifies the degree of need for data to maintain its integrity and availability.

5.1.2.1 Data shall be assigned one of four labels for criticality:

- Low. The loss of data integrity or availability would result in insignificant or no financial loss, legal liability, public distrust or harm to public health and welfare.
- Medium. The loss of data integrity or availability would result in limited financial loss, legal liability, public distrust or harm to public health and welfare.
- High. The loss of data integrity or availability would result in significant financial loss, legal liability, public distrust or harm to public health and welfare.
- Very High. The loss of data integrity or availability would result in catastrophic financial loss, legal liability, public distrust or harm to public health and welfare.

- 5.2 Labels Required by Law. State and federal law may require that certain types of data be labeled in a particular manner. DAS shall determine if there are state or federal legal requirements for labeling DAS data and shall assign the labels as required by law.
- 5.2.1 DAS shall determine whether the Electronic Protected Health Information label applies as required by the Health Insurance Portability and Accountability Act for certain types of data.
- 5.3 Classification Methodology. As a classification authority, DAS shall apply the following data classification method for the labeling of DAS data:
- 5.3.1 DAS shall determine if existing laws, regulations or agreements limit or regulate the collection, use, release, access, retention and disposal of DAS owned data, and apply all applicable published requirements, guidelines and limitations.
- 5.3.2 DAS shall work with its customers to apply all customer specified requirements, guidelines, and limitations to the release, access, retention, and disposal of customer-owned, DAS facilitated data.
- 5.3.3 DAS shall define and use a structured decision process to determine an appropriate data classification label for DAS data.
- 5.3.4 DAS shall establish data maintenance guidelines based upon the results of its data classification which address the following components:
- Creation
 - Access
 - Storage
 - Modification
 - Retention
 - Archive
 - Disposal
 - Distribution
- 5.3.5 DAS shall establish a review process to adjust data classifications in the event of regulatory changes affecting management of DAS information.
- 5.4 Data Ownership. Authorized DAS personnel will designate an information owner responsible for establishing data use guidelines. An information owner shall not be a data or system administrator, but rather the head of a business or program area. In most cases for DAS facilitated data, the information owner will be a designated representative from the customer's organization. DAS customers are responsible for classifying their data and for informing DAS as to its levels of confidentiality and criticality.

DAS information owners shall be responsible for the identification and classification of information for which they have been designated and shall address the following:

- 5.4.1 Assignment of Data Classification Labels. The owner of DAS data shall assign data classification labels based on DAS' business requirements, risk assessment, and FIPS 199.
- 5.4.2 Data Compilation. The owner of DAS information shall ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data.
 - 5.4.2.1 Summary data drawn from various information sources may be classified at a level less restrictive than the original information so long as the individual data from which the summary is derived is not revealed or apparent.
- 5.4.3 Coordinate Data Classification. The owner of DAS information shall ensure that data shared between DAS and other agencies is consistently classified.
- 5.4.4 Data Classification Compliance. The owner of DAS information in conjunction with DAS management and system administrators shall ensure that confidential or personally identifiable information is safeguarded in accordance with applicable federal or state regulations and guidelines.
- 5.4.5 Downloading Data. The owners of DAS information in conjunction with DAS management and system administrators shall explicitly define guidelines and limitations for data classifications with respect to remote systems and portable computing devices in accordance with DAS Policy 2100-02, "Mobile Computing."
- 5.4.6 Data Access. DAS information owners in conjunction with DAS management and system administrators shall develop data access guidelines for each data classification label. More secure levels of data classification shall require more stringent access qualifications.
- 5.5 Contracts. DAS shall ensure that data classification requirements are incorporated into contractor service level agreements and contract terms and conditions as they relate to classified DAS data.
- 5.6 Education and Awareness. DAS shall establish education and awareness programs covering data classification; as a minimum, education and awareness topics shall include the following:
 - 5.6.1 Data classification labels and guidelines for DAS owned or facilitated data.

- 5.6.2 Distribution and disclosure guidelines for DAS owned or facilitated data.
- 5.6.3 Reporting requirements for theft, disclosure, accidental release, or unauthorized modification of DAS owned or facilitated data.
- 5.6.4 Impact or risk of data loss, disclosure, release or modification of DAS owned or facilitated data.
- 5.7 Legal Review. DAS Program Administrators shall coordinate a legal review of all DAS data classification labels to ensure compliance with any laws, regulations, or agreements that regulate the collection, use, release, access, retention, or disposal of DAS data.

6.0 RELATED PROCEDURES

Standards and procedures shall be developed at various levels within the DAS organization in order to effectively and efficiently implement this policy. These standards and procedures shall implement a data classification methodology that is consistent across DAS.

7.0 IMPLEMENTATION

This policy requires that DAS data must be appropriately classified and that certain related controls must be put in place. As of the effective date of this policy, DAS will likely not be able to immediately meet all the data classification requirements of the policy. Data classification will take time to implement.

Given these understandings, DAS' general framework for implementation includes:

- 7.1 Data applicable to DAS initiatives begun after the effective date of this policy shall be appropriately classified. The results of the classification shall guide systems design and related business rules development.
- 7.2 If there is reasonable opportunity, data applicable to DAS initiatives begun but not yet implemented as of the effective date of this policy shall be appropriately classified. The results of the classification shall guide systems design and related business rules development.
- 7.3 DAS data managed by systems replaced or substantially upgraded after the effective date of this policy shall be appropriately classified. The results of the classification shall guide systems design and related business rules development.
- 7.4 DAS data managed by systems already in place and operational shall be appropriately classified, if not already, within a reasonable amount of time in consideration of the risk, complexity, and capability of DAS' environment with priority given to data deemed mission critical or sensitive. A review of the system design and related business rules in consideration of the results of the classification shall be conducted.

- 7.5 For data owned by customers but facilitated by DAS, DAS shall ask customers to inform DAS of the data's classification as soon as it is feasible for the customers to do so.

8.0 COMPLIANCE

It is the responsibility of management to implement and ensure compliance with the laws, rules, policies, procedures, standards, and license agreements applicable to the use of IT resources within their functional areas.

9.0 DEFINITIONS

Availability – The assurance that information and services are delivered when needed. Certain data must be available on demand or on a timely basis.

Classification Authority - Entity with the authority to classify data according to confidentiality and criticality.

DAS – Department of Administrative Services.

DAS Contractors – For the purposes of this policy, DAS contractors are defined as contracted staff and vendor technicians.

DAS Employees – For the purposes of this policy, DAS employees are defined as all employees and representatives of DAS, whether they are permanent staff or temporary staff.

DAS-owned – Purchased with DAS funds or otherwise acquired by DAS; property of DAS.

DAS-provided or **DAS-supplied** – Made available to users by DAS.

Data - Coded representation of quantities, objects, and actions. Data is often used interchangeably with information in common usage and in this policy.

Data Classification Label - Denotes the level of protection based on the criticality and confidentiality requirements of data in accordance with the agency's risk assessment. Data classification labels enable policy-based standards for handling data and sharing information among organizations. The terms data classification label and classification label are used interchangeably.

Data Compilation – Data collected and grouped together from various sources.

Data Owner – See Information Owner.

Information – Data processed into a form that has meaning and value to the recipient to support action or decision. Information is often used interchangeably with data in common usage and in this policy.

Information Owner - Individual or group responsible for classifying information and generating guidelines for its lifecycle management.

Integrity – The assurance that information is not changed by accident or through a malicious or otherwise criminal act. Because businesses, citizens and governments depend upon the accuracy of state data, agencies must ensure that data is protected from improper change.

IT Resources – Any information technology resources, such as computer hardware and software, IT services, telecommunications equipment and services, networks, digital devices such as digital copiers and facsimile machines, supplies, and the Internet.

Management – Management refers to supervisory staff responsible for the completion of activities to fulfill DAS' mission. If Position A is shown as subordinate to Position B on the Table of Organization, then Position B is supervisory in nature for the purposes of this policy.

OIT – Office of Information Technology.

Personally Identifiable Information - Information that can be used to directly or indirectly identify a particular individual. (See Personal Information.)

Personal Information – An individual's last name along with the first name or first initial, in combination with one or more of the following data elements: social security number; driver's license number; state identification card number; financial account number; or credit or debit card number. (See Personally Identifiable Information.)

Portable Computing Device - Computers or devices designed for mobile use. Examples include laptops, personal digital assistants and mobile data collection devices.

Privately-owned - Purchased with personal or corporate (vendor or contractor) funds; not provided by the state.

Public Record – Any record defined as public by the Ohio Revised Code.

Risk Assessment – A process for identifying, analyzing and responding to information technology security risks. Risk assessment attempts to maximize the results of positive events and minimize the results of negative events.

Sensitive Data – Means any electronic information that an agency collects and maintains but must keep confidential as required by law. It also includes "personal information". (See Personal Information.)

Service Level Agreement (SLA) - Defines the services to be delivered, technical support and other parameters that a business or supporting activity is required to deliver contractually. The SLA should describe measures and penalties for failure to perform in accordance with the SLA.

State-owned - Purchased with state funds or otherwise acquired by the state; property of the state of Ohio.

System Assets – System assets include information, hardware, software, and services required to support the business of DAS and identified during the risk assessment process as assets that require protection.

Terms and Conditions - Language included in a contract that describes the limits and expectations related to delivery of requested goods and services.

Users - For the purposes of this policy, users are defined as employees, contractors, temporary personnel and other agents of the state who administer or use privately-owned (if authorized) or state-owned IT Resources on behalf of the state.

10.0 INQUIRIES

For information regarding this policy, please contact:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, Suite 4083
Columbus, Ohio 43215
Telephone: 614.644.9391
Email: state.isp@oit.ohio.gov
Web: infosec.ohio.gov

Department of Administrative Services policies can be found online at:

<http://das.ohio.gov/Divisions/DirectorsOffice/EmployeeServices/DASPolicies/tabid/463/Default.aspx>

11.0 REVISION HISTORY

Date	Description
12/01/2009	New policy for DAS, replaces OIT policy dated 11/02/07
12/05/2012	Policy reissued under Director Robert Blair.

12.0 ATTACHMENTS

None.