



State of Ohio Administrative Policy

Data Classification

No: Information Technology
IT-13

Effective: July 1, 2015

Issued By: 

Robert Blair, Director

1.0 Purpose

This state policy provides a ***data*** classification methodology to state agencies for the purpose of understanding and managing data and ***information*** systems with regard to their level of ***confidentiality*** and criticality. The accurate identification of data helps to ensure that the appropriate security controls are selected and implemented to protect data from unauthorized access or misuse.

A glossary of terms found in this policy is located in Appendix A - Definitions. The first occurrence of a defined term is in ***bold italics***.

2.0 Policy

Data classification is a process that identifies what information needs to be protected against unauthorized access, misuse and the extent to which it needs to be secured and controlled. Each agency shall serve as a ***classification authority*** for the data and information that it collects or maintains in fulfilling its mission.

2.1 ***Data Classification Labels***: The classification of data is a critical tool in defining and implementing the correct level of protection for state information assets. Such classifications are a prerequisite to establishing agency guidelines and system requirements for securing state data throughout its life cycle.

Agencies shall label data for both confidentiality and criticality. Such classification labels are defined at a high level and represent broad categories of information. State and federal law may also require specific labels, such as “protected health information” under the Health Insurance Portability and Accountability Act (HIPAA), “federal tax information” under IRS Publication 1075, and “confidential personal information” under section 1347.15 of the Ohio Revised Code (ORC).

2.1.1 **Confidentiality**: The classification label identifies how sensitive the data is with regard to unauthorized disclosure. “Adverse effects” on individuals may include, but are not limited to, the loss of privacy. Data shall be assigned one of three confidentiality labels:

2.1.1.1 **Confidentiality Low (Public)**: This classification 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. The inappropriate use or unauthorized disclosure of information designated as “confidentiality low” would have a limited adverse effect on State of Ohio interests, the conduct of agency programs, or individuals. A limited adverse effect means that, for example, the loss of confidentiality might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals, including privacy.

2.1.1.2 **Confidentiality Moderate**: This classification includes information that the agency has discretion to release or not release under Ohio public records law but otherwise has no use or disclosure limitations imposed by law. This classification may also include information that may be a public record but requires a review for context or disclosure limitations before it is released. For example, a list of employees of the agency may be a public record but a list of employees conducting a specific undercover investigation may not be for a given period of time. Disclosure to parties outside the state agency shall be authorized by executive management or the Data Owners and General Counsel or in accordance with a formal agency process. Disclosure of confidentiality moderate information internal to the state agency shall be on a need-to-know basis only. Information falls into this classification if its inappropriate use or unauthorized disclosure would have a serious adverse effect on State of Ohio interests, the conduct of agency programs, or individuals. A serious adverse effect means that, for example, the loss of confidentiality might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals, that does not involve loss of life or serious life threatening injuries.

2.1.1.3 **Confidentiality High**: This classification includes information protected by statutes, regulations, State of Ohio policies, or contractual language that restrict the use or disclosure of information solely to the conditions

identified in the statute, regulation, policy or contract. Disclosure to parties outside the state agency shall be authorized by executive management and/or the Data Owners and General Counsel. Disclosure of confidentiality high information internal to the state agency shall be on a need-to-know basis only. Information falls into this classification if its inappropriate use or unauthorized disclosure would have a severe or catastrophic adverse effect on State of Ohio interests, the conduct of agency programs, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries. Disclosure restrictions in State of Ohio regulations, policies, or contracts must be consistent with Ohio's public records law.

2.1.1.4 In addition to Ohio IT Standard ITS-SEC-02, "Enterprise Security Controls Framework," specific security requirements for confidential data are outlined in Ohio Administrative Policy IT-14, "Data Encryption and Securing Sensitive Data."

2.1.2 **Criticality:** The criticality label identifies the degree of need for data to maintain its **integrity** and **availability**. Data shall be assigned one of three labels for criticality:

2.1.2.1 **Criticality Low:** The loss of data integrity or availability would result in limited adverse effect. A limited adverse effect means that, for example, the loss of integrity or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals, including privacy.

2.1.2.2 **Criticality Moderate:** The loss of data integrity or availability would result in a serious adverse effect. A serious adverse effect means that, for example, the loss of integrity or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals, that does not involve loss of life or serious life threatening injuries.

2.1.2.3 **Criticality High:** The loss of data integrity or availability would result in severe or catastrophic adverse effect. A severe or catastrophic adverse

effect means that, for example, the loss of integrity or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

2.2 **Classification Methodology:** Agencies shall systematically go through a data classification process and shall document their classification decisions. The process shall include, but not be limited to, the following steps:

2.2.1 Define and use a structured decision process to determine an appropriate data classification label.

2.2.2 Determine whether existing laws, regulations or agreements limit or regulate the collection, use, disclosure, access, retention and disposal of state data. Agencies shall use all applicable published requirements, guidelines and limitations.

2.2.3 Specifically, for ***personally identifiable information***, agencies shall complete a privacy impact assessment, required by ORC 125.18(C)(2) and ORC 1347.15(B)(8).

2.2.4 Based upon the results of the agency's data classification, establish data maintenance guidelines, which address each of the following data life-cycle components:

- Source(s)
- Creation
- Access
- Use(s)
- Disclosure
- Storage
- Modification
- Retention
- Archive
- Disposal

2.2.5 Establish a process to regularly review the appropriateness of the assigned data classifications and to adjust classifications in the event of:

2.2.5.1 Regulatory changes affecting an agency's management of information under its control.

2.2.5.2 Technologies for which data classification policies do not yet exist. Technologies may include but are not limited to:

- Cloud (Private, public and hybrid)

- Mobility
- Personal Devices
- Social Networks

2.3 **Data Classification Roles and Responsibilities:** The following list identifies the roles and responsibilities associated with data classification. Agencies shall designate individuals who will be responsible for carrying out the duties associated with each of the required roles.

2.3.1 **Data Owner:** Authorized agency personnel shall designate a data owner from a business or program area. The data owner shall be responsible for the identification and classification of information, in consultation with legal counsel, and shall address the following:

2.3.1.1 **Assignment of Data Classification Labels:** The data owner shall assign data classification labels based on the agency's business requirements and risk assessment.

2.3.1.2 **Data Compilation:** The data owner shall ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data.

2.3.1.2.1 Summary data drawn from various information sources may be classified at a lower level of confidentiality than the original information so long as the individual data from which the summary is derived is not revealed or apparent.

2.3.1.3 **Data Classification Coordination:** The data owner shall ensure that data shared between agencies is consistently classified and protected in accordance with a documented agreement detailing, at a minimum, data treatment requirements.

2.3.1.4 **Data Classification Compliance:** The data owner, in conjunction with information technology personnel, shall ensure that sensitive or personally identifiable information is secured in accordance with applicable agency requirements, and federal or state regulations and guidelines.

2.3.1.5 **Data Access:** Data owners, in conjunction with information technology personnel, shall develop data access guidelines for each data classification label. More secure levels of data classification shall require more stringent access qualifications.

2.3.1.5.1 Agencies shall ensure that data access requirements are incorporated into contractor service level agreements and contract terms and conditions as they relate to classified data.

- 2.3.2 **Data Custodian**: In general, data custodians shall be responsible for the safe custody, transport, and storage of state data as well as the implementation of any applicable federal, state, or agency data protection requirements. Some specific data custodian responsibilities include:
- 2.3.2.1 **Access Controls**: Assure that proper access controls are implemented, monitored and audited for building, floor and/or cage access in accordance with the data classification labels assigned by the data owner.
 - 2.3.2.2 **Audit Reports**: Submit an annual report to the data owners which addresses security, availability, processing integrity, confidentiality and privacy.
 - 2.3.2.3 **Data Backups**: Perform regular backups of state data.
 - 2.3.2.4 **Data Validation**: Periodically validate data integrity.
 - 2.3.2.5 **Data Restoration**: Restore data from backup media.
 - 2.3.2.6 **Ensure Compliance**: Fulfill the data requirements specified in agency security policies, standards and guidelines pertaining to information security and data protection.
 - 2.3.2.7 **Monitor Activity**: Retain records of data activity that include information on who accessed the data and what data was accessed.
 - 2.3.2.8 **Secure Storage**: Provide for encryption of **sensitive data** at rest while in storage. Audit SAN “storage area network” administrator activity and review access logs regularly.
 - 2.3.2.9 **Web/Server hosting**: Provide reasonable and appropriate security controls for hosting services according to the data classification labels assigned by the data owners.
- 2.3.3 **Data User**: Person, organization or entity that interacts with, accesses, uses, or updates data for the purpose of performing a task authorized by the data owner.
- 2.3.3.1 **Data Use Expectations**: Particular types of data may carry use limitations. For example, section 1347.15 of the ORC requires agencies to develop rules, policies, and training that establish valid reasons for

accessing confidential personal information. Data users must use data in a manner consistent with the purpose intended, and comply with this policy and all policies applicable to data use.

2.4 **Education and Awareness:** Agencies shall provide data classification education and awareness training that is designed to complement the roles and responsibilities outlined in section 2.3 of this policy. Agencies shall address the following topics as part of their training efforts:

2.4.1 The process for identifying and assigning data classification labels and guidelines for state data.

2.4.2 Distribution and disclosure guidelines.

2.4.3 Impact or risk of data loss, disclosure, release, or modification.

2.4.4 Reporting requirements for theft, disclosure, accidental release, or unauthorized modification of information.

2.5 **Compliance Reviews:** Agencies shall conduct regular compliance reviews with relevant staff (e.g., IT, policy, communications, resources in designated data roles and legal personnel) of all data classification labels to ensure compliance with any state or agency policies, and with federal, state and local laws that regulate the collection, use, release, access, retention and disposal of state data.

2.5.1 Agencies shall ensure that data classification is determined during the design phase when planning a new IT system.

2.5.2 Agencies that do not have IT personnel shall contact the DAS OIT Office of Information Security & Privacy to determine an appropriate approach for compliance.

3.0 Authority

ORC 125.18

4.0 Revision History

Date	Description of Change
07/01/2015	Original Policy.
03/27/2018	Added an entry into Appendix B Resources that refers to the DAS Office of Information Security and Privacy IT Security Tools that are related to data classification.
03/27/2019	Scheduled policy review.

5.0 Inquiries

Direct inquiries about this policy to:

Office of Information Security & Privacy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 19th Floor
Columbus, Ohio 43215

614.644.9391 | state.isp@das.ohio.gov

State of Ohio Administrative Policies may be found online at
www.das.ohio.gov/forStateAgencies/Policies.aspx.

Additional information regarding the Office of Information Security & Privacy may be found online at infosec.ohio.gov.

Appendix A - Definitions

- a. Availability. Ensuring timely and reliable access to and use of information.¹
- b. Classification Authority. Entity with the authority to classify data according to confidentiality and criticality.
- c. Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.²
- d. Data. Coded representation of quantities, objects and actions. The word, “data,” is often used interchangeably with the word, “information,” in common usage and in this policy.
- e. Data Classification Labels. Denotes the level of protection based on the confidentiality and criticality requirements of data in accordance with the agency’s risk assessment. Data classification labels enable policy-based standards for securing and handling data and sharing information among organizations. The terms, “data classification label” and “classification label,” are used interchangeably.³

¹ “NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations,” U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>>.

² *Ibid*.

³ Stine, Kevin, Rich Kissel, William C. Barker, Jim Fahlsing, Jessica Gulick. “NIST Special Publication 800-60 Revision 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories,” U.S. Department of Commerce National Institute of Standards and Technology, August, 2008 <http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf>.

- f. Information. Data processed into a form that has meaning and value to the recipient to support an action or decision. “Information” is often used interchangeably with “data” in common usage and in this policy.
- g. Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.⁴
- h. Personally Identifiable Information (PII). “Personally identifiable information” is information that can be used directly or in combination with other information to identify a particular individual. It includes:
 - a name, identifying number, symbol, or other identifier assigned to a person,
 - any information that describes anything about a person,
 - any information that indicates actions done by or to a person,
 - any information that indicates that a person possesses certain personal characteristics.
- i. Sensitive Data. Sensitive data is any type of computerized data that presents a high or moderate degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. It includes Federal Tax Information under IRS Special Publication 1075, Protected Health Information under the Health Insurance Portability and Accountability Act, and Criminal Justice Information under Federal Bureau of Investigation’s Criminal Justice Information Services (CJIS) Security Policy. The computerized data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

Appendix B - Resources

Document Name
<i>Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems</i> , February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
<i>NIST Special Publication 800-53, Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations</i> , April 2013. http://csrc.nist.gov/publications/PubsSPs.html
<i>Ohio Administrative Policy IT-14, “Data Encryption and Securing Sensitive Data”</i> http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies.aspx
<i>Ohio Revised Code</i> http://codes.ohio.gov/orc/

⁴ “NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations,” U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>>.

Document Name
<i>Ohio IT Standard ITS-SEC-02, "Enterprise Security Controls Framework"</i> http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITStandards.aspx
<i>Ohio Sunshine Laws, 2015.</i> https://ohioauditor.gov/publications/15SunshineManual.pdf
<i>DAS Office of Information Security and Privacy IT Security Tools, including: Data Classification Worksheet; Data Classification Worksheet Training; and Data Classification Training Slides.</i> http://infosec.ohio.gov/Resources/ITSecurityTools.aspx