



<p>State of Ohio IT Policy Data Classification</p>	<p>No: ITP-B.11</p>
	<p>Effective: 03/19/2007</p>
	<p>Issued By: R. Steve Edmonson Director, Office of Information Technology State Chief Information Officer Published By: Statewide IT Policy Investment and Governance Division</p>

1.0 Purpose

This state policy is intended to provide a high-level data classification methodology to state agencies for the purpose of understanding and managing **data** and **information** assets with regard to their level of confidentiality and criticality. Accurate identification provides a basis to employ an appropriate level of security.

2.0 Scope

Pursuant to Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," this state policy is applicable to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government except for those specifically exempted.

The scope of this information technology policy includes state computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the state who use and administer such systems.

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. There may or may not be laws that regulate the use of such data, and agencies may not be certain how to respond to apparent conflicts between privacy, **public records** laws and the need to maintain safety and security. 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 Policy ITP-A.1, “Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services,” defines the authority of the state chief information officer to establish State of Ohio information technology policies as they relate to state agencies’ acquisition and use of information technology, including, but not limited to, hardware, software, technology services and security.
- 4.2 Ohio IT Policy ITP-B.1, “Information Security Framework,” is the overarching security policy for state information and services. Ohio IT Policy ITP-B.11, “Data Classification,” is one of several subpolicies. These security policies should be considered collectively rather than as separate or unrelated. Attachment 1 illustrates the interrelationship of state technology security policies.
- 4.3 Ohio IT Policy ITP-B.5, “Remote Access,” requires state agencies to implement and operate security measures wherever a remote access capability is provided to state systems.
- 4.4 Ohio IT Policy ITP-B.8, “Security Education and Awareness,” requires state agencies to provide information technology security education and awareness to employees and other agents of the state.
- 4.5 Ohio IT Policy ITP-B.9, “Portable Computing Security,” addresses the information technology concerns of **portable computing devices** and provides direction to state agencies for their use, management and control.
- 4.6 A glossary of terms found in this policy is located in Section 9.0 – Definitions. The first occurrence of a defined term is in **bold italics**.

5.0 Policy

State agencies shall establish a data classification policy in compliance with this state policy. Each agency shall serve as a **classification authority** for the data and information that it collects or maintains in satisfaction of its mission.

- 5.1 **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 the secure generation, collection, access, storage, maintenance, transmission, archival and disposal of state data. Data classification shall be part of the agency’s overall **risk assessment** process as outlined in Ohio IT Policy ITP-B.1, “Information Security Framework.”

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.

- 5.1.1 Confidentiality. The confidentiality label identifies how sensitive the data is with regard to unauthorized disclosure. Data shall be assigned one of three labels for confidentiality:
 - 5.1.1.1 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.
 - 5.1.1.2 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.
 - 5.1.1.3 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 discretion to release under public records law exceptions but has chosen to treat the information as highly confidential.
- 5.1.2 Criticality. The criticality label identifies the degree of need for data to maintain its **integrity** and **availability**. Data shall be assigned one of four labels for criticality:
 - 5.1.2.1 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.
 - 5.1.2.2 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.
 - 5.1.2.3 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.
 - 5.1.2.4 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. Agencies shall determine if there are state or federal legal requirements for labeling the data and shall assign the label(s) as required by law.
 - 5.2.1 Agencies 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 classification authorities, agencies shall develop a data classification method for how they label data. Agencies shall:
- 5.3.1 Determine whether existing laws, regulations or agreements limit or regulate the collection, use, release, access, retention and disposal of state data. Agencies shall use all applicable published requirements, guidelines and limitations.
 - 5.3.2 Define and use a structured decision process to determine an appropriate data classification label.
 - 5.3.3 Each agency shall establish data maintenance guidelines based upon the results of its data classification which address the following components in accordance with Ohio IT Policy ITP-B.1, "Information Security Framework:"
 - Creation
 - Access
 - Storage
 - Modification
 - Retention
 - Archive
 - Disposal
 - Distribution
 - 5.3.4 Establish a process to regularly review the appropriateness of the assigned data classifications and to adjust classifications in the event of regulatory changes affecting an agency's management of information under its control.
- 5.4 **Data Ownership.** Authorized agency personnel shall designate an ***information owner*** from a business or program area. The information owner shall be responsible for the identification and classification of information and shall address the following:
- 5.4.1 **Assignment of Data Classification Labels.** The information owner shall assign data classification labels based on the agency's business requirements and risk assessment in accordance with Ohio IT Policy ITP-B.1, "Information Security Framework."
 - 5.4.2 **Data Compilation.** The information owner 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 information owner shall ensure that data shared between agencies is consistently classified.
- 5.4.4 Data Classification Compliance. The information owner in conjunction with agency information technology personnel shall ensure that confidential or **personally identifiable information** is secured in accordance with applicable federal or state regulations and guidelines.
- 5.4.5 Downloading Data. Information owners in conjunction with agency information technology personnel shall explicitly define guidelines and limitations for data classifications with respect to downloading data to remote systems and portable computing devices in accordance with Ohio IT Policy ITP-B.9, "Portable Computing Security," and Ohio IT Policy ITP-B.5, "Remote Access Security."
- 5.4.6 Data Access. Information owners in conjunction with agency 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.
 - 5.4.6.1 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.
- 5.5 Education and Awareness. Agencies shall establish data classification education and awareness efforts in accordance with Ohio IT Policy ITP-B.8, "Security Education and Awareness." As a minimum, agencies shall include the following:
 - 5.5.1 The process for identifying and assigning data classification labels and guidelines for state data.
 - 5.5.2 Distribution and disclosure guidelines.
 - 5.5.3 Reporting requirements for theft, disclosure, accidental release, or unauthorized modification of information.
 - 5.5.4 Impact or risk of data loss, disclosure, release or modification.
- 5.6 Legal Review. Agencies shall conduct a legal review of all data classification labels to ensure compliance with any laws, regulations or agreements that regulate the collection, use, release, access, retention and disposal of state data.

6.0 Procedures

None.

7.0 Implementation

This state policy requires that data must be appropriately classified, and that certain related management controls must be in place.

As of the effective date of this state policy, some agencies will likely not be completely aligned to the requirements of this policy. Given the varying degrees of risk, complexity and capability of each agency's environment, alignment to certain requirements may require a development period.

Given these understandings, a general implementation framework for the requirements of this policy includes:

- 7.1 Data applicable to initiatives begun after the effective date of this policy shall be appropriately classified, the results of which shall inform systems design and related business rules development.
- 7.2 If there is reasonable opportunity, data applicable to initiatives begun but not yet implemented as of the effective date of this policy shall be appropriately classified, the results of which shall inform systems design and related business rules development.
- 7.3 Data managed by systems replaced or substantially upgraded after the effective date of this policy shall be appropriately classified, the results of which shall inform systems design and related business rules development.
- 7.4 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 the agency's 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 A process of incremental efforts toward implementation of the management controls contemplated by this policy shall begin.

8.0 Revision History

Date	Description of Change
03/19/2007	Original policy.
03/19/2011	Scheduled policy review.

9.0 Definitions

- 9.1 Availability. The assurance that information and services are delivered when needed. Certain data must be available on demand or on a timely basis. Information systems that must ensure availability will likely deploy techniques such as uninterrupted power supplies or system redundancy.

- 9.2 Classification Authority. Entity with the authority to classify data according to confidentiality and criticality.
- 9.3 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.
- 9.4 Data Classification Label. Denotes the level of protection based on the confidentiality and criticality requirements of data in accordance with the agency’s risk assessment per Ohio IT Policy ITP-B.1, “Information Security Framework.” 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.
- 9.5 Data Compilation. Data collected and grouped together from various sources.
- 9.6 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.
- 9.7 Information Owner. Individual or group responsible for classifying data and generating guidelines for its lifecycle management.
- 9.8 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 data in state databases, agencies must ensure that data is protected from improper change. Information systems that must ensure integrity will likely deploy techniques such as scheduled comparison programs using cryptographic techniques and audits.
- 9.9 Personally Identifiable Information. Information that can be used to directly or indirectly identify a particular individual.
- 9.10 Portable Computing Device. Computers or devices designed for mobile use. Examples include laptops, personal digital assistants and mobile data collection devices.
- 9.11 Public Record. Public record means any record that is kept by any public office, including, but not limited to, state, county, city, village, township, and school district units. Exceptions include: medical records; probation and parole records, under-age abortion notification records, adoption proceedings; putative father registry records, trial preparation records; confidential law enforcement investigatory records, DNA records stored in the DNA database, inmate records released by the department of rehabilitation and correction to the department of youth services or a court of record, records maintained by the department of youth services pertaining to children in its custody released by the department of youth services to the department of rehabilitation and correction, intellectual property records, donor profile records and all records the release of which is prohibited by state or federal law (Ohio Revised Code 149.43).

- 9.12 Risk Assessment. A process concerned with 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. See Ohio IT Policy ITP-B.1, "Information Security Framework," for assessment guidelines.
- 9.13 Service Level Agreement. Defines the services to be delivered, technical support and other parameters that a business or supporting activity is required to deliver contractually. The service level agreement should describe measures and penalties for failure to perform in accordance with the service level agreement.
- 9.14 Terms and Conditions. Language included in a contract that describes the limits and expectations related to delivery of requested goods and services.

10.0 Related Resources

Document Name
Chapter 149 of the Ohio Revised Code includes companion provisions to this policy with regard to records management requirements and public records requirements. Section 149.433 of the Ohio Revised Code specifically addresses information technology security records.
Chapter 1306 of the Ohio Revised Code and Rule 123:3-1-01 of the Ohio Administrative Code specifically govern the use of legally binding records and signatures in electronic formats and includes companion security requirements to this policy.

11.0 Inquiries

Direct inquiries about this policy to:

Statewide IT Policy
Investment and Governance Division
Ohio Office of Information Technology
30 East Broad Street, 39th Floor
Columbus, Ohio 43215

Telephone: 614-644-9352
Facsimile: 614-644-9152
E-mail: State.ITPolicy.Manager@oit.ohio.gov

Ohio IT Policy may be found on the Internet at: www.ohio.gov/itp.

12.0 Attachments

- 12.1 Attachment 1 – Interrelationship of the Information Security Framework Policy and Subpolicies. A cross-reference table showing the relationship between the primary framework policy and the subpolicies.

Attachment 1

**Interrelationship of the Information Security Framework Policy
and Subpolicies**

Information Security Framework Practices	Risk Management	Confidentiality	Integrity	Availability	Protect, Detect and Respond	Identification & Authentication	Access Control & Authorization	Security Audit Logging	Security Management & Administration
Information Security Framework Policy Paragraphs	5.1	5.2	5.2	5.2	5.3	5.4	5.5	5.6	5.7
SUBPOLICIES									
Boundary Security (B.2)	X			X	X	X	X	X	X
Business Resumption (E.7)	X			X	X				X
Data Classification (B.11)	X	X	X	X	X	X	X	X	X
Disposal, Servicing and Transfer of IT Equipment (E.1)	X	X							X
Internet Security (B.6)	X					X	X		X
Intrusion Prevention and Detection (B.12)	X		X		X		X	X	X
Malicious Code Security (B.4)	X		X		X				X
Password & PIN Security (B.3)	X	X			X	X	X	X	X
Portable Computing Security (B.9)	X	X				X	X	X	X
Remote Access Security (B.5)	X	X		X		X	X	X	X
Security Education and Awareness (B.8)	X	X	X	X	X	X	X	X	X
Security Incident Response (B.7)	X		X	X	X			X	X
Security Notifications (B.10)	X	X			X	X	X		X