



Ohio

Department of Taxation

John Kasich, Governor
Joseph Testa, Tax Commissioner

30 E. Broad St., 22nd Floor
Columbus, Ohio 43215

(614) 466-2166
Fax (614) 466-6401

POLICY

Policy: Data Classification	Number: ODT-307	Effective: September 14, 2015
Issued By: Joseph Testa (Original signature on file with Internal Audit)	Published By: Information Services Division	Three Year Review Date: September 14, 2018

1. Authority

The Tax Commissioner issues Ohio Department of Taxation (herein referred to as the “Department”) Policy ODT-307 in accordance with Ohio Revised Code (O.R.C.) § 5703.05. O.R.C. § 5703.05 grants the Tax Commissioner powers, functions, and duties including the authority to manage and direct the Department’s operations.

2. Purpose

The purpose of this policy is to provide a methodology for understanding, managing and protecting Department information 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, disclosure and misuse.

3. Applicability

This policy applies to all Department employees and contractors.

4. Definitions

- 4.1. **Availability** – Ensuring timely and reliable access to and use of information.
- 4.2. **Classification Authority** – Entity with the authority to classify data according to confidentiality and criticality.
- 4.3. **Confidentiality** – Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- 4.4. **Confidential Personal Information (CPI)** - Personal information that is not a public record for purposes of section 149.43 of the O.R.C.
- 4.5. **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.
- 4.6. **Data Classification Labels** – Denote 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 in this policy.
- 4.7. **Federal Tax Information (FTI)** - Federal tax returns or return information received from the Internal Revenue Service (IRS).

- 4.8. **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.
- 4.9. **Integrity** – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- 4.10. **Personally Identifiable Information (PII)** – 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.
- 4.11. **Sensitive Data** – Sensitive data is any type of computerized data that presents a high or medium 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 medium 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. 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.

5. Policy

Data classification is a process that identifies information that needs to be protected against unauthorized access and misuse, and the extent to which it needs to be secured and controlled.

- 5.1. **Responsibility for Data Management** – Data is a critical asset of the Department, its business partners and its taxpayers. All employees and contractors of the Department have the responsibility to protect the confidentiality, integrity and availability of the data generated, accessed, modified, transmitted, stored and/or used by the Department, irrespective of the medium on which the data resides and regardless of format (e.g., electronic, paper or other form).

5.2. Roles for Data Management

- 5.2.1. **Data User** – The data user is a person, organization or entity that interacts with, accesses, uses or updates data for the purpose of performing a task authorized by Department personnel. The data user is responsible for (i) using data in a manner consistent with the purpose intended, and (ii) complying with this policy and all other policies applicable to such use of the data.

- 5.2.2. **Data Owner** – The data owner is the person responsible for, or dependent upon, the business process associated with an information asset. The data owner should be knowledgeable about how the information is acquired, transmitted, stored and otherwise processed. The data owner:

- determines the appropriate value and classification of information generated by, or at the request of, the owner or division,
- must communicate the information classification to the external data user of the information when the information is released outside of the Department,
- controls access to the information and must be consulted when access is extended to others or modified by others,
- must communicate to the data custodian the information classification so that the data custodian may provide the appropriate level of protection.

Each business unit will designate a data owner for that business unit who will be responsible for the duties listed above.

- 5.2.3. **Data Custodian** – The data custodian maintains the protection of data according to the information classification associated with it by the data owner. The data custodian role is delegated by the data owner and is usually personnel from the Department’s Information Services Division.
- 5.2.4. **Data Classifications** – Data owned, used, created or maintained by the Department is classified into one of the following three confidentiality categories:
- Public
 - Limited
 - Restricted
- 5.2.4.1. Public classification is information that must be released under Ohio public records law or instances where an agency unconditionally waives an exception to the public records law. Examples of public access data include the following:
- press releases,
 - job announcements,
 - Vendors License numbers.
- Disclosure of public data must not violate any pre-existing non-disclosure agreements.
- 5.2.4.2. Limited classification is information that the Department may release if it chooses to waive an exception to the public records law and places conditions or limitations on such a release. This data is protected from unauthorized access, modification, transmission, storage or other use. This information is restricted to data owner designated personnel who have a legitimate business purpose for accessing such data. Examples of limited access data include the following:
- employment data,
 - taxpayer demographic information,
 - taxpayer summary information.
- Limited access data must be:
- protected by the data custodian to prevent loss, theft, unauthorized access and/or unauthorized disclosure,
 - protected by confidentiality agreement between the Department and the data user before access is allowed,
 - stored by the data user in a closed container (e.g., file cabinet, closed office, or area where physical controls are in place to prevent disclosure) when not in use,
 - destroyed in accordance with the Department’s data retention policy when the data is no longer needed.
- 5.2.4.3. Restricted data is information that state or federal law prohibits from disclosure of release. This category of data also applies to records that the Department has discretion to release under public records law exceptions but has chosen to treat the information as highly confidential. Examples of restricted data include the following:
- FTI,
 - CPI,
 - security records such as physical security documents, detailed computer system documentation.
- Access to restricted data is limited to individuals who have a business-related need and have been granted proper authority/permissions. Disclosure to parties outside of the Department must be approved either by a Deputy Tax Commissioner and/or Chief Information Officer, or be covered by a binding confidentiality agreement between the Department and the external data user.
- Restricted data must be:
- protected by the data custodian with a minimum level of authentication to include strong passwords,
 - encrypted by the data custodian or data user when stored on mobile devices and media; encryption must meet best practice industry standards,

- stored by the data user in a locked drawer, room or area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know,
- encrypted by the data custodian with strong encryption when transferred electronically to any entity outside the Department,
- destroyed in accordance with the Departments data retention policy when the data is no longer needed.

Restricted is the default classification level unless the data owner specifically designates another data classification.

5.2.5. **Data Criticality** – The criticality label identifies the degree of need for data to maintain its integrity and availability. Data owned, used, created or maintained by the Department shall be assigned one of three labels for criticality:

- Low
- Medium/Moderate
- High
- Very High/Extreme¹

Data Criticality Classification Scale			
	Low	Medium	High
Effect of Data Loss	None or slight	Duration: < 1 day Staff impact: <10% of agency staff downtime, system downtime, project delay	Duration: > 1 day Staff Impact: > 10% of agency staff downtime; impacts mission critical process
Financial Remediation	None or slight	< \$25K (within agency spending authority)	\$ amount requires OIT or controlling board approval
Financial Sanctions	None or slight	< \$25K (within agency spending authority)	\$ amount requires OIT or controlling board approval
Legal Impact	None or slight	Limited risk associated with a civil suit; limited regulatory requirements	Significant risk associated with a civil suit; stringent regulatory requirements
Reputation	None or slight	Intense media scrutiny; budget reductions; loss of political capital	Loss of public confidence; loss of legislature support/funding

5.3. **Directives and Policies of the Ohio Department of Administrative Services (DAS) with applicability to Departmental operations** - In addition to Departmental policies, DAS establishes

¹ Very High/Extreme criticality classification is for data which, if compromised, would result in catastrophic loss such as serious injury or loss of life, loss equal to 100% of the agency budget, and/or loss of statutory authority. This criticality classification is not applicable to the Department.

directives and policies with applicability to the Department's operations. As provided in Departmental Policy ODT-002, Section 5.3.3. Statewide Information Technology (IT) Standards, employees must comply with State of Ohio IT statutes, rules, orders, policies, bulletins, procedures, and standards. Employee may obtain copies of these policies from human resources or on DAS's website by opening the following hyperlink: [DAS > Information Technology > State of Ohio IT Policies](#).

6. Procedures

- 6.1. Compliance Reviews – Data classifications shall be reviewed and documented by the data owner on a periodic basis, the frequency of which is determined by the data owner. The review should generally include a review of the following items: (i) the data (content); (ii) any regulations governing the data (old and new); (iii) access levels/roles associated with the data; (iv) data user access rights; (v) data sharing and confidentiality agreements.
- 6.2. **Notification of Disclosure** – The Department employee or agent who intends to disclose taxpayer CPI or FTI must, prior to such disclosure to any party other than (i) other Department representatives who have a business-related need for such information, and (ii) the taxpayer and/or the taxpayer's representative, obtain from the Department's Disclosure Officer permission to disclose the taxpayer's CPI or FTI. The Department is required by federal regulations to notify the Internal Revenue Service 45 days prior to the disclosure of FTI. This requirement to obtain permission from the Department's Disclosure Officer also applies to contractors and subcontractors.

Any Department employee or agent who discovers any disclosure of information categorized as Limited or Restricted, and not authorized in accordance with the policy must immediately inform the Department's IT Security Manager and the Department's Disclosure Officer of such disclosure. The Department is required by law to report to affected outside persons and entities unauthorized disclosures of CPI or FTI. There may also be additional reporting requirements of non-public data classifications and/or data categories.

- 6.3. **Education and Awareness** - Data classification topics are addressed in the Department's annual disclosure training and other security-related training (e.g., Securing the Human).

7. Administrative Consequences

Employees and contractors may be held civilly or criminally liable for violating laws related to unauthorized disclosure of sensitive information. Employees or contractors may also be subject to disciplinary action, up to and including termination or contract termination, for failure to follow this and other policies related to Departmental networks, email or other IT resources.