



  
**POLICY**  
*Ohio Department of Taxation*

**Policy Description:**  
Data Classification

---

**Policy No:** ODT – IT - 007

---

**Authorities:**

IRS Publication 1075 – Tax Information Security Guidelines for  
Federal, State and Local Agencies and Entities  
ITP-B.11, State of Ohio IT Policy, Data Classification

**Pages:** 5 Pages

---

**Effective Date:** April 6, 2009

**Division With Primary Responsibility:**

Information Services Division

**Revised Date:**

---

**1.0 Purpose**

The purpose of this policy is to provide a system for protecting information that is critical to the Ohio Department of Taxation (ODT), its fellow business partners, and its taxpayers. In order to provide more appropriate levels of protection to the information assets entrusted to ODT, data must be classified according to the risks associated with the following components:

- Creation
- Access
- Storage
- Modification
- Retention
- Archive
- Disposal
- Distribution

Consistent use of this data classification policy will ensure the efficacy of ODT’s process of identifying (i) the information needs to be protected against unauthorized access, use or abuse, and (ii) the extent of that protection.

**2.0 Scope**

This policy applies equally to any individual, and process that interacts with or uses ODT information resources in any manner. All personnel who may come in contact with “Limited Access” or “Restricted” information must familiarize themselves with and adhere to this policy.

**3.0 Policy**

**3.1 Responsibility for Data Management**

Data is a critical asset of ODT, its business partners, and its taxpayers. All individuals employed by ODT have the responsibility to protect the Confidentiality, Integrity, and Availability of the data generated, accessed, modified, transmitted, stored and/or used by ODT, irrespective of the medium on which the data resides and regardless of format (i.e. electronic, paper or other physical form).

**3.1.1 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 other ODT personnel. A 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.

### **3.1.2 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, deleted, 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;
- The Data Owner must communicate the information classification to the external data user of the information when the information is released outside of the division and/or ODT;
- The Data Owner controls access to his/her information and must be consulted when access is extended to others or modified by others; and
- The Data Owner must communicate to the Data Custodian the information classification so that the Data Custodian may provide the appropriate levels of protection.

### **3.1.3 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 Information Services Division (ISD) personnel.

## **3.2 *Data Classifications***

### **3.2.1 Data Confidentiality**

Data owned, used, created or maintained by ODT is classified into one of the following three confidentiality categories:

- Public
- Limited Access
- Restricted

#### **3.2.1.1 *“Public” Classification***

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 data include the following:

- Publicly posted press releases
- Publicly posted job announcements
- Publicly posted information such as Vendors License numbers

Disclosure of public data must not violate any pre-existing non-disclosure agreements.

#### **3.2.1.2 *“Limited Access” Classification***

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. 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 ODT and the data user before access is allowed.
- Stored by the data users in a closed container (i.e., file cabinet, closed office, or division where physical controls are in place to prevent disclosure) when not in use.
- Destroyed in accordance with ODT’s Data Retention policy when the data is no longer needed by ODT.

### 3.2.1.3 “Restricted” Classification

Information that state or federal law prohibits from disclosure or release. This category of data also applies to records that ODT 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:

- Federal Tax Information (FTI)
- Personally Identifiable Information (PII). PII is a person’s name (when stored in combination or linked to one of the items below)
  - Social Security Number
  - Taxpayer identification number
  - Driver’s license number or state identification card number
  - Medical information
  - Information that can be used to access financial resources (such as bank account number, credit or debit card number, EFT numbers, etc.); or
  - Other personal information required by law to be maintained in a secure manner
- Security records such as physical security documents, detailed computer system documentation, etc.

Access to restricted data is limited to individuals on a “need-to-know” basis. Disclosure to parties outside of ODT must either be approved by a Deputy Tax Commissioner and/or Chief Information Officer or be covered by a binding confidentiality agreement between ODT 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 the standard outlined in ITS-SEC-01, Data Encryption and Cryptography standard.
- Stored by the data users 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 ODT.
- Destroyed in accordance with ODT’s Data Retention policy when the data is no longer needed by ODT.

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

### 3.2.2 **Data Criticality**

Data criticality is used to identify the degree of need for the data to maintain its integrity and availability. Data owned, used, created or maintained by ODT is classified by the data owner into one of the following three criticality categories:

- Low
- Medium/Moderate
- High
- Very High/Extreme<sup>1</sup>

<b>Data Criticality Classification Scale</b>			
	<b>Low</b>	<b>Medium</b>	<b>High</b>
<b>Effect of Data Loss</b>	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
<b>Financial Remediation</b>	None or slight	< 25K (within agency spending authority)	\$ amount requires OIT or controlling board approval
<b>Financial Sanctions</b>	None or slight	< 25K (within agency spending authority)	\$ amount requires OIT or controlling board approval
<b>Legal Impact</b>	None or slight	Limited risk associated with a civil suit; limited regulatory requirements	Significant risk associated with a civil suit; stringent regulatory requirements
<b>Reputation</b>	None or slight	Intense media scrutiny; budget reductions; loss of political capital	Loss of public confidence; Loss of legislature support/funding

#### 3.2.2.1 **Low Criticality**

Definition: The loss of data integrity or availability would result in insignificant or no financial loss, legal liability, or public distrust. The data is readily accessible from another source and/or easily recoverable, and not critical to normal business functions.

- Statistical, reporting or summary data for a monthly status report

#### 3.2.2.2 **Medium/Moderate Criticality**

Definition: The loss of data integrity or availability would result in limited financial loss, legal liability, or public distrust. The data is difficult to obtain from another sources, difficult to recover, or is important to normal business functions.

- Business taxpayer data

#### 3.2.2.3 **High Criticality**

Definition: The loss of data integrity or availability would result in significant financial loss, legal liability, or public distrust. Data is unavailable from another sources, unrecoverable, or mission critical to normal business functions.

<sup>1</sup> 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 ODT.

- Banking or credit card information
- Federal tax information
- Individual taxpayer data
- Personally Identifying information

#### **3.2.2.4 Very High/Extreme Criticality**

Definition: The loss of data integrity or availability 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 ODT.

### **3.3 Data Labels**

Data labels are applied to data based on the data owners classification of the data.

### **3.4 Data Classification Reviews**

Data classifications and data management plans are reviewed by the Data Owner on a regular basis. The frequency of the review is determined by the Data Owner. The review includes the following items:

- Review the data (content)
- Review any regulations governing the data (old and new)
- Review access levels/roles associated with data
- Review data user access rights
- Review data sharing and confidentiality agreements

### **3.5 Notification of Disclosure**

The ODT representative who intends to disclose taxpayer FTI must, prior to such disclosure to any party other than (i) other ODT representatives who have a need to know such information and (ii) the taxpayer and/or the taxpayer's representative, obtain from the ODT Disclosure Officer permission to so disclose the taxpayer's FTI. ODT is required by federal regulations to notify the Internal Revenue Service of such disclosures 45 days prior to the disclosure. This requirement to obtain permission from the ODT Disclosure Officer also applies to contractors and sub-contractors.

Each ODT representative who discovers any disclosure of information categorized as "Limited Access" or "Restricted" and not authorized in accordance with this Policy must immediately inform the ODT IT Security Manager of such disclosure. ODT is required by law to report to affected outside persons and entities disclosures of PII or FTI. There may also be additional reporting requirements of non-public data classifications and or data categories.

### **3.6 Education and Awareness**

Data Classification topics are addressed in ODT Disclosure Training and ODT Security Awareness training.

### **3.7 Discipline**

Failure to comply with this policy may result in the imposition of discipline in accordance with ODT work rules including, but not limited to, Neglect of Duty, Insubordination, and/or Ohio Revised Code Section 124.34.