OhioDAS Department of Administrative Services | Office of Information Technology

DATA Classification

State of Ohio Administrative Policy IT-13

OhioDAS Office of Information Technology | Office of Information Security and Privacy
Service · Support · Solutions

Agenda

- Background
- Classification Elements
- Roles & Responsibilities
- Methodology
- Education & Awareness
- Compliance & Implementation

Purpose

- The 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

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.

Source: State of Ohio Administrative Policy IT-13

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).

Source: State of Ohio Administrative Policy IT-13

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.

Confidentiality Low (Public)

Confidentiality Moderate

Confidentiality High

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.

Criticality Low

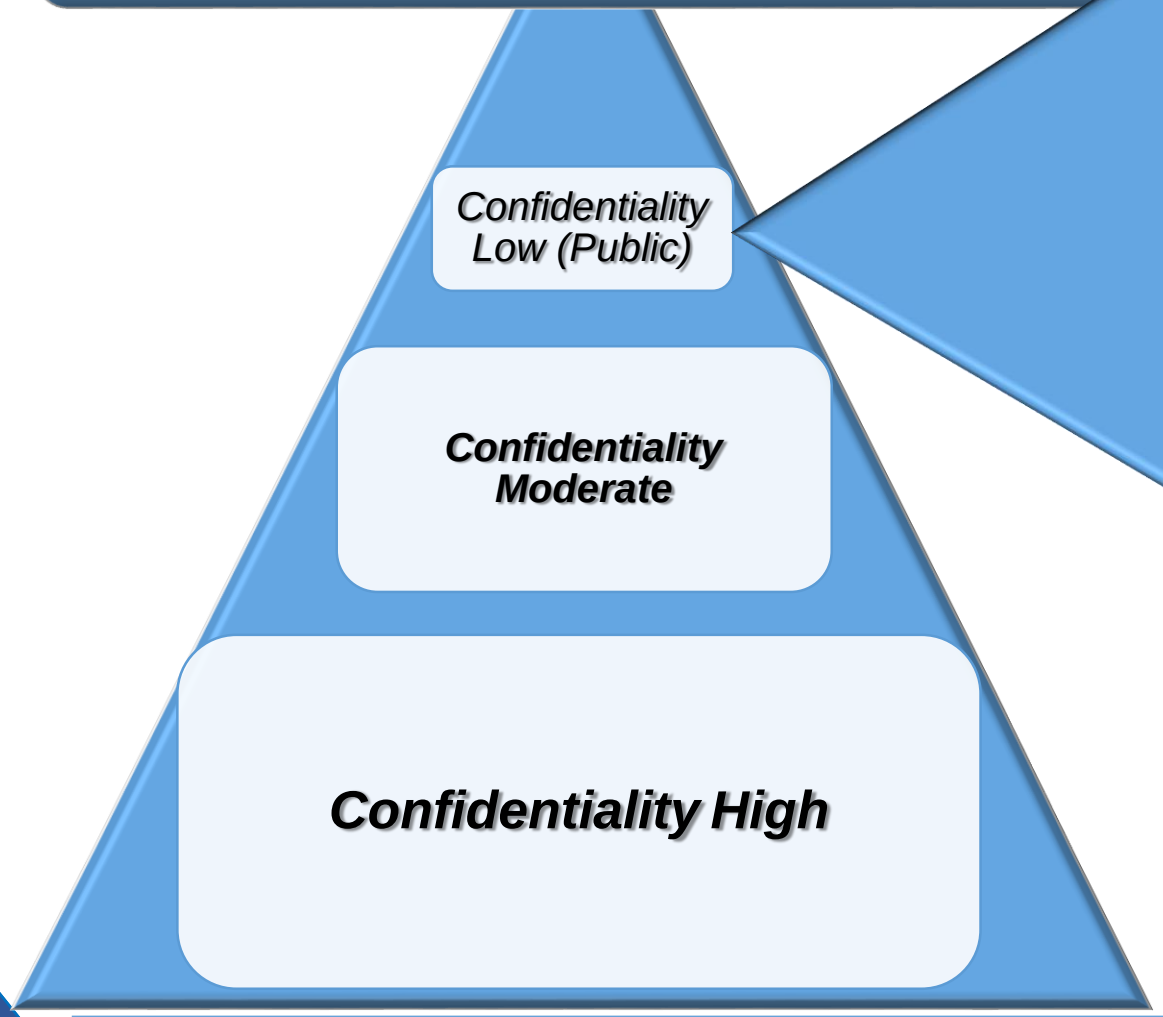
Criticality Moderate

Criticality High

Source: State of Ohio Administrative Policy IT-13

Confidentiality Data Classification Labels

Further Defined



Limited adverse effect might cause:

A degradation in mission capability, but the effectiveness of the functions is noticeably reduced.

May cause a result in minor damage to organizational assets, as well as result in minor financial loss, or harm to individuals including privacy.

Example: A financial organization managing routine *administrative information* (not privacy-related information) determines that the potential impact from a loss of confidentiality is low if there was unauthorized disclosure. Why?

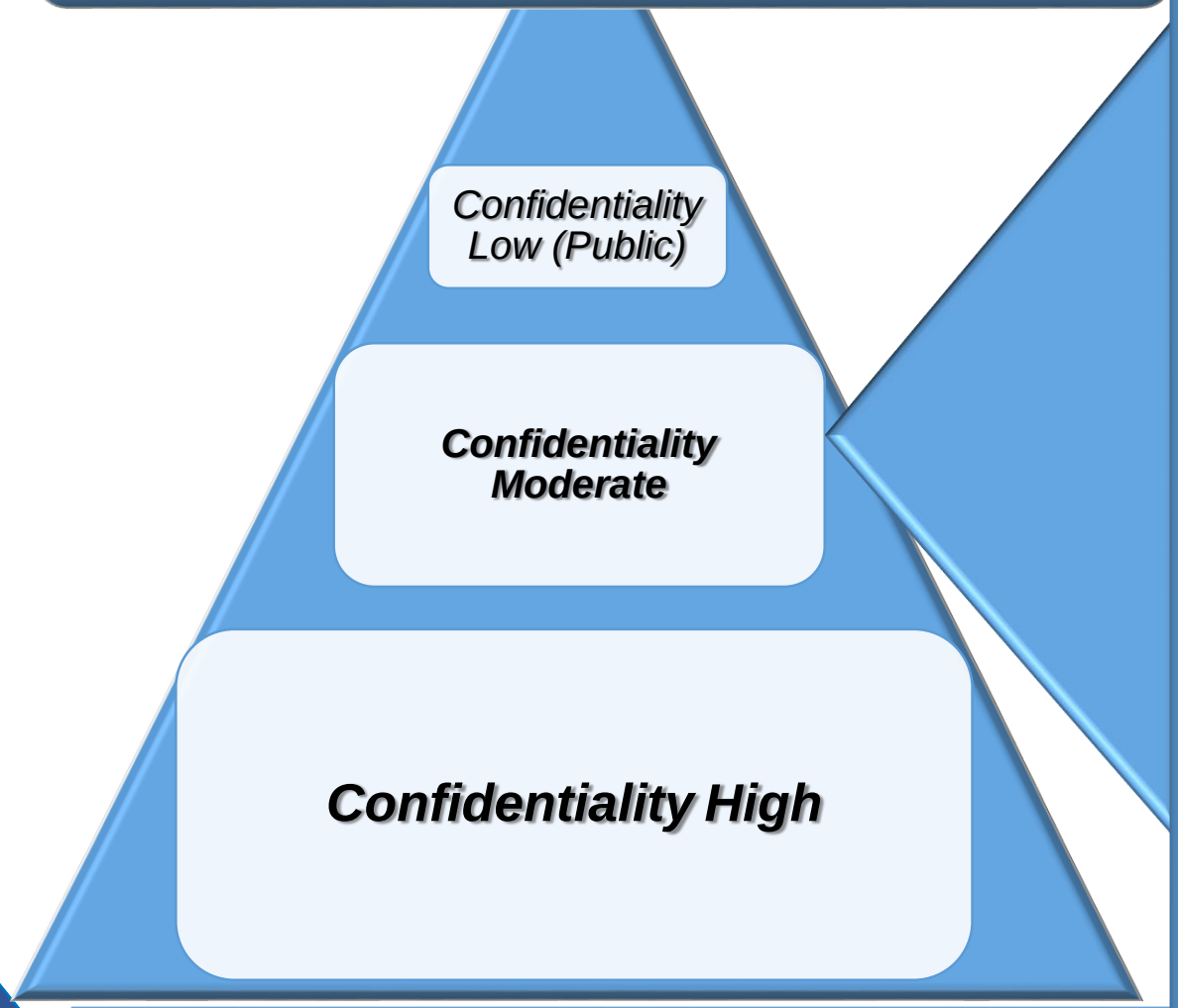
Includes information that must be released under Ohio public records law or instances where an agency unconditionally waives an exception to the public records law.

The inappropriate use or unauthorized disclosure of would have a **limited adverse effect** on State of Ohio interests, the conduct of agency programs, or individuals.

Source: State of Ohio Administrative Policy IT-13 and FIPS-199

Confidentiality Data Classification Labels

Further Defined



Serious adverse effect might 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.**
- **May result in significant damage to organizational assets, as well as result in significant financial loss or result in significant harm to individuals, that does not involve loss of life or serious life threatening injuries**.

Example: An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. The management within the contracting organization determines that the potential impact from a loss of confidentiality is moderate. Why?

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.

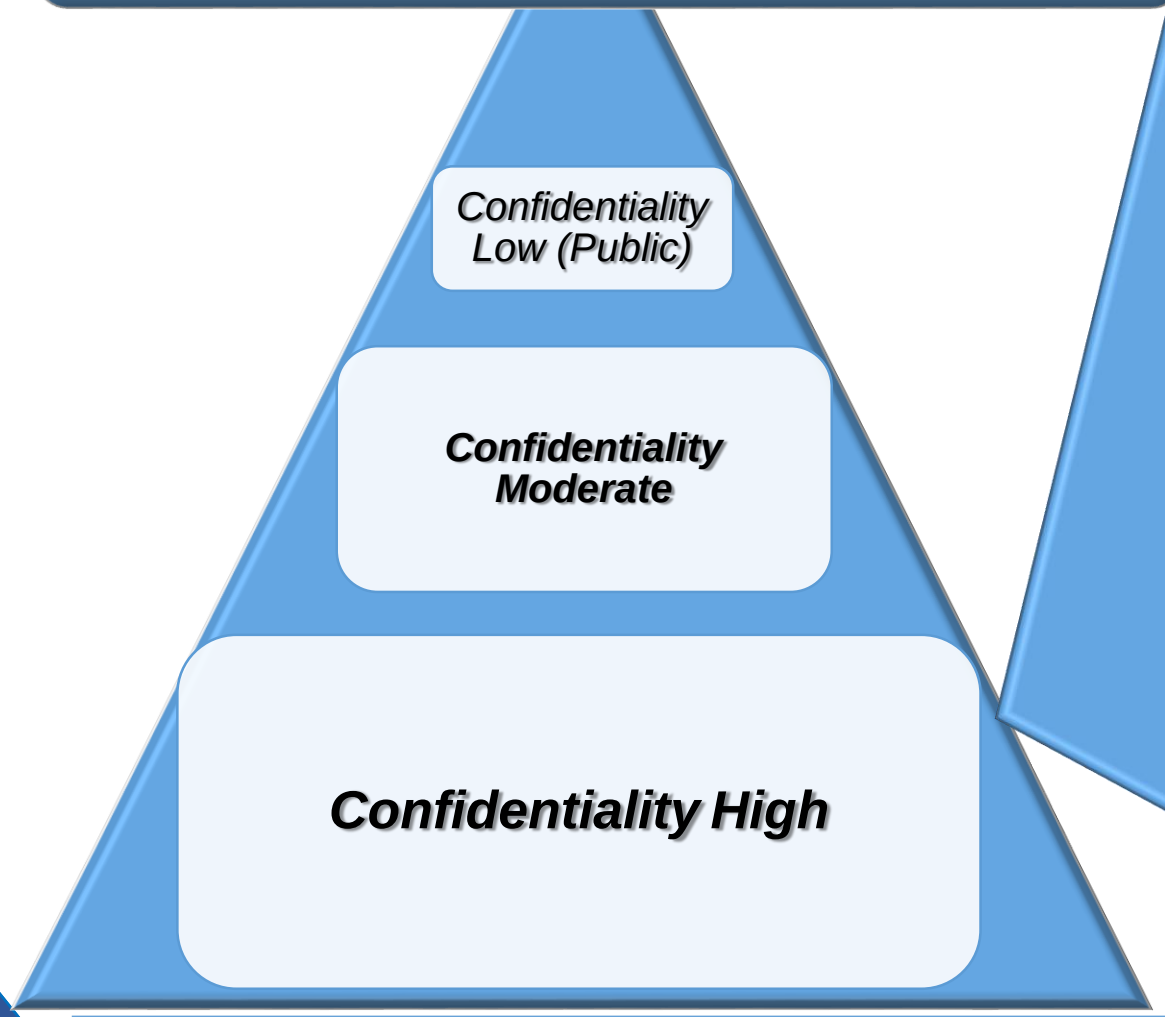
Disclosure to parties outside the state agency shall be authorized by executive management or the Data Owners and General Counsel or in accordance with a formal agency process. Disclosure internally to the state agency shall be on a need-to-know basis only.

Inappropriate use or unauthorized disclosure would have a **serious adverse effect** on State of Ohio interests, the conduct of agency programs, or individuals.

Source: State of Ohio Administrative Policy IT-13 and FIPS-199

Confidentiality Data Classification Labels

Further Defined



Severe or catastrophic adverse effect might 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.**
- **May result in major damage to organizational assets and result in major financial loss.**
- **Additionally could result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.**

Example: A law enforcement organization managing extremely sensitive *investigative information* determines that the potential impact from a loss of confidentiality is high. Why?

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 restrictions in State of Ohio regulations, policies, or contracts must be consistent with Ohio's public records law

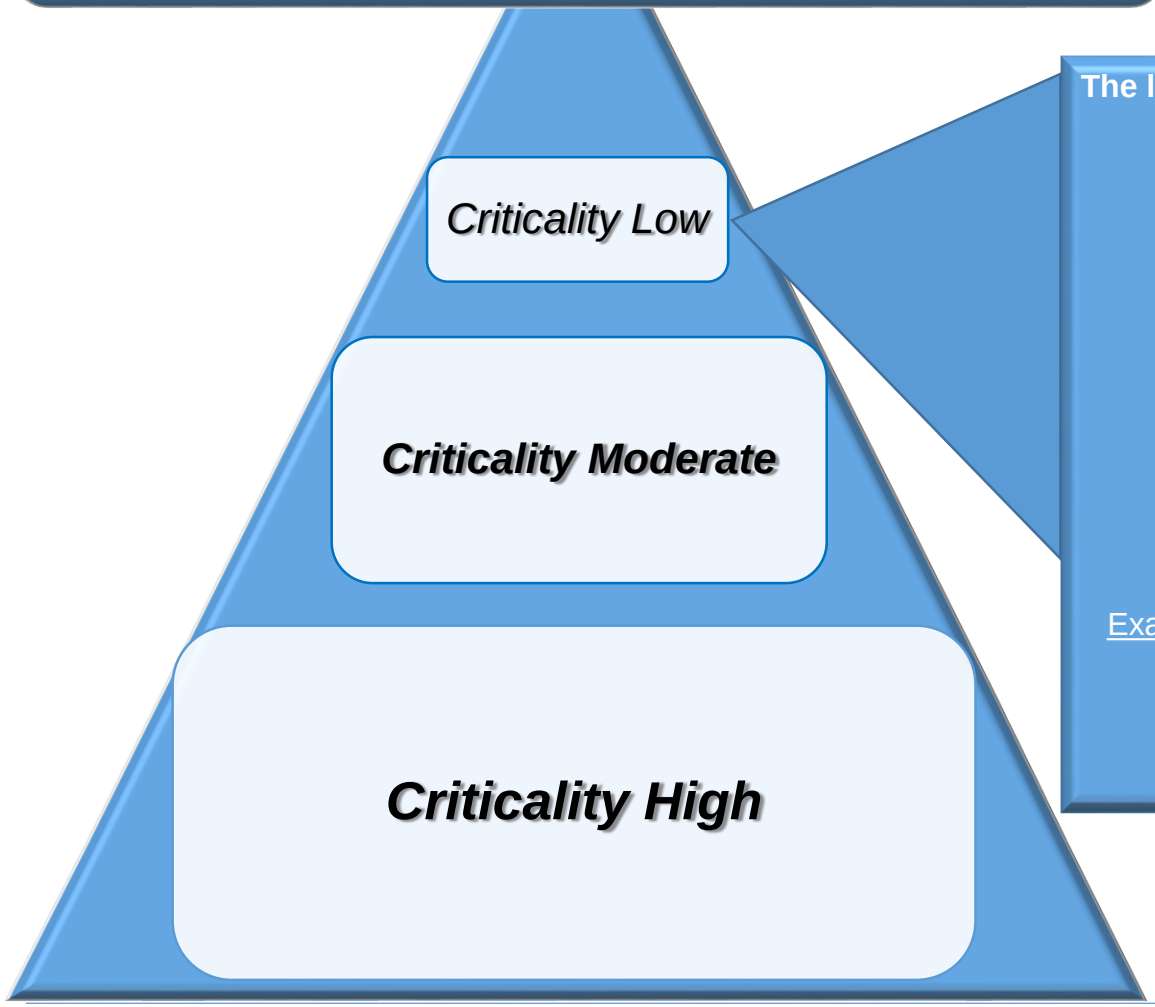
Disclosure to parties outside the state agency shall be authorized by executive management and/or the Data Owners and General Counsel. Disclosure of confidentiality high information internal to the state agency shall be on a need-to-know basis only.

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.

Source: State of Ohio Administrative Policy IT-13 and FIPS-199

Criticality Data Classification Labels

Further Defined



The loss of data integrity or availability would result in limited adverse effect.

Limited adverse effect might cause:

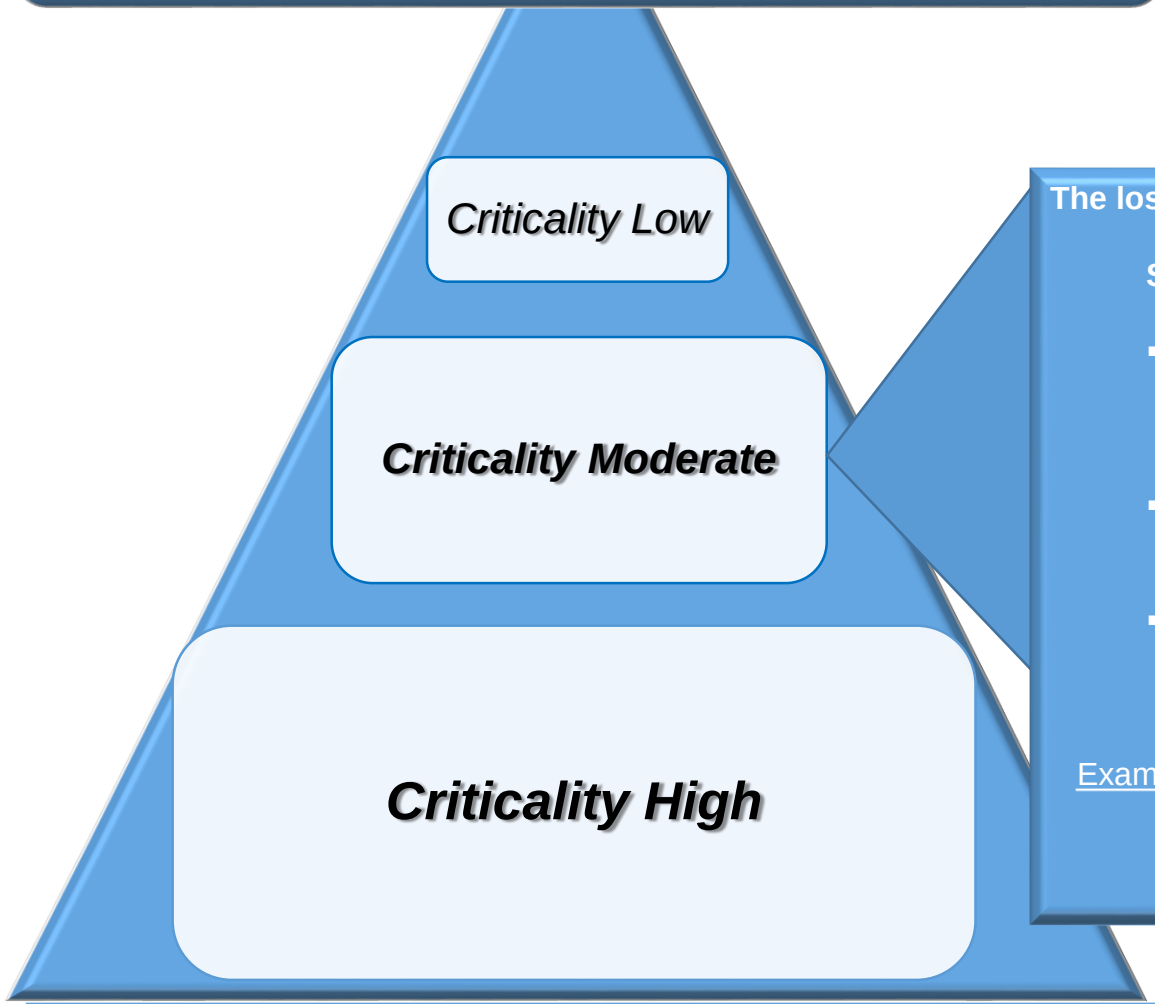
- **A degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced.**
- **May result in minor damage to organizational assets and/or result in minor financial loss.**
- **Additionally may result in minor harm to individuals, including privacy.**

Example: A financial organization managing routine administrative information (not privacy-related information) determines that the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. Why?

Source: State of Ohio Administrative Policy IT-13 and FIPS-199

Criticality Data Classification Labels

Further Defined



The loss of data integrity or availability would result in a serious adverse effect.

Serious adverse effect might cause:

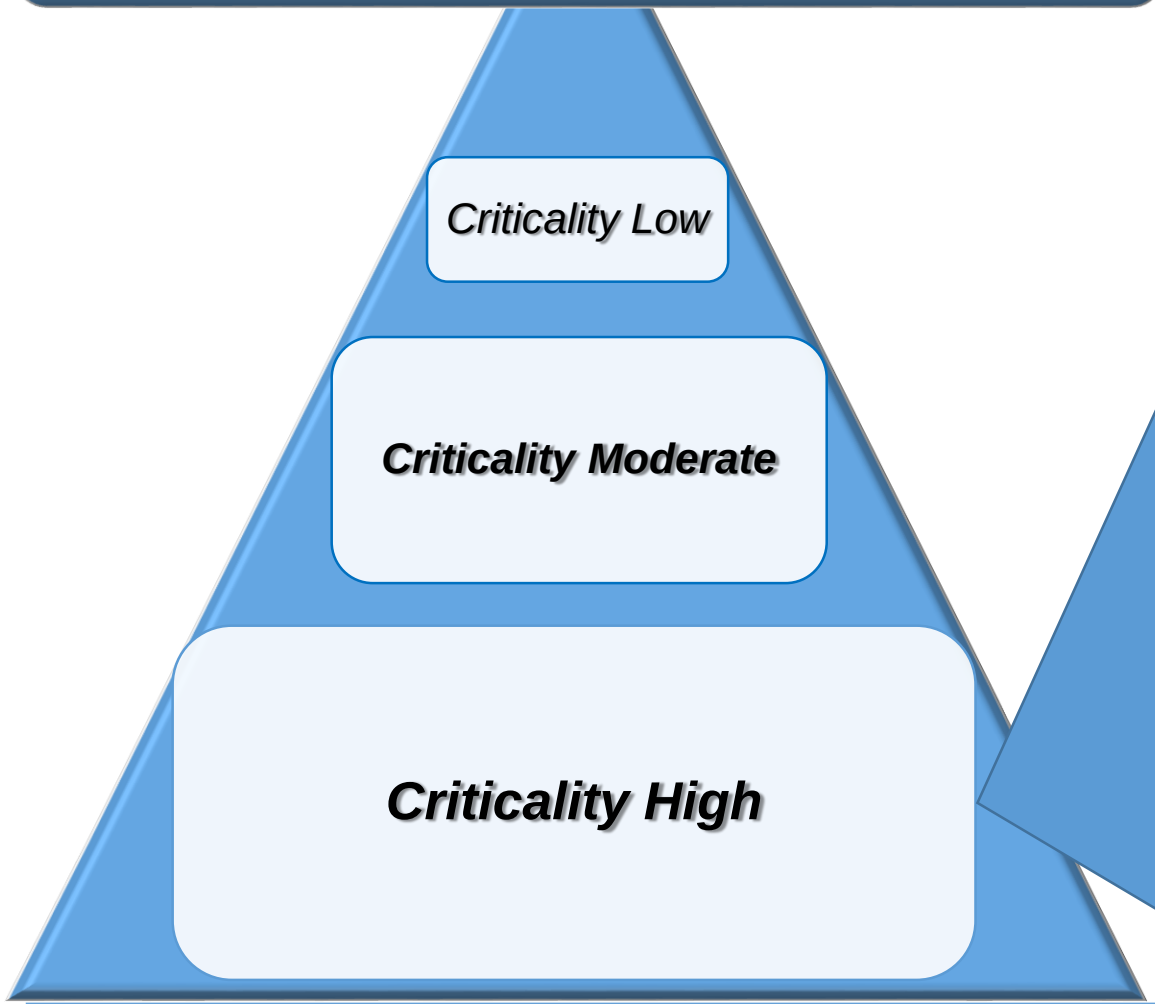
- **A significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.**
- **May result in significant damage to organizational assets and/or result in significant financial loss.**
- **Additionally may result in significant harm to individuals, that does not involve loss of life or serious life threatening injuries.**

Example: An Organization managing public information on its web server determines there is a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. Why?

Source: State of Ohio Administrative Policy IT-13 and FIPS-199

Criticality Data Classification Labels

Further Defined



The loss of data integrity or availability would result in severe or catastrophic adverse effect.

Severe or catastrophic adverse effect might 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.**
- **May result in major damage to organizational assets and/or result in major financial loss.**
- **Additionally may result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.**

Example: A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The management at the power plant determines there is a high potential impact from a loss of integrity, and a high potential impact from a loss of availability. Why?

Source: State of Ohio Administrative Policy IT-13 and FIPS-199

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:

Define

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

Determine

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.

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).

Analyze Results

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

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

Establish Review Process

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.

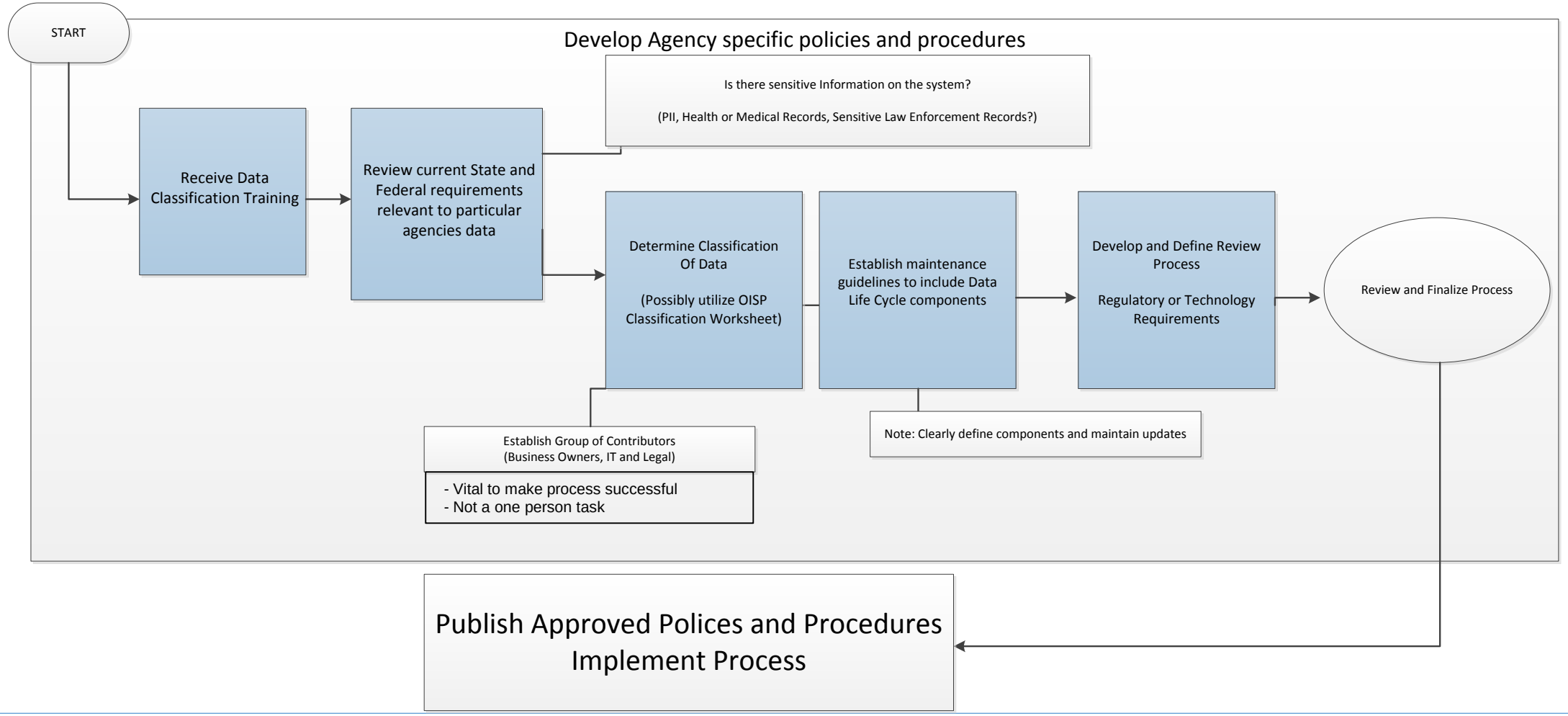
Technologies for which data classification policies do not yet exist. Technologies may include but are not limited to:

- Cloud (Private, public and hybrid), Mobility, Personal Devices and Social Networks

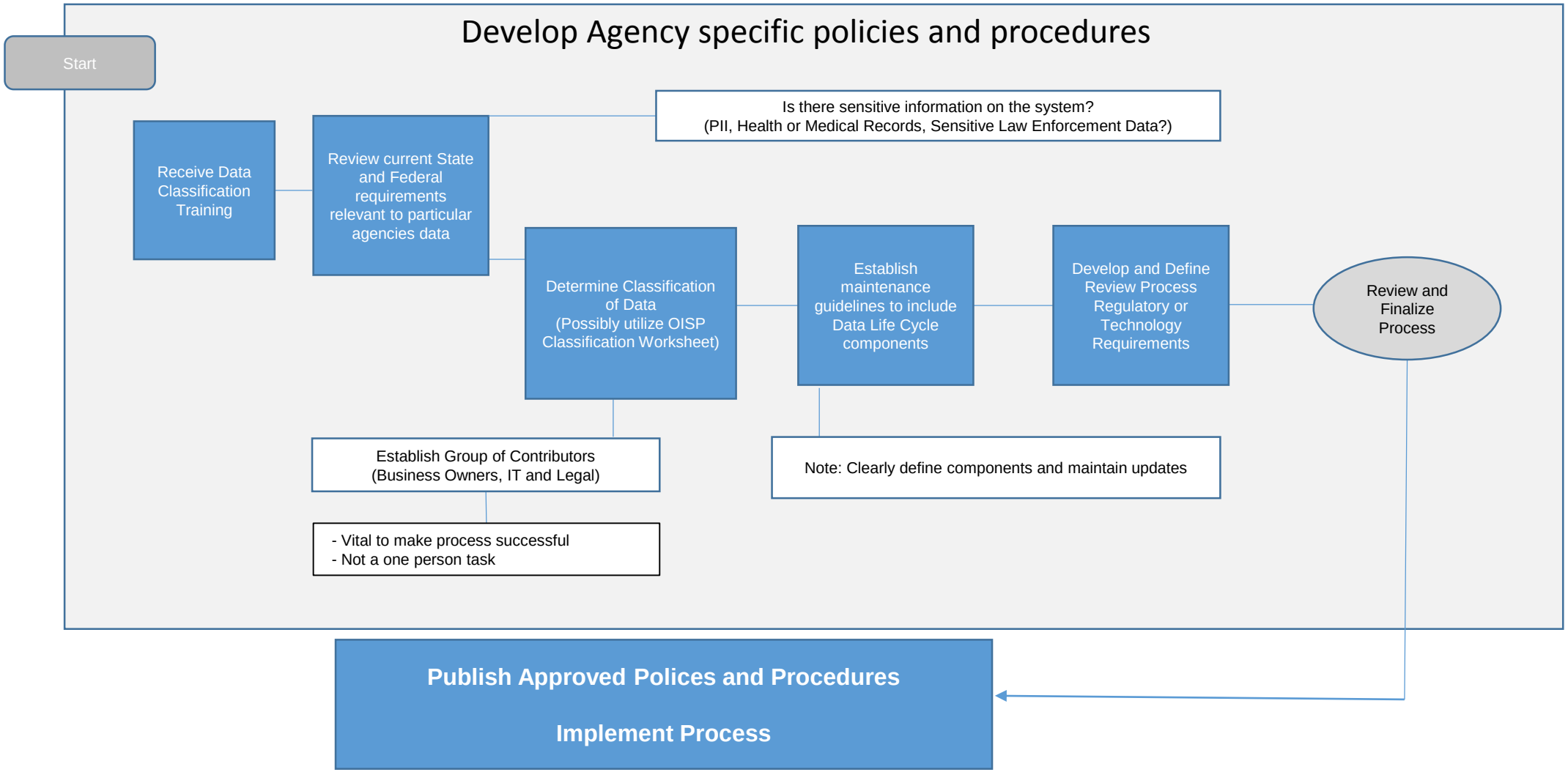
Ensures that the appropriate classifications selected and implemented to protect data from unauthorized access or misuse.

Source: State of Ohio Administrative Policy IT-13

Methodology Implementation Example



Methodology Implementation Example



Roles and Responsibilities

Agencies shall designate individuals who will be responsible for carrying out the duties associated with each of the required roles.

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:
  - Assignment of Data Classification Labels
  - Compilation
  - Coordination
  - Compliance
  - Access

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:
  - Access Control
  - Audit Reports
  - Backups
  - Validation
  - Restoration
  - Ensure Compliance
  - Monitor Activity
  - Secure Storage
  - Web/server hosting

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.
- Data Use Expectations:
  - Types of data my carry limitations
- Example: Section 1347.15 of ORC requires agencies to develop rules, polices, and training that establishes valid reasons for accessing confidential information.
- Data users must be in compliance with all policies applicable to data use.

Source: State of Ohio Administrative Policy IT-13

Education & 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 the IT-13 Data Classification policy.

Agencies shall address the following topics as part of their training efforts:

Source: State of Ohio Administrative Policy IT-13

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.

Implementation

Agencies are expected to begin planning and working towards compliance with this IT-13 Data Classification policy. A general implementation framework for the requirements of this policy includes:

- Six month from effective date of IT-13 to implement Classification requirements
- Ensure that data classification is determined during design phase when planning a new IT system.
- Agencies that do not have IT personnel shall contact DAS OSIP to determine path for compliance.

Source: State of Ohio Administrative Policy IT-13

Questions?

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.

Source: State of Ohio Administrative Policy IT-13 and FIPS-199