ENT-102: Enterprise Data Classification Process

		Document Revision History	
Version	**Date**	**Change Description / Notes**	**Author / Editor**
1.0	8/29/2019	Enterprise Data Classification Process	Tom Walters
2.0	1/27/2022	Enterprise Data Classification Process	CC Webber
3.0	3/13/2025	Removed Data Stewart role, duties re-allocated to the Cabinet; minor grammar formatting changes	Karen Chrisman / Tracy Burgess

Purpose

The purpose of this process is to define how data is identified, classified, labeled, and properly handled and protected in accordance with its importance and potential impact to the Commonwealth. Data must be properly handled throughout its entire lifecycle, from creation to disposal. The importance of such information varies and requires different levels of protection.

Scope

This process applies to all executive branch Commonwealth employees, contactors, and any other users authorized to access data stores, information in any medium, and/or information systems. In addition, third parties may be subject to this process through contractual obligations to the Commonwealth.

Each agency shall perform due diligence to ensure proper data classification in accordance with applicable legal, regulatory, and compliance obligations.

Definitions and Roles

Data User: Individuals who access data at any point during its lifecycle. Anyone within the agency could be a data user of appropriately accessed data.

Data Creator: Individuals, either Commonwealth employees or contractors, who create new data and are responsible for classifying it as it is created. The creator should assess the content of the data to efficiently select the classification.

Data Processor: Individuals responsible for implementing data policies, processes and procedures, including physical data storage, backup and recovery, and the operation of security and data management systems.

Data Controller: Individuals who have direct responsibility for the data that is primarily used within their department, division, office or cabinet. The Controller is accountable for classifying the data and reviewing the classification. Individuals are responsible for data governance, practices and requirements including responsibility for the agency data classification program.

Data Lifecycle: The lifecycle includes these actions: creation, storage, use, transmission, archival and destruction.

Definitions and Roles (continued)

Data Classification Levels:

- **CONFIDENTIAL**: Applies to data that must be kept private under federal, state, and local laws, or contractual agreements, or to protect its proprietary value, or must be kept private for any combination of these reasons.
- **INTERNAL**: Applies to data that is intended for use within the Commonwealth. Unauthorized external disclosure could adversely affect the Commonwealth, its citizens, employees, and business partners. This classification also applies to open records as defined by the Kentucky Open Records Act, KRS 61.870(2). It applies to data that is not openly published, but that can be made available via open record requests. Direct access to this data is restricted to authenticated and authorized users.
- **OPEN**: Applies to data that is readily available to the public with anonymous access.

Process

1. Data Controllers (at the cabinet, office, division or department level) shall identify a Data Processor. The Data Processor will work with the Agency Data Controllers to classify agency data according to the data classification levels.
2. Each Cabinet shall identify and classify their information systems and data stores and manage access to those systems and stores in compliance with the ENT-101 Enterprise Data Classification Standard.
3. Agencies will ensure that all data is appropriately identified, including restrictions on redistributions when transmitted via email or physical mail, in accordance with the ENT-101 Enterprise Data Classification Standard.
4. Agency Data Controllers (with assistance from Data Processor as needed) will establish a Cabinet-wide data-handling training curriculum.
5. Agency Data Controllers will work with information technology to ensure appropriate asset protection measures are in place relative to the data's classification.
6. Commonwealth employees, contractors, volunteers, and any other users authorized to access data stores, information in any medium, and/or information systems, will comply with the information asset handling standards established in the ENT-101 Enterprise Data Classification Standard.

Process Compliance

Any exception to this process must be approved by the COT Chief Information Security Officer (CISO) in writing. Any Executive Branch Commonwealth employee, contractor, or authorized user discovered to have violated this process may be subject to disciplinary action, up to and including termination of employment. Unauthorized disclosure of regulated data, such as personally identifiable information, may lead to legal repercussions.

Information received by the Commonwealth Marked as Confidential or Proprietary Information

Any information received by the Commonwealth marked as Confidential or Proprietary Information by the disclosing party shall be treated according to the designation. If the Commonwealth disagrees with this classification, advice from legal counsel is required.

References

Helpful references can be found on the Enterprise IT Policies webpage.

"END"