Office of the Chief Information Officer Enterprise Standards

ENT-101: Enterprise Data Classification Standard

Effective Date: 8/29/2019

Overview

Working with the Agency Data Steward, each Cabinet will identify its data for the purpose of defining its value, location, and level of protection. This standard defines the classification scheme and outlines the expected data handling requirements throughout the lifecycle of data. This document also provides recommended sample disclaimers to be used when storing and transferring data of various classifications.

KRS 61.870(7) defines a "Public record" as all books, papers, maps, photographs, cards, tapes, discs, diskettes, recordings, software, or other documentation regardless of physical form or characteristics, which are prepared, owned, used, in the possession of or retained by a public agency. **This is the data classification scheme for these public records.**

This standard is the minimum Commonwealth Office of Technology (COT) requirement for data classification. If an agency has a business need for or a statutory or regulatory requirement with a stricter standard, the stricter standard is required. This standard is applicable when a stricter standard does not apply.

Standard Data Classification Levels

Classification Level	Definition	Some Examples Not a complete list of each category
Confidential	Applies to data that must be kept private under federal, local, or state laws, or contractual agreements, or to protect its proprietary value, or must be kept private for any combination of these reasons.	• Criminal history data (especially pre-conviction) • Trade secrets • Government classified information • Authentication Verifier (password, cryptographic private keys) • Protected Health Information • Personal Information as defined by KRS 61.931(6) • Business Strategy • Payment card information • Social security numbers • Federal Tax Information • Personally Identifiable Education records • Personal Data as defined by the General Data Protection Regulation (GDPR) and that is subject to the GDPR

		• Data protected by federal code or regulation or state statute or regulation • System Documentation
Internal	Applies to data that is intended for use within the Commonwealth. Unauthorized external disclosure could adversely impact 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). 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.	• Employment application records and employee records • Licensed software • Communication between Commonwealth citizens and Commonwealth staff • Memos • Training manuals
Open	Applies to data that is readily available to the public with anonymous access.	• Press releases • Open access website pages • Brochures • Published information (including data files) • Public presentations

Electronic Data Handling Requirements Matrix

Creation

	Open	Internal	Confidential
Creation of data	Ensure proper labeling immediately upon creation. Creation of Open data must be approved by the appropriate data owner(s).	**All Open requirements** and the following requirements: Creation/discussion of new data in public or on a public network is prohibited. Ensure use of secure connection (e.g. https, VPN, SFTP) Creation of Internal data must be approved by the appropriate data owner(s).	**All Open and Internal requirements** and the following requirement: Ensure all creation/ discussion is done in private with authorized personnel only.

Storage

	Open	Internal	Confidential
Storing of data on static assets **Non-removable media** **(Examples: servers, workstations, endpoint devices)**	Follow Commonwealth drive storage conventions.	**All Open requirements** and the following requirements: Must be stored within a protected boundary that is continuously monitored. Physical boundary protections must be in place to prevent unauthorized physical access. Appropriate access control mechanisms must be employed to prevent unauthorized logical access and enforce least privileged access. Data must be protected in transit through encryption or isolation. Data encryption is not required but recommended. All encryption keys must be managed including creation, issuance, renewal, and disposal. For mobile computing devices, full drive encryption is required. (Example: a workstation that is mobile such as a laptop or a tablet)	**All Open and Internal requirements** and the following requirements: Access to confidential data must be logged and logs retained for a minimum of 90 days or as required by regulatory guidance. Data must be encrypted at rest and in transit.
Storage of data on any removable media	Follow Commonwealth drive storage conventions and ensure secure storage of the physical device.	**All Open requirements** and the following requirements:	**All Open and Internal requirements** and the following requirement: Chain of custody documenting the

(CD, DVD USB drive, storage external to a computing device)	Label removable media with appropriate classification level.	The removable media device shall be encrypted. The removable media shall be securely stored and transported. Data must be sanitized in compliance with enterprise policy.	lifecycle of the media from creation through sanitization must be documented.

Usage

	Open	Internal	Confidential
Accessing of data	Anonymous access allowed	Standard user authentication practices in place for remote access to systems hosting the data (username and password). Remote access by VPN that is managed by a central directory. Data is password protected.	**All Internal requirements** and the following requirement: Two-factor authentication for remote access, and auditable data system administration.
Auditing of data	Change history of Open data is publically available.	Auditing data is restricted to designated internal users. All unusual behavior (alterations and/or deletions) is brought to the attention of the data owner.	**All Internal requirements** and the following requirements: Ensure system logging, audit of user credentials and use, audit of errors, failed attempts, permissions, and changes. File integrity monitoring is performed.
Printing of data	Printed data follows the requirements of the Non-Digital Data Handling Requirements Matrix.	**All Open requirements.**	**All Open and Internal requirements.**
Posting data on social media	Permitted	Not permitted	Not permitted.

Transmission

	Open	Internal	Confidential
Emailing of data internally	All email defaults to an Internal category and displays language such as the Sample Email Disclaimer and Restrictions.	**All Open requirements** and the following requirements: Data must not be emailed outside of the organization unless approved to do so. All email defaults to Internal requirements.	**All Open and Internal requirements** and the following requirements: Data must be email encrypted or password protected. If using password encryption, the password must be sent in a separate communication.
Granting permission to view, write, or edit data externally (i.e. third parties)	None	Must follow formal data sharing agreements and/or formal contractual agreements.	**All Internal requirements**.

Archiving

	Open	Internal	Confidential
Archiving of data	All archiving shall follow KDLA State Government Records Retention Schedules and follow the requirements of the Electronic Data Handling Requirements Matrix.	**All Open requirements.**	**All Open and Internal requirements.**

Destruction

	Open	Internal	Confidential
Destruction (or sanitization) of data and data bearing devices.	Destruction or sanitization only in accordance with KDLA State Government Records Retention Schedules and must comply with CIO-092 Media Protection Policy.	**All Open requirements.**	**All Open and Internal requirements.**

Destruction of data on third-party hosted services	Must follow formal data sharing agreements and/or formal contractual agreements.	**All Open requirements.**	**All Open and Internal requirements.**

Non-Digital Data Handling Requirements Matrix

Creation

	Open	Internal	Confidential
Creation	Ensure proper labeling immediately upon creation.	**All Open requirements.**	**All Open and Internal requirements** and the following requirement: All creation or discussion of data must be completed in private with authorized personnel only.

Storage

	Open	Internal	Confidential
Storage	Follow KDLA State Government Records Retention Schedules.	**All Open requirements** and the following requirements: Data must be kept out of sight after business hours or when visitors are present. Access to the facility requires centralized electronic badge access based upon least privilege. Access is reviewed regularly.	**All Open and Internal requirements** and the following requirement: Data must be stored in a secure environment or locked compartment, such as a filing cabinet or desk drawer when not attended by an authorized user.

Usage

	Open	Internal	Confidential
Usage	None	Data should only be printed when there is a legitimate business need. Data should only be printed/copied internally or to satisfy	**All Internal requirements** and the following requirements: Copies must only be shared with individuals with authorized

		an Open Records Request. Copies must only be shared with individuals on a need-to-know basis.	clearance. Data can only be printed if allowed by statute or regulation. All data must be marked as appropriate (e.g. "Confidential"). All usage must be performed in private.

Transmission

	Open	Internal	Confidential
Transmission	None	Include a statement identifying the classification level and list restrictions for redistribution.	**All Internal requirements** and the following requirement: Transmission must be logged. Agencies should comply with any additional agency requirements for transmission of confidential information.

Archiving

	Open	Internal	Confidential
Archiving	Follow KDLA State Government Records Retention Schedules.	**All Open requirements** and the following requirement: Ensure physical security of the offsite facility with centralized management of access based upon least privilege.	**All Open and Internal requirements.**

Destruction

	Open	Internal	Confidential
Destruction	None	Follow KDLA State Government Records Retention Schedules and CIO-092 Media Protection Policy.	**All Internal requirements.**

Sample Disclaimers and Statements

Sample Email Disclaimer and Restrictions

The following table provides sample disclaimers and statements to include in transmission of email containing information that has been classified as Internal or Confidential in accordance with the Commonwealth's CIO-110 Enterprise Data Management Policy, ENT-101 Enterprise Data Classification Standard (this document), and ENT-102 Data Classification Process.

For Confidential data, the classification must be labeled in the subject line in all capital letters (CONFIDENTIAL), and the attached document(s) must be labeled with the classification. This label alerts the recipient to the level of care and restriction required.

Classification	Sample Email Disclaimer and Restrictions
Internal or Confidential	This email and any attachments contain information that has been classified as **"**[**Internal** (or) **Confidential**]." It is intended exclusively for the use of the individual(s) to whom it is addressed. This information may be protected by federal and state laws or regulations. If you are not the intended recipient, you may not use, copy, distribute, or forward this message or contents to anyone. If you have received this email in error, please notify the sender immediately and delete the email from your email system.

Sample Non-Digital Data Disclaimer and Restrictions

The following table provides sample disclaimers and statements to include along with any mailing that has been classified in accordance with the Commonwealth's CIO-110 Enterprise Data Management Policy, ENT-101 Enterprise Data Classification Standard (this document), and ENT-102 Data Classification Process.

For Confidential data, the classification must be labeled in all capital letters (CONFIDENTIAL) and the attached document(s) or devices must be labeled with the classification of the data they contain. This label alerts the recipient to the level of care and restriction required.

Classification	Sample Non-Digital Data Disclaimer and Restrictions
Confidential	This document and any attachments contain information that has been classified as **"[Confidential]."** It is intended solely for the use of the individual(s) to whom it is addressed. It contains information that may be protected by federal and state laws or regulations. If you are not the intended recipient, you may not use, copy, distribute, or forward this document, its content, or its attachments to anyone. If you have received this document in error, please notify the sender immediately.

References

- CIO-092 Media Protection Policy
- CIO-110 Enterprise Data Management Policy
- ENT-102 Enterprise Data Classification Process

- General Data Protection Regulation (GDPR)
- KDLA State Government Records Retention Schedules
- Kentucky Department for Libraries and Archives (KDLA)
- Kentucky Revised Statutes (KRS)
- KRS 61.870 to KRS 61.884, *Kentucky Open Records Act (KORA)*
- KRS 61.870(2), “Public record” defined
- KRS 61.931 to 61.934, *Personal Information Security and Breach Investigations*
- Personal Data as defined by the GDPR