Data Classification Standard

City of Lynnwood - Information Technology

Originator:	Will Cena	**Included:**	**[X] Standard** **[ ] Procedure** **[ ] Guideline**
Approved by:	Will Cena		
Approval Date:	January 29, 2026		

OVERVIEW:

A data classification standard is necessary to provide a framework for securing data from risks, including unauthorized destruction, modification, disclosure, access, use, and removal.

PURPOSE:

This standard outlines how the City of Lynnwood classifies its data.

Scope:

This policy applies to all City of Lynnwood data and all user-developed datasets and systems that may access these data, regardless of the environment where the data resides (including cloud systems, servers, personal computers, mobile devices, etc.). The policy applies regardless of the media on which data reside (including electronic, microfiche, printouts, CD, etc.) or the form they may take (text, graphics, video, voice, etc.).

Standard:

Classification Category	Definition	Examples
Category 4: Confidential Information Requiring Special Handling	Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:	• Credit card information • Criminal Justice Information (CJI)

Category 2: For official use only & disclosure permissible by law.

	• Statutes, regulations, or agreements dictate strict handling requirements. • Serious consequences could arise from unauthorized disclosure, such as threats to health and safety or legal sanctions.	
Category 3: Confidential	Confidential information is information that is specifically protected from disclosure by law.	• Employee personnel records • Personal identifiable information (PII) • IT Infrastructure and security information
Category 2: Sensitive Information	Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.	• Internal procedures, workflows, and training materials • Internal emails that do not contain confidential or personal information • Budget planning documents not yet approved for public release
Category 1: Public	Public information is currently available to the public. It does not require protection from unauthorized disclosure but does need controls for integrity and availability.	• Press releases • Public access website pages • Information released by public record request

DATA HANDLING REQUIREMENTS MATRIX:

Storage:

	CATEGORY 1 PUBLIC	CATEGORY 2 SENSITIVE	CATEGORY 3 CONFIDENTIAL	CATEGORY 4 CONFIDENTIAL WITH SPECIAL HANDLING
Storing data on local drives	Not recommended as local drives are not backed up.	Not recommended as local drives are not backed up.	Not Permitted	Not Permitted
Storing data on corporate mobile	Follow City storage conventions.	Cat 1, and must be managed through MDM solution.	Not Permitted	Not Permitted

devices (e.g. smartphones)		Mobile device must be password protected. Not recommended as local drives are not backed up.		
Storing data on personally owned mobile devices	Follow City storage conventions.	Not Permitted	Not Permitted	Not Permitted
Storage of data on any sanctioned third-party hosted application (such as SharePoint Online)	Follow City storage conventions.	Cat 1, and third party must meet security requirements set up by the IT team before being used. Basic levels of authentication and access are required.	Cat 2, and encrypted when stored on systems managed by a vendor performing services for the organization. Access must be federated.	Not permitted.
Storage of data on any unsanctioned third-party hosted application (such as SurveyMonkey, Google, Dropbox)	Follow City storage conventions.	Not Permitted	Not Permitted	Not Permitted
Storage of data on any removable media	Follow City storage conventions.	Cat 1, and data owner approval required for storage on removable media. Only company-issued devices may be used.	Cat 2, and removable media must be encrypted OR cannot be removed from the premises	Same as Cat 3.

Usage:

	CATEGORY 1 PUBLIC	**CATEGORY 2 SENSITIVE**	**CATEGORY 3 CONFIDENTIAL**	**CATEGORY 4 CONFIDENTIAL WITH SPECIAL HANDLING**

Posting of data on public website	Permitted only by approved by posters.	Cat 1 and permitted only after formal reclassification from "sensitive" to "public" classification.	Not Permitted	Not Permitted
Posting of data on social media	Follow standard practices aligning with the Social Media Acceptable Use Policy.	Cat 1 and permitted only after formal reclassification from "sensitive" to "public" classification.	Not Permitted	Not Permitted
Printing and other use of physical data	Follow standard printing practices.	Cat 1 and data should only be printed/copied internally or to satisfy an open records request.	Cat 1 and employees should be in close proximity to the printer to ensure the printed document is immediately taken by the appropriate employee or use secure printing. Copies must only be shared with individuals with authorized clearance. Copies must be marked as appropriate (e.g. “Confidential”). All usage must be performed in private.	Same as Category 3.

Transmission:

	CATEGORY 1 PUBLIC	**CATEGORY 2 SENSITIVE**	**CATEGORY 3 CONFIDENTIAL**	**CATEGORY 4 CONFIDENTIAL WITH SPECIAL HANDLING**
EMAILING OF DATA INTERNALLY	Follow standard practices aligning with the Email Acceptable Use Policy.	Category 1, and attention must be paid to verify recipient information to avoid unintentional information disclosure.	Category 2, and the email shall include a statement identifying the classification Category and list restrictions for redistribution.	Not Permitted
EMAILING DATA	Follow standard practices aligning	Category 1, and the email shall	Category 2, and data must be	Not Permitted

EXTERNALLY TO SANCTIONED THIRD PARTIES (SUCH AS CUSTOMERS AND PARTNERS)	with the Email Acceptable Use Policy.	include a statement identifying the classification Category and list restrictions for redistribution. If transmitting in response to open records request, ensure proper redactions are applied. Attention must be paid to verify recipient information to avoid unintentional information disclosure.	password-protected and encrypted, without the password sent through email. Transmission by non-encrypted email is prohibited. Sending of data must be approved by the appropriate data owner(s).	
EMAILING DATA EXTERNALLY TO UNSANCTIONED THIRD PARTIES (SUCH AS AUTO-FORWARDING TO PERSONAL EMAIL, FRIENDS)	Follow standard practices aligning with the Email Acceptable Use Policy.	Category 1, and not permitted unless formal reclassification and redaction (e.g., Open Requests Request).	Not permitted.	Not permitted.
OTHER FILE SHARING PLATFORMS	Follow standard practices aligning with the relevant Acceptable Use Policy.	Category 1, and file sharing must be through IT-approved platforms, such as City accounts OneDrive and SharePoint There must be a legitimate business need for file sharing at this Category. Non-sanctioned platforms are not permitted for file sharing.	Category 2, and documents must be password-protected on the approved sharing platform.	Not Permitted
GRANTING PERMISSION TO VIEW,	No requirement.	Employees can decide whether other employees	Category 2, and read, write, and/or edit access is not	Same as Category 3.

WRITE, OR EDIT DATA INTERNALLY		need access to data. Read, write, and/or edit access will be dictated by role-based access.	permitted, unless approved by the appropriate data owner(s) Read access may be provisioned, while write/edit access is typically not recommended.	
GRANTING PERMISSION TO VIEW, WRITE, OR EDIT DATA EXTERNALLY (I.E. THIRD PARTIES)	No requirement.	Request for information to be shared externally must be through proper channels (Open Records Request). The data owner must approve the third-party handling of this data. Links expire after one year	Read access may be provisioned when approved by the appropriate data owner(s). Write or edit access is not permitted.	Not Permitted

Destruction:

	CATEGORY 1 PUBLIC	**CATEGORY 2 SENSITIVE**	**CATEGORY 3 CONFIDENTIAL**	**CATEGORY 4 CONFIDENTIAL WITH SPECIAL HANDLING**
Destruction of data and files	Follow the standard file deletion process in accordance with the Electronic Messages, Email, and Electronic Records Retention Policy.	Category 1 and verify that backups and alternate copies have been destroyed, if applicable.	Category 2 and maintain a record of disposal.	Same as Category 3.
Destruction of data storage devices (e.g. hard drives, USBs)	Media must be appropriately sanitized to ensure that data cannot be recovered from it.	Same as Category 1.	Hardware must be disintegrated, shredded or incinerated and maintain a record of disposal.	Same as Category 3.
Destruction of data on third-party hosted services	Follow standard data deletions practices.	Category 1 and verify that the third party adheres to internal data destruction requirements.	Category 2 and maintain a record of disposal.	Same as Category 3.

Appendix A: References

Version History and Approvals

Contact Info:	Will Cena Information Technology Department Phone 425-670-5957 E-mail wcena@lynnwoodwa.gov
Standard History:	• 1/29/2026 Initial version
Approval:	Will Cena, Information Technology Director
Effective Date:	1/29/2026