CITY OF SHELBYVILLE **INFORMATION TECHNOLOGY DEPARTMENT**	POLICY NUMBER: ITD 3
SUBJECT: INFORMATION CLASSIFICATION POLICY	DISTRIBUTION DATE: 6/17/2024
	EFFECTIVE DATE: 6/11/2024
ISSUING AUTHORITY: Director of Information Technology	EXPIRATION: UNTIL RESCINDED

PURPOSE

The purpose of this policy is to ensure that the Information of the City of Shelbyville Government (City) receives an appropriate level of protection.[1]

POLICY

1. Generally
   The City of Shelbyville (City) shall classify Information of the City in terms of their value, legal requirements, sensitivity, and criticality to the business and operations of the government and those it serves or as specified by any superseding state or federal law or regulation. Such legal requirements shall include applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance. This policy and accompanying procedures shall be reviewed/updated at least annually.

2. Information Classifications
   The following classifications shall be used by the City to assign potential risk and to provide guidelines for Information of the City of Shelbyville:

[1]In addition to this policy, care should be taken to ensure compliance with other applicable federal, state and local laws and authorities including but not limited to the Tennessee Public Records Act, T.C.A. § 10-7-503.

Public Information (no risk)	Public Information is Information of the City that it must provide for access to Tennessee residents. Public Information is shared publicly to facilitate City operations. *Examples of public Information include Information provided on the Citys' Web site and reports meant for public distribution.*
Internal Information (lowest risk)	Internal Information is non-sensitive Information of the City that is used in daily business operations. If internal Information is inappropriately altered, or is subject to unauthorized access, use or disclosure, little or no loss would be incurred. *Examples of internal Information include staff phone numbers or building address.*
Confidential Information (high risk)	Confidential Information is sensitive Information of the City. If confidential Information is inappropriately altered, or is subject to unauthorized access, use or disclosure, considerable loss could occur. *Examples of confidential Information include social security numbers, banking information, and credit card Information.*
Restricted Information (highest risk)	Restricted Information is highly sensitive Information of the City. If restricted Information is inappropriately altered, or is subject to unauthorized access, use or disclosure, significant loss including loss of life could occur. *Examples of such Information are witness protection Information, Active case files, and Information related to critical infrastructure by the U.S. Department of Homeland Security.*

All Information of the City regardless of physical form or characteristics shall be assigned a classification by the Information Owners in accordance with the requirements set forth within this section in order to ensure that they receive an appropriate level of protection from unauthorized disclosure, use, modification, or destruction.

The City shall comply with the Tennessee Public Records Act (the "TPRA") default presumption that all City records are available for inspection and copying unless they are protected by a specific exception under the TRPA. Any City department, agency or entity that disseminates Information in response to a TPRA request shall ensure that the appropriate classification is applied when that Information is released from their department.

When Information of the City with multiple classifications is stored, transmitted, or destroyed together, Information handling requirements for the higher classification shall apply.

3. Labeling and Handling

The City Information Owners shall develop and implement an appropriate set of procedures for information labeling and handling in accordance with the classification of information.

3.1 Access

The City shall restrict access to all forms of media containing Information of the City to only those authorized. Access shall be controlled using appropriate security measures (password protected, key lock, electronic locks, etc.) based on the characteristics of the information, including, but not limited to, the classification, physical state, use case, of the information.

The information shall be encrypted as part of the handling process if required by the classification of the information, as directed by the Information Owner or designee or as required by applicable statutes and regulations.

3.2 Labeling

The City shall label removable media (i.e. electronic, magnetic, optical, and paper) indicating:

- if it contains Sensitive Information;
- the distribution limitations of the information;
- any other applicable security and handling descriptions (see Section 3.3 below).

Removable media containing Sensitive Information may be exempted from labeling as long as the media remains in a defined Secure Area.

Classification of Information Assets, including workstations and servers, shall be based on the highest classification of the Information stored on the asset and secured appropriately.

3.3 Security and Handling Descriptions

3.3.1 The City shall support and use descriptions and other representations of information classification. These include tags in metadata, watermarks, footers, headers, etc. Descriptions and other representations should be clearly displayed where appropriate.

3.3.1 Established security shall be maintained when information is exchanged between and/or within information systems or additional parties, including hosting providers.

DEFINITIONS

Terms used in this policy are defined in the *Shelbyville Information Security Glossary*.

CONTACT

Questions should be directed to email at kade.stier@shelbyvilletn.org, or by mailing them to Director, Information Technology Department, 201 N Spring St, Shelbyville, TN 37160.

REFERENCES

ISO 27002: sections 7.2, 7.2.1, 14.1.2, 7.2.2, 9
NIST Special Publication 800-53 Rev5, *Recommended Security Controls for Federal Information Systems and Organizations*: RA-2, CC-9, AC-16, MP-2, MP-3, SC-16
Tennessee Public Records Act, T.C.A. §
10-7-503 Tennessee Code Annotated
10-7-101 et seq.
Criminal Justice Information Services Security Policy version 5.6
Center for Internet Security Critical Security Controls v 6.0, 10.1, 13.1, 13.2, 13.3, 13.4, 14.2 14.5 NIST Cyber Security Framework, ID.AM-4, PR.AC-4, PR.PT-2

REVISION HISTORY

REVISION	APPROVAL DATE	CHANGES
1.00	6/17/2024	Initial Release