Texas Veterans Commission
Data Classification Policy

I.   Purpose

Information security is best managed when data is classified and the risks associated with each category are uniform and understood. Data classification is the act of assigning a level of sensitivity per its adverse impact on the security goals of Confidentiality, Integrity and Availability. Among the benefits of proper data classification are: define common terms for managing data assets; establish minimum security controls; assist in achieving economies of scale with security services and protection; assist in contingency and disaster planning. This policy is to establish a framework for properly classifying and managing Data assets in accordance with Texas Administrative Code, Title 1, Chapter 202 (1 TAC 202).

II.   Scope

All Data, in whatever form and media that is the property of the Texas Veterans Commission (TVC), that is transmitted, processed, used or stored in whatever Information Resource must be classified. Data that is personal to the User and transmitted, processed, used or stored on TVC Information Resources because of incidental personal use does not have to be classified.

III.   Data Classification Standard

The data classification scheme outlines three classification labels.

Public

The Public information label is used for information such as published reports, press releases, and information published to the TVC public website. Such information requires no authentication and is freely distributable by all TVC personnel.

Sensitive

Information may still be subject to public release under an open records request, but the information should be vetted and verified before release by select employees who are familiar with state and federal rules regarding its disclosure. These types of data include items such as employee records and some PII. While these records and information are considered "public" under the PIA, they should still be afforded a higher level of protection to ensure its integrity and that Confidential data is not comingled.

Confidential

The Confidential label is used to identify information that is typically excepted from public disclosure, whether specified in law or through a decision by the Open Records division of the Texas Attorney General's office. Confidential items include information such as attorney-client communications, protected draft communications, and computer vulnerability reports. Additionally, the Confidential label is used to identify information that may be regulated by federal statute such as HIPAA, FERPA or third-party agreements and may have specific requirements placed on that information by a non-Texas regulation. Confidential data is released by select employees who are familiar with state and federal rules regarding its disclosure.

IV.   Calculating a Data Classification and Minimum Security Controls

It is the responsibility of the Information Owners to identify Data, to assign its classification label and to ensure it is protected by minimum security controls. To classify Data, consider its expected impact on security goals and decide as guided by the following table:

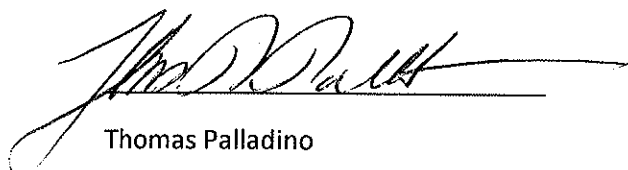|	Expected Impact on the CIA	Marking Requirement	Read/write Access Restriction	Encryption (transit and storage)
Public	Limited adverse effect	No	No for read access	No
Sensitive	Serious adverse effect; e.g. loss of reputation or trust	No	Yes	No
Confidential	Severe or catastrophic effect; e.g. potential criminal or civil penalties, loss of right to collect revenue	Yes	Yes	Yes, for Data on electronic media

Additional security controls may apply on certain data as required by TVC Information Security Policy or state and federal regulations. The classification labels on data may change throughout its lifecycle. The labels used in this data classification standard are in no way meant to subvert, contradict, supplant, or conflict with any applicable laws.

V.   Version History

1.0   May 31, 2017 – Adoption

VI.   Approval and Adoption

The Texas Veterans Commission Data Classification Policy was approved and adopted by the Executive Director per the signature and date below. This policy is subject to periodic review and may change to supersede existing policies.

_____   6/8/17
Thomas Palladino   Date

Executive Director