Title: Data Classification		Code Number: IT.018.00
Functional Category: Information Technology Services	Issuing Department: Information Technology Services	Effective Date: 12/15/2014

1.0 PURPOSE

1.1 To ensure the Board's information assets are identified, properly classified, and protected throughout their lifecycles.

2.0 DEPARTMENTS / PERSONS AFFECTED

2.1 This policy applies to all employees and consultants/contractors with access to the Board's network that use or intend to use the following:

2.1.1 The Board's data, user-developed data sets, and systems that may access this data, regardless of the environment where data resides (including systems, servers, cloud services, personal computers, laptops, mobile devices, etc.).

2.1.2 Media on which data resides (including hardcopy, electronic, microfiche, USB flash drive, CD, etc.) in any form (e.g., text, graphics, video, and voice).

3.0 POLICY

3.1 **Data Classification.** Classification of the Board's information shall be determined on the basis of confidentiality, integrity, availability, and impact levels. All data created, used, processed, transmitted, stored, or otherwise held by the Board shall be assigned to one of the categories listed below.

3.1.1 **Public Data.** Data designated as public is open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Some examples of public data include: publicly posted press releases, certain maps, public access webpages, etc.

3.1.2 **Internal Use Only Data.**

3.1.2.1 Internal use only data is information that is restricted to those who have a legitimate purpose based on business need for accessing such data.

3.1.2.2 Internal use only data must be protected to prevent loss, theft, unauthorized access, and/or unauthorized disclosure. All employees must follow the Public Information Requests policy before providing this information to external parties.

3.1.3 **Confidential Data.**

3.1.3.1 Confidential data is information protected by statutes and regulations or contractual language. Unauthorized disclosure, alteration, or destruction of the confidential data could cause a significant level of risk to the Board. Confidential data includes, but is not limited to, passwords, encryption keys, Personally Identifiable Information (PII), Sensitive Security Information (SSI), Payment Card Industry (PCI) information, and Electronic Protected Health Information (ePHI).

3.1.3.2 Confidential data must be protected to prevent loss, theft, unauthorized access, and/or unauthorized disclosure. All employees must follow the Public Information Requests policy before providing this information to external parties.

3.2 **Information Asset Protection.**

3.2.1 All Board information should have an Information Owner. Owners are established within the Board's lines of business functions.

3.2.2 Hardcopy materials that include confidential data shall only be distributed or available to authorized individuals or individuals with a legitimate need to know. Access to any area where hardcopy records with confidential data are stored must be limited by the use of controls (e.g., locks, monitoring, etc.) sufficient to prevent unauthorized entry.

3.2.3 National Institute of Standards and Technology (NIST) approved encryption shall be applied when transmitting and storing confidential information.

3.2.4 Electronic media containing confidential information must be sanitized appropriately and/or physically destroyed by shredding the media prior to disposal.

3.2.5 In case of an unauthorized access to confidential data such as PII, SSI, PCI, and ePHI, the Senior Information Security Manager or the Senior Vice President of Information Technology Services (ITS) must be contacted immediately.

3.3 **Exceptions.** Exceptions to this policy require the approval of the Chief Financial Officer with concurrence of the Executive Vice President of Administration and Diversity. Requests for exceptions, along with sufficient justification, must be submitted in writing by the requesting department head to the Chief Financial Officer. Each subsequent request for an exception must stand on its own merit and circumstances without regard to prior exceptions granted.

4.0 PROCEDURE

4.1 Not applicable.

5.0 RESPONSIBILITIES

5.1 **Chief Financial Officer**. Authorized to approve exceptions to this policy with concurrence of the Executive Vice President of Administration and Diversity; also responsible for ensuring Board-wide compliance with this policy.

5.2 **Senior Vice President of ITS**. Responsible for ensuring Board-wide compliance with this policy.

5.3 **Information Owners.** Responsible for:

5.3.1 Creating an initial classification, including assigning classification levels to all data.

5.3.2 Ensuring that information will be regularly reviewed to ensure confidentiality, integrity, and availability of the data.

5.3.3 Performing periodic reclassification based upon business impact analysis and changing laws, regulations, and/or security standards.

5.3.4 Confirming compliance with the Board's retention schedules and procedures based on the content for proper disposition of all information assets.

5.3.5 Granting and revoking access rights to confidential and internal use only data that reflects users' current roles and responsibilities.

5.4 **Senior Information Security Manager.** Responsible for:

5.4.1 Implementing access rights to confidential and internal use only data approved by Information Owners/Business Process Owners.

5.4.2 Regularly reviewing user access to confidential data for appropriateness.

5.4.3 Educating end users regarding classification and ensuring that there is appropriate level of security awareness for proper handling of confidential information.

5.5 **Employees.** Responsible for complying with this policy and protecting Board data from unauthorized access, modification, generation, disclosure, transmission, or destruction.

6.0 DEFINITIONS

6.1 **Electronic Protected Health Information (ePHI).** Has the meaning set forth in 45 CFR 160.103, and generally means individually identifiable health information that is transmitted or maintained in any electronic media.

6.2 **Information Owner.** A person or group of people with authority for specified information and responsibility for establishing controls for its generation, collection, processing, dissemination, and disposal.

6.3 **National Institute of Standards and Technology (NIST).** A measurement standards laboratory which is a non-regulatory agency of the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life.

6.4 **NIST-Approved Encryption.** NIST develops and promotes cryptographic standards that enable U.S. Government agencies and others to select cryptographic security functionality for protecting their data.

6.5 **Payment Card Industry Data Security Standard (PCI DSS).** A worldwide information security standard defined by the Payment Card Industry Security Standards Council. Provides an actionable framework for developing a robust payment card data security process – including prevention, detection, and appropriate reaction to security incidents.

6.6 **Personally Identifiable Information (PII).** Per NIST, PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

6.7 **Sensitive Security Information (SSI).** Information obtained or developed in the conduct of security activities, including research and development, the disclosure of which Department of Homeland Security/Transportation Security Administration has determined would, among other things, be detrimental to the security of transportation.

7.0 RESOURCES / FORMS

7.1 **Standards for Security Categorization of Federal Information and Information Systems.** Visit http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

7.2 **Texas Public Information Act.** Chapter 552 of the Texas Government Code, formerly known as the "Texas Open Records Act." Gives individuals the right to access government records; however, certain exceptions may apply to the disclosure of the information.

7.3 **Related Policies**.

7.3.1 Public Information Requests.

8.0 REVISION HISTORY

8.1 12/15/2014 – IT.018.00 – Original document.