ADMINISTRATIVE PROCEDURES

Title: DATA CLASSIFICATION AND HANDLING	**Identification:**	**9.08**
	Page:	**1 of 23**
	Effective Date:	**March 18, 2014**
Authority: **SBE 6A-14.0261** **FS 1001.64; 1001.65**	**Signature/Approval:**	**Dr. Ken Atwater**

PURPOSE

This procedure establishes a framework for classifying and handling of data at Hillsborough Community College based on its level of sensitivity, value and criticality. The classification of data will be used to determine baseline security controls for the protection of data.

PROCEDURE

All data or information created, collected, stored or processed by Hillsborough Community College in any form, electronic or non-electronic shall be classified and handled based on its level of sensitivity, value and criticality which will be used to determine the baseline security controls for the protection of data. Data Owners shall be identified for Restricted and Sensitive data and will typically be the senior leadership or their designee, with the ultimate responsibility for protection of data. All data at the College shall be categorized in one of the three following categories (tiers), with the highest level category (tier) applied to the data, if the data falls into multiple categories.

1. **Restricted (Tier 1**): This is the highest level of data classification category. Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to HCC or its affiliates. Data in this category is highly sensitive and may have personal privacy considerations, or may be restricted by federal and/or State of Florida laws. In addition, the negative impact on the institution, should this data be incorrect, improperly disclosed, or not available when needed, is typically very high.

   Examples of Restricted data include official student grades and financial aid data, social security and credit card numbers, and individuals' health related information.

   Access to Restricted data must be controlled from creation to destruction, and will be granted only to those persons affiliated with HCC who require such access in order to perform their job ("need-to-know"). Access to Restricted data must be individually requested and then authorized by the Data Owner or designee who is responsible for the data.

2. **Sensitive (Tier 2):** This is the second level of data classification category. Data should be classified as Sensitive when the unauthorized disclosure, alteration or destruction of that data could cause a moderate level of risk to HCC or its affiliates. This type of Data is moderately sensitive in nature. Often, this type of data is used for making

decisions for making decisions, and therefore it is important that this information remain timely and accurate. The risk for negative impact on the institution, should this data be incorrect, improperly disclosed, or not available when needed, is typically moderate

Examples of Sensitive data include official College records such as human resources information, financial information, strategy documents and information used to secure the college's physical or information environment.

Access to Sensitive data must be requested from, and authorized by, the Data Owner or designee who is responsible for the data. Access to Sensitive data may be authorized to groups of persons by their job classification or responsibilities ("role-based" access).

3. **Public (Tier 3):** Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the College and its affiliates. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

   Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions.The integrity of Public data should be protected. The appropriate Data Owner must authorize replication or copying of the data in order to ensure it remains accurate over time.

   Examples include, but are not limited to, advertisements, job opening announcements, college catalogs, regulations and policies, faculty publication titles and press releases.

RESPONSIBILITIES

Data owners/custodians are responsible for appropriately classifying data. Every data user is responsible for complying with data use requirement.

Please refer to Data Classification Guidelines and Data Handling Requirements at https://www.hccfl.edu/oit/operational-procedures.aspx