Information Technology Policies Manual	Policy Number	IT-03
	Effective Date	02-Mar-2014
Subject Academic and Administrative Systems – Data Classification	Most Recent Review Date	01-Dec-2013
	Due Date for Next Review	01-Sep-2016
Responsible Office: Chief Information Officer	Pages of this Policy	**1** of **1**

3. Academic and Administrative Systems - Data Classification

Overview

Defines data classification in various UAEU business areas according to its degree of sensitivity and risk.

Scope

Applies to any individual who may access or manage any UAEU academic or administrative information system.

Objective

Ensures that UAEU has appropriate means to protect its electronic data accessed through any academic or administrative system and that all community members appreciate the importance of data protection and act in a way that ensures appropriate data use.

Policy

1. UAEU information assets are crucial to its operations. This data classification policy framework has been established to protect UAEU data and to minimize any risk that could negatively impact UAEU's operations or its ability to fulfill its mission. Data classification is a method of identifying the levels of data based on sensitivity and risk.
2. The data used in any academic or administrative system can be classified into four categories:

LEVEL 1 - CONFIDENTIAL (Restricted)

Restricted data is defined as highly sensitive data. Disclosure of such data may have severe negative impact on UAEU. The highest level of control should be applied to data classified in this category. Some examples of such data include financial information, protected student information, staff and faculty personal information, and file encryption keys.

LEVEL 2 -PRIVATE

Private data is defined as moderately sensitive data; disclosure of such data may seriously impair UAEU's operations. Such data would not normally include information considered 'confidential'. Private data include research results and some financial transactions.

LEVEL 3 -SENSITIVE (Internal Use Only)

Sensitive data is not approved for distribution outside UAEU; however disclosure of this information is considered low-risk and unlikely to damage or inconvenience UAEU. Examples of sensitive information include meeting minutes (when appropriate), memoranda, business plans, and internal project reports.

LEVEL 4 -PUBLIC

Public data are defined as data that can be readily accessed by the public. The disclosure of such data has either a neutral or a positive impact on UAEU. Some examples include media and press statements, class schedules, UAEU maps, and newsletters.

جامعة الإمارات العربية المتحدة United Arab Emirates University UAEU	**Information Technology Procedures Manual**	Related Policy	IT-03
		Effective Date	01-Sep-2014
	Subject Academic and Administrative Systems – Data Classification	Most Recent Review Date	01-Dec-2013
		Due Date for Next Review	01-Sep-2016
	Responsible Office: Chief Information Officer	Pages of these Procedures	**1** of **1**

Procedures of Policy No. (3) - Academic and Administrative Systems - Data Classification

1. It is the responsibility of each data custodian to define the data classification for his/her business area. Users who have access to any UAEU academic or administrative systems must verify the data classification of the data they access with the data custodian before sharing such data internally or externally.

2. The designated data custodians for any academic and administrative systems are responsible for reviewing data within their domain and labeling such data based on the categories described above.

3. The data custodians are responsible for applying all necessary controls to ensure adequate protection of UAEU data within their assigned responsibilities.

4. The Chief Information Officer (CIO) is responsible for enforcing this policy.

5. The academic or administrative systems officer is responsible for coordinating and working with UAEU data custodians to assist in applying controls to data, based on definitions and labels provided by the data custodians.

6. The systems' end-users are responsible for usage of data following the definitions and classifications provided by the data custodians.