Information Technology Group
Policy Name: Data Classification Policy
Date Issued: 05/02/2013

1. Introduction
   Columbia Business School community members have a shared responsibility to protect University data from unauthorized access, modification, disclosure or destruction.
2. Audience and Scope
   This policy is applicable to all faculty and staff of Columbia Business School that use CBS owned and managed systems.
3. Purpose
   The purpose of this document is to set policy for CBS Faculty and Staff policy with respect to data classification. This policy outlines our commitment to protecting University-owned data.
4. Data Classification
   a. Confidential
      i. Data should be classified as confidential when the unauthorized disclosure, modification, or destruction of that data could cause a significant risk to Columbia Business School, Columbia University, or its business partners. Examples of Confidential data include data that is protected by state or federal regulation or contractual obligation. This is the most stringent data classification level.
   b. Private
      i. Data should be classified as private when the unauthorized disclosure, modification, or destruction of that data could cause a moderate risk to Columbia Business School, Columbia University, or its business partners. By default all CBS data that is not classified as confidential or public should be considered private. Careful consideration and care should be taken with private data.
   c. Public
      i. Data should be classified as public when the unauthorized disclosure, modification, or destruction of that data would result in little to no risk to Columbia Business School, Columbia University, or its business partners.
5. Definitions
   a. PII – Personally identifiable information: PII is defined as any information about an individual maintained by Columbia Business School, 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. All PII should be treated as confidential information.
   b. FERPA – Family Educational Rights and Privacy Act – If “right of privacy” is invoked, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance of that student or student’s family (under 18 years of age) must be treated as confidential information.

Revision History:

Version	Author	Date	Comments
1.0	Ryan Whitworth	05/02/2013	Draft Document