UNION COLLEGE
of Union County, NJ

**Data Classification Security**

**Purpose**

Any person who uses, stores or accesses data contained in the technology systems of Union College of Union County, NJ ("Union College") has the responsibility to safeguard that data. Data classification is one method of determining the safeguard required for certain data and the appropriate College response to the unauthorized release of that data. Such safeguards and response plans are not only good stewardship for College data, but are required by certain state and federal law and regulations.

**Scope**

This policy governs the privacy, security and integrity of College data stored on College IT systems and outlines the responsibilities of the individuals and organizational units that manage, use, access, store or transmit that data. This policy supplements, but does not supersede, the College's Confidentiality Agreement.

**Policy**

I. Union College IT Services maintains systems that store data essential to the performance of College business. All members of the community have a responsibility to protect College data from unauthorized access, use, storage, transmission, disclosure or destruction.

II. All College data is classified into four levels of security classification: Protected Data, Sensitive Data, Directory Data, and Public Data. For the purposes of this policy, data not formally classified (Unclassified Data) will be considered Sensitive Data. For the purposes of the College's Confidentiality Agreement, all data except Public Data is to be considered confidential.

    a. Protected Data is data that (a) if compromised would expose members of the College and its community to a high risk of identity theft or financial fraud and (b) is protected by Federal or state law or regulations. Applicable law and regulatory requirements include (but are not limited to) the Family Educational Rights and Privacy Act (FERPA), the Fair and Accurate Credit Transactions Act (FACTA), the Health Insurance Portability and Accountability Act (HIPAA), and other applicable Federal and NJ State laws. Examples of Protected Data include, but are not limited to:

        i. Social Security Number
        ii. Driver's License Number, Passport Number, or any State ID Number
        iii. Credit Card Information (Number, expiration date, security code)
        iv. Date of Birth
        v. Users' Systems Passwords
        vi. Medical history
        vii. Disability
        viii. Student and family financial history
        ix. Student account balances
        x. Donor financial history

xi. Student Financial Aid history
xii. Student academic history, including student grades

b. Sensitive Data is data that, while not explicitly protected by federal or state law, is proprietary to the College and would, if released, expose the College and members of the community to a heightened risk of identity theft or financial fraud. Examples of Sensitive Data include, but are not limited to:
    i. Employee salary or employment history
    ii. Permanent or Local Address
    iii. Department budgets
    iv. Student registration Personal Identification Numbers
    v. Internal operating procedures and operational manuals
    vi. Internal memoranda, emails, reports and other documents
    vii. Technical documents such as system configurations and floor plans
c. Directory Data is data that is used for College communication or to link records between College systems or reports. Such directory information is widely available to members of the College community, but nevertheless should be handled with care, since exposure could result in an increased risk of financial fraud or identity theft for the College and members of the community. Examples of Directory Data include, but are not limited to:
    i. Usernames
    ii. Campus wide IDs
    iii. ID photos
    iv. Class Rosters/Advisor Rosters
d. Public Data is data that the College may or must make available to the public with no legal or other restrictions, via its website or various reports, press releases, reports and the like. Examples of Public Data include:
    i. Information posted on the College's website
    ii. The College phone directory
    iii. The College's annual financial reports
    iv. Data published in the Integrated Postsecondary Education Data System documents
    v. Copyrighted materials that are publicly available

III. The loss, unauthorized access to or disclosure of Protected Data must be reported to the appropriate College officials, including the management of the organizational unit in which the data breach was discovered, the College's Chief Information Officer (CIO) and the Technology Helpdesk so that the appropriate response to the incident, including required notification of appropriate federal and state agencies, can be initiated.

IV. The loss, unauthorized access to or disclosure of Sensitive Data should be reported to the management of the organizational unit in which the data breach was discovered for their appropriate response.

V. For the purposes of the College's Confidentiality Agreement, all data except Public Data are considered confidential. The unauthorized access, disclosure or transmission of confidential information may result in disciplinary action by the College, including termination or expulsion, as outlined in the College's Confidentiality Agreement and other relevant College policies.

VI. College data are assets belonging to the College. Departments which collect, use, store and transmit College data should classify their data according to the level of risk associated with handling that data and implement appropriate safeguards to that data based on that risk. Data are generally stored in sets. The classification of a data set should be to the highest level of any data element in that set; for example, a report containing a combination of protected, sensitive directory and public data should be considered protected and provided with the safeguards appropriate for protected data. Individuals and departments must implement appropriate safeguards for accessing, transmitting and storing College data. Examples of appropriate safeguards for Protected and Sensitive Data include, but are not limited to:

a. The data must be protected to prevent loss, theft, and/or unauthorized access, disclosure, modification, and/or destruction.
b. The data may only be accessed or disclosed if necessary for College business purposes and consistent with applicable College policies.
c. The data must not be downloaded, stored or transmitted unless appropriately secured and/or encrypted.
d. The data must not be posted on any website or shared file storage space unless College standard authentication methods are used.
e. The data must be destroyed when no longer needed and in accordance with College policies.