Policy

Any person who uses, stores, or accesses data contained in the information technology systems (either academic or administrative) of Ocean County College has the responsibility to safeguard that data. Data classification is one method of determining the safeguard requirements for certain data and the appropriate College response to any 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.

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.

I. Ocean College IT Services maintains systems that store data essential to the performance of College business. All members of the College 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: Restricted (Protected) Data, Confidential (Sensitive) Data, Internal (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. Restricted or Protected Data is data that (1) if compromised would expose members of the College and its community to a high risk of identity theft or financial fraud and (2) 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), the Gramm-Leach-Bliley Act (GLBA), and other applicable Federal and New Jersey 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. Student Financial Aid history
    xi. Student academic history, including student grades

b. Confidential or 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. Internal or Directory Data is data that the College chooses to keep private, but any disclosure would most likely not cause material harm. It can also be used for College communication or to link records between College systems or reports. This could include directory information that is widely available to members of the College community, but nevertheless should be handled with care, since exposure could result in increased risk of financial fraud or identity theft for the College and members of the community. Examples of Internal/Directory Data include, but are not limited to:

i. Departmental policies and procedures
ii. Grant applications
iii. Usernames
iv. Campus wide IDs
v. ID photos
vi. 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, 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

e. When in doubt as to how any data should be classified among the four levels of security classifications above, contact your supervisor.

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 its 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.

An Information Security Classification Reference Guide is attached to this policy to assist in identifying data classification.

ADOPTED: June 29, 2023

Information Security Classification Reference Guide – June 29, 2023

Public Use Data Intended for release to the public	Internal/Directory Data May be shared only within the OCC community	Confidential/Sensitive Data Intended only for those with a "business need to know"	Restricted/Protected Data Requires strict controls
The College intentionally provides this information to the public.	The College chooses to keep this information private, but any disclosure would not cause material harm.	Disclosure of this information beyond the intended recipients may cause harm to the individual and/or the College.	Disclosure of this information beyond the specified recipients would likely cause serious harm to the individual and/or the College.
Examples: • Public phone directories • Student directory information* • Marketing materials • Course catalogs • Annual reports • Press releases • Regulatory and legal filings *Directory information about students who have requested FERPA blocks must be classified and handled as Confidential/Sensitive data.	**Examples:** • Departmental policies and procedures • Grant applications • Physical plant information that is not confidential or restricted • Non-public building plans or layouts that are not confidential or restricted • Campus wide IDs • ID photos • Class Rosters/Advisor Rosters	**Examples:** • Non-directory student information • Information protected under FERPA • Personnel Records • Donor information • Budget/financial transactions • Internal operating procedures and operational manuals • Internal memoranda, emails, reports and other documents • Technical documents such as system configurations and floor plans	**Examples:** • Government issued identifiers such as Social Security Number, Passport number, Driver's License Number, or any State ID Number • Individually identifiable financial account information such as Bank accounts, Credit/Debit Card information (number, expiration date, security code) • Personally Identifiable Information (PII) • User System Passwords/PINs • Individually identifiable health or medical/disability information • Student and family Financial/Financial Aid history, account balances, etc.

Feedback: If you have questions or concerns about the policy, or if you know of items that are out of compliance, please contact your supervisor or the College Chief Information Officer (CIO).

Use Your Good Judgement: The lists above are only examples and are not definitive classifications. When in doubt as to how any data should be classified among the four levels of security classification, contact your supervisor.