Policy Title	Original Adoption Date	Policy Number
Protection of Sensitive and Restricted Information	01/19/2015	IN-710
Responsible College Division/Department	**Responsible College Manager Title**	
Technology	Vice President of Administration	

Policy Statement

I. PURPOSE & APPLICABILITY

The purpose of this Policy is to help protect the confidentiality and integrity of sensitive information. This Policy requires the protection of sensitive information including Personally Identifiable Information (PII), Payment Cardholder Information (PCI), financial account/payment information, Protected Health Information (PHI), competitive business information, and Family Educational Rights and Privacy Act of 1974 (FERPA) non-directory information. This Policy applies to all employees.

II. CLASSIFICATIONS

Information is categorized into three different levels of classification.

Public: Information that is not restricted and is subject to open records requests. This includes FERPA directory information and some employee information.

Sensitive: Information used for college business and academic activities, although not covered with the same level of concern or legal protection as restricted information, sensitive information still needs to be protected. This includes financial account/payment information, competitive business information, and FERPA non-directory information (except social security number which is restricted information). Sensitive information will not be distributed to external parties except under written terms that protect the information's confidentiality and integrity.

Restricted: Information where improper disclosure or inappropriate access requires a breach notification in accordance with law or regulation. This includes PII, PCI, and PHI. Restricted information will not be distributed to external parties except under written terms that protect the information's confidentiality and integrity.

III. REQUIREMENTS

Sensitive and restricted information should only be collected, used, shared, transmitted, and stored when there is an academic, financial, patient care, community relations, or business purpose.

Sensitive and restricted information shall not be posted to web sites, portal sites, unprotected shared drives, or any other location that compromises the confidentiality or integrity of the information.

All sensitive and restricted information in electronic and paper formats must be controlled.

The President, Vice Presidents, Deans, Directors, and Managers have ultimate accountability for compliance with this Policy in their department/division, even if specific responsibilities are delegated.

The Director of Technology is responsible for developing, implementing, updating, and enforcing this Policy.

Immediately notify the Director of Technology if sensitive or restricted information has been lost, compromised, or disclosed without authorization.

IV. ENFORCEMENT

Employees who violate this Policy will be subject to the disciplinary process in accordance with College policies.

Reason for Policy

LTC is committed to protect sensitive information that is in its custody or control.

Historical Data, Cross References and Legal Review

Cross References:
Wis.Stat.134.98(1)(b)
Federal Regulations Title 34 §a Part 99
LTC Vendor security agreement
Family Educational Rights and Privacy Act of 1974 (FERPA)
NACHA Operating Rules - ACH Security Framework
NACHA - Sensitive ACH Data Security Policy
Payment Card Industry - Cardholder Data Security Policy
Payment Card Industry Data Security Standards (PCI DSS)
Records Management Policy

Legal Counsel Review and Approval:
Board Policy: III.F. Asset Protection

Definitions

Personally Identifiable Information (PII) means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable:

1. The individual's social security number.
2. The individual's driver's license number or state identification number.
3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.
4. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

Payment Cardholder Information (PCI) means debit/credit card numbers, expiration dates, card validation code, magnetic stripe track 1/2 data, etc.

Financial Account/Payment Information means full bank/brokerage account with associated routing numbers, balances, debts, etc.

Protected Health Information (PHI) means health records, treatment data, etc.

Competitive Business Information means intellectual property, legal/compliance, or other types of data elements subject to client-assigned confidentiality requirements.

Family Educational Rights and Privacy Act of 1974 (FERPA) Directory Information means information including name, city of residence, student email address, field(s) of study, current enrollment status, dates of attendance, degrees received, most recent previous educational institution attended, honors and awards received, including selection to a dean's list or honorary organization, and photos and videos of students for use in college presentations/displays, news releases, publications, and websites.

Family Educational Rights and Privacy Act of 1974 (FERPA) Non-Directory Information means information contained in the education records of a student that would be considered harmful or an invasion of privacy if disclosed.