3354:2-11-04 Data Security and Privacy Assurance.

A. Purpose

1) Lakeland Community College endeavors to protect the confidentiality, integrity and availability of all data in its care. Lakeland provides legitimate and timely access to information necessary to its teaching, learning, and administrative functions in support of its mission. The College recognizes that the interests of information security and free access to information are at times in conflict. Lakeland will attempt to resolve these conflicts, but prefers to protect data in what it views as necessary in compliance with federal, state, or local laws.

2) Information Security is to be embedded into all Lakeland activities. Rather than being merely the responsibility of the designated Compliance Officers, every Lakeland employee is responsible for the security of College information.

B. Definitions

1) Information Security provides that data that should remain confidential is protected against inappropriate use, while data required to carry out the College's mission is available to those who need it.

2) Covered Data refers to all information collected by, shared with, or reported to the College in the course of its daily activity that is protected by local, state or federal law or that the College is contractually obligated to protect. In addition, Lakeland may designate additional covered data through the creation of standards, procedures and guidelines. Covered data includes, but is not limited to:

   i. education records of students as defined by the Family Educational Rights Privacy Act (FERPA)
   ii. protected health information as specified by the Health Insurance Portability and Accountability Act (HIPAA);
   iii. identity theft regulations as enacted by the Federal Trade Commission at 16 C.F.R. 681 ("Red Flag" Rules);
   iv. student and customer financial information as specified by the Gramm Leach Bliley Act; and
   v. credit card data covered by the Payment Card Industry standards.

C. Guiding Principles

1) Compliance. Lakeland is committed to ethical business practices and compliance with all applicable laws, regulations, and policies that govern the privacy of Covered Data.
2) Minimize Access Privileges. Lakeland only grants to assigned individuals the reasonable, minimum access to Covered Data as needed to accomplish their institutional or pedagogical goals.
3) Separation of Duties. As can be reasonably accommodated, for each assigned duty that uses Covered Data, the College assigns one or more individuals or review bodies to oversee the proper handling and protection of that data.
4) Balance with Ohio Public Records Laws. Lakeland favors reasonable expectations of privacy of its constituents, consistent with the accomplishment of institutional goals and

in accord with applicable laws, standards and College policies. However, the College must always balance that expectation relevant to any records request under the State of Ohio's Public Records Law.

5) Notification. In the event of a breach of security that leaks Covered Data, senior College officials will determine, in light of the circumstances and applicable law, what risks are posed by the breach and whether and how those persons whose covered data was released should be notified.

D. Responsibilities

1) Compliance Officers are responsible for the creation, implementation, and oversight of Information Security for Lakeland's Covered Data. Although these Compliance Officers may report to different College officials, they are required to work closely together, along with other Lakeland employees, to: (a) identify reasonable, foreseeable vulnerabilities and threats to Covered Data; (b) design and implement safeguards to minimize risk, including the development and communication of College procedures; (c) periodically evaluate the effectiveness of safeguards; (d) limit the damage from security breaches; and (e) report findings to relevant College officials. Lakeland's designated Compliance Officers by area are the:
    i. Director for Admissions & Registrar for the Family Educational Rights and Privacy Act;
    ii. Director for Human Resources for the Health Insurance Portability and Accountability Act;
    iii. Controller and Bursar for Red Flag Rules;
    iv. Director of Administrative Technologies for the Gramm Leach Bliley Act; and
    v. Director of Financial Systems and Deputy Treasurer for Payment Card Industry Data Security standards.

2) In addition to its Compliance Officers, Lakeland has established additional responsibilities to support Information Security for its Covered Data including, but not limited to:
    i. Network, system, database, and application security administrators to define standards, procedures, and guidelines that minimize the risk of intrusion or breach, while allowing Lakeland entities to utilize these assets to their maximum benefit;
    ii. Area Data Custodians. Every piece of information collected by the College in its daily activities is collected on behalf of a department that requires that data for the realization of a specific goal. Employees in these departments are the custodians of that data, and have a responsibility to work with relevant Compliance Officers for maintaining the confidentiality and integrity of any Covered Data; and
    iii. Incident Response Teams. An Incident Response Team will be activated when a possible breach in Information Security for College Covered Data occurs to provide effective and orderly response and communications. An Incidence Response Team will include relevant College Officers and the affected Compliance Officer(s).

E. Additional Assurance Responsibilities

1) If, in the process of executing their duties, a member of Lakeland discovers a possible breach of Information Security for College Covered Data, they must report their findings immediately to either: (a) a College Officer; or (b) the relevant Compliance Officer. That College or Compliance Officer will coordinate necessary steps to investigate that possible breach as well as concurrently notify the College's Chief of Staff. The College's Chief of Staff will determine the appropriateness of activating an Incident Response Team.

2) As permitted by federal, state, or local laws, Covered Data may be disclosed to third parties pursuant to an executed agreement that requires that third party by contract to implement and maintain necessary Information Security safeguards.

Replaces: 3354:2-11-04

Effective: 11/05/2009

CERTIFIED ELECTRONICALLY

Certification

03/10/2015

Date

Promulgated Under: 111.15
Statutory Authority: 3354
Rule Amplifies: 3354
Prior Effective Dates: 11/5/2009