LIM COLLEGE

Draft - Data Security Policy ("DSP) and Program

Created on: March 3, 2019
Last Updated: July 17, 2020

Authored by: Chief Technology Officer
Approved by Board of Directors: July 30, 2020

Overview:

The purpose of Data Security Policy ("DSP") is to outline essential roles and responsibilities within the LIM College community for creating and maintaining an environment that safeguards systems and data from threats to personal, professional and institutional interests, and to establish a comprehensive information security program in compliance with applicable law.

As a Title IV participating institution, under Federal and state laws and other authorities, financial services organizations, including institutions of higher education, are required to ensure the security and confidentiality of customer records and information. Applicable law includes, but is not limited to, the Higher Education Act, as amended **(HEA)**; the Family Educational Rights and Privacy Act **(FERPA)**; the Gramm-Leach-Bliley Act **(GLBA)**; the Privacy Act of 1974, as amended; and the New York State - Stop Hacks and Improve Electronic Data Security Act **(SHIELD)**.

Definitions:

Data Resource: A Data Resource is a discrete body of information created, collected and stored in connection with the operation and management of the College, and used by members of the College having authorized access. Information Resources include electronic records and physical files.

Information System: An Information System is an integrated set of technologies used for collecting, storing, processing, and providing information (e.g. Sonis, Slate, Great Plains). An Information System may contain one or more Data Resources.

Data Security and Technology Framework: Data Security and Technology Framework (DSTF) shall mean a written set of technical requirements, standards, related procedures and protocols designed to protect against risks to the security and integrity of data that is processed, stored, transmitted, or disposed of through the use of LIM College Information Systems and Data Resources.

Information Security Officer ("ISO"): An individual responsible for the implementation, oversight, coordination and monitoring of this Data Security Policy program.

Data Security Working Group: The Data Security Working Group ("DSWG") shall be chaired by the Information Security Officer and shall consist of Data Security Managers also responsible for assisting with the implementation and management of LIM's Data Security Policy and program.

Users: Users include all members of the LIM College community to the extent they have authorized access to LIM Data Resources and Information Systems, and may include students, faculty, staff, contractors, consultants and temporary employees.

Data Security Breach: A Data Security Breach is any unauthorized access, disclosure, misuse, alteration, destruction or other compromise of LIM information.

Data Security Directive: Data Security Directives shall be issued from time to time by the Information Security Officer or members of the Data Security Working Group to provide clarification of this policy, or to supplement this policy through more detailed procedures or specifications, or through action plans or timetables to aid in the implementation of specific security measures. All Data Security Directives issued by the DSWG shall be deemed incorporated herein. Publications shall be shared on applicable digital platforms (email, College website, intranet portal).

Policy Statements and Responsibilities:

1. All members of the college community share in the responsibility for protecting the security and confidentiality of LIM systems and data.

2. This policy is designed to establish the authority and responsibilities for ensuring proper administrative, technical and physical safeguards, protecting LIM College systems and its data.

3. It is the policy of the College that all Confidential, Restricted, and Public information be safeguarded from unauthorized access, use, modification or destruction. This policy applies to all information collected, stored or used on behalf of any operational unit, department and person within the LIM community. This also applies to all 3rd party providers – consultants, vendors, cloud (SAAS) service providers.

4. This policy assigns roles and duties of the Information Security Officer, the Data Security Working Group and LIM users.

5. This policy outlines LIM's Data Security and Technology Framework ("DTSF"), a written set of technical requirements, standards, related procedures and protocols designed to protect against risks to the security and integrity of LIM systems and data.

6. This policy outlines response procedures and requirements, in the event of a security breach.

Data Security and Technology Framework:

LIM College's Data Security Program is built within the Data Security and Technology Framework ("DSTF"), which includes a written set of technical requirements, standards, related procedures and protocols designed to protect against risks to the security and integrity of systems and data that is processed, stored, transmitted, or disposed of through the use of LIM College Information Systems and Data Resources. This includes security policies, controls, procedures, ongoing monitoring and management for the Information System(s) and Data Resources which support all operational aspects of the College.

DSTF shall include system, computer, network, physical, and paper security requirements that meet basic requirements, set forth in the guidelines and standards outlined by regulations of the Federal Trade Commission (FTC), and applicable federal and state laws, rules and regulations. The Data Security Policy shall establish minimum / basic data security standards and may elect to modify and / or include additional data security requirements, standards, and protocols at any given time.

This Data Security Policy and Program is built on the following Six (6) steps, and fourteen (14) requirements outlined in LIM's Data Security and Technology Framework.

Six (6) Steps:

1. Develop, implement, and maintain a written data security program;
2. Designate the employee(s) responsible for coordinating the data security program;
3. Identify and assess risks to customer information;
4. Design and implement an information safeguards program;
5. Select appropriate service providers that are capable of maintaining appropriate safeguards; and
6. Periodically evaluate and update the security program.

14 Requirements:

1. **Access Control -** Limit information system access to authorized users;
2. **Awareness and Training -** Ensure that system users are properly trained;
3. **Audit and Accountability -** Create information system audit records;
4. **Configuration Management -** Establish baseline configurations and inventories of systems;
5. **Identification and Authentication -** Identify and authenticate users appropriately;
6. **Incident Response -** Establish incident-handling capability;
7. **Maintenance -** Perform appropriate maintenance on information systems;
8. **Media Protection -** Protect media, both paper and digital, containing sensitive information;
9. **Personnel Security -** Screen individuals prior to authorizing access;
10. **Physical Protection -** Limit physical access to systems;
11. **Risk Assessment -** Conduct risk assessments;
12. **Security Assessment -** Assess security controls periodically and implement action plans;
13. **System and Communications Protection -** Monitor, control, and protect organizational communications;
14. **System and Information Integrity** - Identify, report, and correct information flaws in a timely manner.

Security Breach Response:

As provided above, LIM Users, Data Security Working Group Members, and the Information Security Officer must document and report any known Data Security Breach or incident that has caused or is likely to cause a Security Breach. Examples of reporting bodies include college leadership, general counsel, Board of Directors, Federal, State and local entities. These incidents include, but are not limited to, internal data theft, computer malware and viruses, worms, or computer "attacks" that may lead to unauthorized access of confidential or restricted information. See ***"Appendix A – Data Security Policy and Program"*** for additional information on the colleges breach response procedures.

Note on Enforcement: Per the Computer and Network Use Policy, the College reserves the right to monitor network traffic, perform random audits, and to take other steps to ensure the integrity of its information and compliance with this policy. Violations of this policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this policy may result in dismissal from the College.

Roles and Responsibilities:

1. **ROLE OF THE INFORMATION SECURITY OFFICER ("ISO"):** Responsible for the implementation, oversight, coordination and monitoring of this Data Security Policy and its security procedures. Information Security Officer shall be responsible for:
    a. Prompt coordination and communication of any data security breaches with the Data Security Working Group and LIM Senior leadership
    b. Serving as the primary point person for reporting breaches to government agencies per applicable law(s)
    c. Oversight and management of the LIM "Data Security and Technology Framework"

d. Chairing the Data Security Working Group (DSWG).

2. **ROLE OF THE DATA SECURITY WORKING GROUP ("DSWG"):** Responsible for (a) assisting with the implementation and management of LIM's Data Security Policy and program, (b) aiding in the development of procedures and guidelines concerning the collection, storage, and use of digital and physical data by the College community, and (c) assisting the Information Security Officer in the implementation of this policy. The DSWG shall be responsible for:
    a. Monitoring federal, state, and local legislation concerning privacy and data security.
    b. Remaining abreast of evolving best practices in data security and privacy in higher education and assessing whether any changes should be made to LIM's Data Security and Technology Framework.
    c. Establishing data privacy and security training and awareness programs for the College
    d. Periodically assessing whether these programs are effective.
    e. Inventorying Personally Identifiable Information (PII) on Data Resources and Information Systems
    f. Periodically reassessing this policy to determine if amendments are warranted
    g. Discussing any Security Breaches, violations of this policy, and recommending any further actions or changes in practice or policy.

3. **USERS:** Users are responsible for complying with all security-related procedures pertaining to any Data Resource and Information Systems to which they have authorized access or any information therefrom that they possess. Users obligations will be (a) posted on LIM's website, intranet, employee handbook, student handbook, and (b) disseminated via email and through the use of other marketing campaigns. Users include all Staff, Faculty, Student, and 3rd party providers – consultants, vendors, cloud (SAAS) service providers.

    Specifically, a User is responsible for:
    a. Becoming familiar with and complying with all College technology / data policies
        i. Including, without limitation, this policy, and all Data Security Directives contemplated hereby, the Computer and Network Use Policy, Electronic Mail ("email") Policy & Procedure, P2P Policy, and Data Classification Policy.
    b. Adhere to digital and physical security safeguards of LIM data, computing systems, storage media, and physical (paper) files. The following uses are strictly prohibited:
        i. The use of LIM data in an unsecured, unauthenticated manner.
        ii. The use of LIM systems and equipment by unauthorized Users (on campus and remotely).
        iii. Unattended confidential paper files not stored in a secure location.
    c. Adhere to LIM College's **"Confidential, Restricted, or Public Data Classification Policy"**
        i. Users must comply with this Policy and all relevant Data Security Directives irrespective of where the LIM College data might be located, including, for example, on home devices, mobile devices, on the Internet, or other third-party service providers.
    d. Adhere to the following procedure when access to information is no longer required by a User. Contact ISO or DSWG with any / all questions pertaining to access.
        i. Restricting of access and/or disposing of data in a manner to insure against unauthorized interception of any "Confidential or Restricted" information.
        ii. Paper-based copies of Confidential or Restricted documents should be properly shredded and destroyed.
        iii. Electronic data taken from Confidential and Restricted databases should also be properly destroyed or archived with proper encryption.
    e. Immediately ensure notification is made to the Information Security Officer or a member of the Data Security Working Group of any incident that may cause a security breach or violation of this policy.