Title: Cybersecurity and Information Technology Risk Management Policy

Background: Risk identification, assessment, and mitigation is a way for security professionals to identify, assess, and mitigate potential risks to reduce their impact and maximize opportunities. It's a way of looking at potential threats, weaknesses, and unknowns that could affect an organization's goals, projects, or activities. The goal is not to eliminate all risks, which is often impossible, but to proactively manage and control them within acceptable levels.

Point of Contact: Director of Information Technology

Other LC State offices directly involved with the implementation of this policy, or significantly affected by the policy: All offices at LC State

Date of approval by LC State authority: March __, 2024

Date of State Board Approval: N/A

Date of Most Recent Review: March __, 2024

Summary of Major Changes incorporated in this revision to the policy: New Policy to comply with federal requirements, including with the Gramm-Leach-Bliley Act (GLBA)

1. Philosophy:

A. Cybersecurity is a collective responsibility that requires policies that apply to all components of LC State. Threat, vulnerability, and the likelihood of exploitation are complex and unique to specific business processes and technologies. Cybersecurity risk is measurable depending on quantified or classified aspects of the data; characteristics of the information system; the definitions and characteristics of internal or external threats, systems, or environmental vulnerabilities; and the likelihood that the event or situation may manifest itself within a given application, information system or architecture. External threats evolve rapidly and are persistent based on the criminal intent or the resources of the attacker, whether they are criminal or nation-state backed. Internal threats can be accidental or intentional.

B. The impact of using diverse but competing approaches in implementing security controls applied to information systems tends to elevate overall cybersecurity risk. The management of cybersecurity risk will use a detailed Risk Management Framework tied to the Center for Internet Security Critical Security Controls (CIT CSC) and cross walked to NIST 800-171 through to balance academic/business needs, the potential impact of adverse events, and the cost to reduce the likelihood and severity of those events.

C. The risk management process is established in policy so that the LC State community can share a common understanding that:

   i. LC State is determined to manage cybersecurity risk proactively. Not doing so will likely have unacceptable consequences for individuals and increase costs to the institution.

   ii. This is a mandatory and universally applicable process for managing cybersecurity risk. The process can be tailored to specific technologies, processes, or services.

   iii. The process must include policy and procedural controls to ensure that privacy and academic freedom are respected.

2. Definitions

A. Cybersecurity Governance, Risk Management, & Compliance (GRC) Team

Individuals who are knowledgeable about the organization's Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security and Health Information Technology for Economic and Clinical Health Act (HITECH) policies, procedures, training program, computer system set up, technical security controls, and who are responsible for the Cybersecurity risk management process and procedures outlined below. This team manages responsibilities for Cybersecurity risk management processes and procedures with the following areas of responsibilities: Cybersecurity, Public Safety, Enterprise Privacy, Legal, HR, Communications, Compliance and Enterprise Risk Management, Internal audit, Information Technology Services, and Security/Technology subject matter experts.

B. Cybersecurity Risk Management

Refers to two major process components: risk assessment and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

C. Electronic Protected Health Information (ePHI)

Any identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

D. Family Educational Rights and Privacy (FERPA) Protected Data

Any personally identifiable information in a student's education record covered under FERPA regulations.

E. Protected Data-NPI (nonpublic personal information)

i. provided by a consumer to a financial institution

ii. resulting from any transaction with the consumer or any service performed for the consumer

iii. otherwise obtained by the financial institution

F. Payment Card Industry Data Security Standard (PCI DSS)

Data collected by organizations that accept, store, transmit, or process cardholder data must comply with the PCI DSS and is administered by the PCI SSC (Payment Card Industry Security Standards Council) to decrease payment card fraud across the internet and increase payment card data security. This includes sensitive data presented on or stored on a card - and personal identification numbers entered by the cardholder.

G. Risk

The likelihood that a threat will exploit a vulnerability and the impact of that event on the confidentiality, availability, and integrity of ePHI, financial NPI, protected cardholder data, and student education records (and other confidential or proprietary electronic information, and other system assets).

H. Risk Assessment

Referred to as Risk Analysis in the HIPAA Security Rule, and is the process that identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;

prioritizes risks; and results in recommended possible actions/controls that could reduce or offset the determined risk.

I. Risk Mitigation

Referred to as Risk Management in the HIPAA Security Rule, and is a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

J. Threat

The potential for a particular threat-source to successfully exercise a particular vulnerability.

Threats are commonly categorized as:

i. **Environmental**: external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, hazardous material spills. etc.

ii. **Human**: hackers, data entry, workforce/ex-workforce members, impersonation insertion of malicious code, theft, viruses, SPAM, vandalism, etc.

iii. **Natural**: fires, floods, electrical storms, tornados, etc.

iv. **Technological**: server failure, software failure, ancillary equipment failure, etc.

v. **Other**: explosions, medical emergencies, misuse, or resources, etc.

K. Threat Source

Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental, which can impact the organization's ability to protect ePHI, financial NPI, protected cardholder data, and student education records.

L. Threat Action

The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

M. Vulnerability

A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

3. Policy

It is the policy of LC State to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, availability of its electronic data, including any FERPA-protected data, health information (ePHI), protected cardholder data, financial nonpublic personal information (NPI), and student education records (and other confidential and proprietary electronic information) and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the organization's Cybersecurity program.

4. Responsibilities

A. Director of Information Technology (DIT)

i. Manage the Cybersecurity Risk Management program and coordinate the development and maintenance of Cybersecurity Risk Management policies, procedures, and standards.

ii. Ownership of risk register.

B. Executive Senior Leadership

i. Participate in the Cybersecurity Risk Management program, including identification of assets and services, allocation of resources, risk prioritization, risk acceptance, and implementation of risk treatment plan.

ii. Consider and jointly accept residual risk and Cybersecurity policy exceptions with the LC State Director of Information Technology where the assessed risk level is medium or high.

C. Administrative and Faculty and Staff

i. Collaborate with the cybersecurity engineer and the director of Information Technology to complete cybersecurity risk assessments.

ii. Develop and implement a risk treatment plan.

iii. Report updates on the risk treatment plan to the DIT or designate.

iv. Submit exceptions to the Cybersecurity Policy and work with LC State Cybersecurity through the exceptions process.

D. Cybersecurity Governance, Risk Management and Compliance (GRC) Team

i. Schedule and prioritize cybersecurity risk assessments.

ii. Request from administrative and collegiate faculty and staff information related to their collection and use of private data

iii. Conduct cybersecurity risk assessments.

iv. Process and follow up on requested exceptions to the cybersecurity policy

5. Procedures

A. This policy establishes the scope, objectives, and procedures of LC State's cybersecurity risk management process. The Cybersecurity risk management process is intended to support and protect the organization and its ability to fulfill its mission. Cybersecurity risk analysis and risk management are recognized as important components of LC States' compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the evaluation standards set forth in the HIPAA Security Rule, 45 CFR 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(1)(i), and 164.308(a)(8), the Privacy Rule (16 C.F.R. Part 313) and are in compliance with the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) as well as PCI Data Security Standard version 3.2.1 (PCI DSS).

B. Risk assessments are done throughout IT system life cycles:

i. Before the purchase or integration of new technologies and before changes are made to physical safeguards;

ii. While integrating technology and making physical security changes; and

iii. While sustaining and monitoring appropriate security controls.

C. LC State performs periodic technical and non-technical assessments of the security rule requirements as well as assessments in response to environmental or operational changes affecting the security of ePHI, financial NPI, protected cardholder data, and student education records.

D. LC State implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

   i. ensure the confidentiality, integrity, and availability of all ePHI, financial NPI, protected cardholder data, and student education records the organization creates, receives, maintains, and transmits

   ii. protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, financial NPI, protected cardholder data, and student education records

   iii. protect against any reasonably anticipated uses or disclosures of ePHI, financial NPI, protected cardholder data, and student education records that are not permitted or required

   iv. ensure compliance by the workforce

E. Any risk remaining (residual) after other risk controls have been applied requires approval by Executive Senior Leadership and will be recorded by LC State's Cybersecurity GRC Team. Information Technology Services management will be designated as additional approvers of residual risk associated with their respective areas.

F. All Cybersecurity risk management efforts, including decisions made on what controls to put in place as well as those not put into place, are documented, and the documentation is maintained for seven (7) years.

6. Responsibility

A. The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of LC State's Director of Information Technology and the Cybersecurity GRC Team.

B. For software and hardware security risk assessments, the entity or department who owns the technology in use is responsible for collecting and submitting information for security review.

C. Evaluation information from vendors must be submitted by the requesting department to the Cybersecurity Engineer to begin the vendor security review process. A Security Review of the vendor will determine any additional information that will be required.

7. Risk Assessment

The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

A. System Characterization

   i. The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI, financial NPI, protected cardholder data, and student education records are created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Consider policies, laws, the remote workforce and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media).

   ii. Output – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundaries. Endpoints and data are discovered and inventoried.

B. Threat Identification
   i. Potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. Consider all potential threat-sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats.
   ii. Output – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.

C. Vulnerability Identification
   i. Develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network.
   ii. Output – A list of the vulnerabilities (observations) that could be exploited by the potential threat-sources.

D. Control Analysis
   i. Document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a threat source exploiting a system vulnerability.
   ii. Output – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exploited and reduce the impact of such an adverse event.

E. Likelihood Determination
   i. Determine the overall likelihood rating that indicates the probability that a threat-source could exploit a vulnerability given the existing or planned security controls.
   ii. Output – Quantitative ranking of likelihood.

F. Impact Analysis
   i. Determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance of the organization's mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.
   ii. Output –Documented description of impact.

G. Risk Determination
   i. Establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management must take for each risk level.
   ii. Output – Quantitative ranking of Risk.

H. Control Recommendations
   i. Identify controls that could reduce or eliminate the identified risks, as appropriate to the organization's operations, to an acceptable level. Factors to consider when developing

controls may include the effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, cost, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

ii. Output – Recommendation of control(s) and alternative solutions to mitigate risk.

I. Results Documentation

i. Document results in an official report or briefing and provided to senior management to make decisions on policy, procedure, budget, and system operational and management changes.

ii. Output – The risk register is the source of record for risk management activities at LC State.

8. Risk Mitigation

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity, and availability of ePHI, financial NPI, protected cardholder data, and student education records. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

A. Prioritize Actions

i. Using results from the Risk Determination of the Risk Assessment, sort the threat and vulnerability pairs according to their risk levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources.

ii. Output – Actions ranked from high to low

B. Evaluate Recommended Control Options

i. Review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a "most appropriate" control option for each threat and vulnerability pair.

ii. Output – list of feasible controls

C. Conduct Cost-Benefit Analysis

i. Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.

ii. Output – Documented cost-benefit analysis of either implementing or not implementing each specific control

D. Select Control(s)

i. Considering the information and results from previous steps, LC State's mission, and other important criteria. The Cybersecurity GRC Team, in cooperation with senior leadership including but not limited to the Director of Information Technology, determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity,

and availability of ePHI, financial NPI, protected cardholder data, and student education records. These controls may consist of a mix of administrative, physical, and technical safeguards.

ii. Output – Selected control(s)

E. Assign Responsibility

i. Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step and assign their responsibilities. Also, identify the equipment, training, and other resources needed for the successful implementation of controls.

ii. Resources may include time, money, equipment, etc.

iii. Output – List of resources, responsible persons, and their assignments

F. Develop Plan of Action and Milestone (POA&M)

i. Develop an overall implementation program and individual project plans needed to implement the safeguards and controls identified. The POA&M should contain the following information as appropriate:

a) Each risk or vulnerability/threat pair and risk level

b) Prioritized actions

c) The recommended feasible control(s) for each identified risk

d) Required resources for implementation of selected controls

e) Team member responsible for the implementation of each control

f) Start date for implementation

g) Target date for completion of implementation

h) Requirements

ii. The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals' time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators, will be reported to the LC State's executive management/leadership team (e.g. the Board, senior management, and other key stakeholders).

iii. Individual project plans for safeguard implementation may be developed and contain detailed steps that resources assigned carry out to meet implementation timeframes and expectations (often referred to as a work breakdown structure). Additionally, consider including items in individual project plans such as a project scope, a list of deliverables, key assumptions, objectives, task completion dates, and project requirements.

iv. Output – Project Plans for selected safeguards

9. Implement Selected Controls

A. As controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations. Elimination of all risks is not practical. Depending on individual situations, implemented controls may lower a risk level but will not completely eliminate the risk. Continually and consistently communicate expectations to Cybersecurity GRC

Team members, senior management, and other key people throughout the risk mitigation process. Identify when new risks are identified and when controls lower or offset risk rather than eliminate it.

B. Additional monitoring is especially crucial during major environmental changes, organizational or process changes, or major facility changes. If risk reduction expectations are not met, then repeat all or a part of the Cybersecurity risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

C. Output – Residual Risk

10. Cybersecurity Risk Management Schedule

The two principal components of the Cybersecurity risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and continuous improvement of LC State's Cybersecurity program:

A. Scheduled Basis – an overall risk assessment of LC State's information system infrastructure will be conducted at least annually. The assessment process should be completed promptly so that risk mitigation strategies can be determined and included in the corporate budgeting process. The Cybersecurity GRC Team must communicate and collaborate with LC State Risk Management coordinator at least annually.

B. Throughout a System's Development Life Cycle – from the time that a need for a new information system is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.

C. As Needed – the cybersecurity engineer (or other designated employee) or Cybersecurity GRC Team may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect LC State's information systems.

11. Authority

A. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

B. Health Insurance Portability and Accountability Act of 1996 ("HIPAA")

C. Privacy and Security regulations:

i. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, as amended (including the Breach Notification Rule)

ii. PCI Data Security Standard version 3.2.1 (PCI DSS)

iii. GLBA Privacy Rule (16 C.F.R. Part 313)

12. Additional Information

Questions, requests for assistance, or other issues regarding this policy should be directed to the Director of Information Technology.