SECTION: 1.0 GENERAL

SUBJECT: DATA GOVERNANCE

Title: Data Governance Policy

Background: This policy is written to establish the authority and responsibilities of the Data Governance Council, and the Data Working Group, and to ensure Lewis-Clark State College (LC State) employees, students, contractors, consultants, affiliates, and vendors act ethically and responsibly with respect to data.

Point of Contact: Office of the Vice President for Institutional Research, Planning & Effectiveness, and Information Technology Department

Other LC State offices directly involved with the implementation of this policy, or significantly affected by the policy: LC State president and vice presidents

Date of approval by LC State authority: August xx, 2024

Date of State Board Approval: N/A

Date of Most Recent Review: August xx, 2024

Summary of Major Changes incorporated in this revision to the policy: New policy

1. Policy

LC State is committed to protecting the access, use, quality, security, and retention of all college data. Data are a valuable institutional asset and must be maintained and protected for the purpose of carrying out institutional business. The college has established the Data Governance Council and the Data Working Group to establish governing operating standards, policies, procedures, practices, and ethical use standards, representing the broad interests of the college as a whole. The Data Governance Council reports to the college president.

2. Philosophy

All data is LC State data and is an institutional asset vital to the success of the mission of the college. Therefore, structured efforts must be undertaken to protect, enhance, and leverage LC State data assets.

3. Definitions

A. Data Governance

Formalizes behavior around how data are defined, produced, used, stored, and destroyed to enable and enhance organizational effectiveness.

B. Data Governance Council (DGC)

the managing authority for the establishment of college operating standards, policies, and values to promote and guide effective and responsible data governance.

C. Data Quality

Refers to the planning, implementation, and control of activities that apply quality management techniques to data, in order to assure they are reliable, valid, fit for consumption and meets the needs of data consumers.

D. Data Standards

Reflect the operational use and application of different types of college data and definitions for various purposes.

E. Data Working Group (DWG)

Provides expert functional area knowledge and expertise to enable all college departments and divisions to collaborate in data stewardship and governance.

F. Institutional Data

Includes all items of information that are collected, maintained, and utilized by the college for the purpose of carrying out institutional business. This includes data that are aggregated into metrics relevant to operations, planning, or management of any unit at LC State. Note that research data independently collected by faculty for research may not fall within the scope of Institutional Data.

4. Data Governance Council (DGC)

A. The DGC serves as the executive governing body and is led by the vice president for Institutional Research, Effectiveness, and Planning on issues about data governance throughout Lewis-Clark State College.

B. The DGC meets quarterly. Additional meetings may be scheduled if proposals require discussion before the next scheduled meeting. The DGC is chaired by the vice president for Institutional Research, Effectiveness, and Planning and is further comprised of the provost/vice president for Academic Affairs, senior vice president/vice president for Student Affairs, vice president for Finance and Administration, and the director of Information Technology.

5. Data Working Group (DWG)

A. The DWG is comprised of standing representatives from the offices of information technology and institutional research. The DWG is a a task force that is convened as needed, therefore additional representatives from other college functional areas may be included when the topic of data governance relates to their business function, expertise, and/or are critical stakeholders in those data integrity. Examples include the offices of the:

i. Registrar when topic of data governance is related to student records.

ii. Finance and Administration when topic of data governance is related financial or facilities information.

iii. Human Resource Services when topic of data governance is related to personnel records.

B. Discusses solutions and recommends policies and procedures regarding the stewardship of LC State data. The DWG may form subcommittees for focus areas (e.g., Data Integrity and Data Access & Security) and create temporary workgroups to address individual data issues.

C. The DGC makes appointments to the DWG based on nominations from the functional areas represented on the DWG; the DGC may appoint additional members to the DWG as needed. The associate director of Institutional Research will serve as DWG chair, and the DGC may appoint a co-chair if deemed appropriate. The DWG will be scheduled to meet when necessary to address critical issues or define potential solutions for timely issues.

6. The DGC and the DWG will coordinate to accomplish the following

A. Data Access

i. Adopt, communicate, and oversee the implementation of college-wide standards for data administration and business processes around permissions for internal and external access to data.

ii. Ensure data are available to support LC State initiatives, projects, and services that benefit the college as a whole.

iii. Establish and/or endorse processes and guidelines for responding to internal and external requests for data (e.g., the data entry and collection process and responsibilities for fulfilling institutional requests).

iv. Endorse and/or approve authorities of record for data sources.

B. Data Use

i. Create a "common data culture" in which data are centralized, stored securely, and ensure that data are used with cross-institutional understandings of the meanings and uses of key data elements.

ii. Enhance data-driven decision-making through improved access to reliable, valid, and well-documented data elements allowing better decision-making and planning.

iii. Draft and recommend policies or enhance existing policies to help safeguard college data.

iv. All protected data must be saved to encrypted files. Any protected data stored on removable media, the media title must also be encrypted.

v. Develop, document, and publish data standards for core reports and college metrics.

C. Data Quality

i. Enable increased data interoperability by establishing standards for data collection, storage, and data use (e.g., reporting), including common data definitions, data dictionaries, and naming conventions.

ii. Promote data quality standards (validity and timeliness) and address issues that threaten data quality.

D. Data and Record Retention

Promote best practices and support existing college policy in record retention.

7. Authority

A. GLBA Requirements for Higher Education

B. LC State Policy 1.211 Control and Access of SSNs

C. LC State Policy 1.212 Cybersecurity and Information Technology Risk Management

D. LC State Policy 4.103 Records Retention

8. Additional Information

Questions, requests for assistance or other issues regarding this policy should be directed to the Vice President for Institutional Research, Planning & Effectiveness or the Director of Information Technology

SECTION: 1.0 GENERAL

SUBJECT: SOCIAL SECURITY NUMBERS AND PERSONALLY IDENTIFIABLE INFORMATION

Title: Collection, Use, and Protection of Social Security Numbers and Protected Personally Identifiable Information

Point of Contact: Information Technology Director and Institutional Research, Planning & Effectiveness Vice President at Lewis-Clark State College (LC State)

Other LC State offices directly involved with the implementation of this policy, or significantly affected by the policy: Registrar, Student Records, Enrollment Services, Financial Aid, Human Resource Services, Payroll

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

1. Background

Cybercrime has greatly increased during the past five years, with over 1,800 data breaches reported in 2022 alone. To prevent identity theft through unauthorized access or use of an individual's Social Security Number (SSN) or protected Personally Identifiable Information (PII), and to comply with federal and state law, a policy is needed to guide LC State on the acquisition, storage, and access of this information. In addition to federal law, Idaho state law mandates reporting to state agencies and to the individuals affected, whenever a SSN is disclosed in a manner not in compliance with law. Idaho law places specific restrictions on how an individual's SSN and PII may be acquired, used, stored, and communicated.

2. Philosophy

The reasons for the creation of this policy are to create an active, thoughtful, and planned environment that will actively decrease the likelihood and impact of identity theft through unauthorized use and improper access and storage of an individual's SSN and/or PII. Further, the policy is required to ensure compliance with appropriate federal and state laws. Federal and state laws mandate reporting to appropriate agencies and to the individuals affected, whenever a SSN is disclosed in a manner not in compliance with law. Idaho law places specific restrictions on how an individual's SSN and PII may be acquired, used, stored and communicated.

3. Definitions

A. Personal Identifying Information (PII) refers to:

i. an individual's social security number (protected)

ii. student education records protected by FERPA (protected)

iii. home address or telephone number (private)

iv. personal electronic mail address (private)

v. passwords (protected, should NOT be shared)

vi. parent's surname prior to marriage (protected)

vii. drivers' license number or state ID number (protected)

viii. credit or debit card number, or bank account number (protected)

B. Private

Refers to information that is sensitive or otherwise in need of confidential treatment and only to be accessed by those who have a legitimate business need. Common sense and good practice dictate that this information remains accessible on a need-to-know basis by employees and sometimes by students, but never accessible by individuals outside LC State except with signed confidentiality agreements.

C. Protected

Refers to information that must be stored, used, and disclosed to others only on a need-to-know basis to permit the individual faculty or staff member to perform their LC State functions for which the information was acquired and for which it is maintained. Access to legally restricted information must be carefully safeguarded.

D. Social Security Number

Means an individual's full SSN or any significant part of it (e.g., last four digits).

4. Policy

A. LC State will collect and record SSNs and PII only as necessary to comply with requirements of law, to support student admission, enrollment and goal completion, or to carry on necessary LC State functions.

B. Where a unique identification number is required for a purpose not based in law, contract or student success, LC State will use a number other than SSN or, if there is no current reasonably feasible alternative, will maintain SSN in a secure environment.

C. LC State will protect the confidentiality of the SSN and other protected information that it holds and permit access to them only for legitimate purposes. LC State will not communicate a student or employee's PII to the general public.

5. Restrictions and Permissions on Use of Protected PII

No LC State employee who receives, accesses, or records a SSN may:

A. solicit, record, or communicate the SSN of any individual, except as permitted by this policy or as authorized in writing by the director of Information Technology or an LC State vice president or president.

B. disclose it, except as required by law, permitted by this policy, or authorized by the director of Information Technology or an LC State vice president or president.

C. intentionally communicate, post, display, or otherwise make available an SSN or PII to a member of the public.

D. create a card, tag, or identification badge, including a time card, on which an SSN appears that is required for an individual to access products, services, or benefits provided by LC State.

E. ask an individual to submit his or her SSN over the Internet unless it is encrypted, or the connection is otherwise deemed secure by senior IT staff.

F. create a website that asks an individual to use their SSN to access the site, unless an authorized need for the data exists, and a secure password or unique personal identification number or other authentication device is also required to gain access.

G. communicate SSN and/or PII to any non-LC State person unless required by law, or there is a legally binding agreement in place that obligates the non-LC State person to protect the confidentiality, use, and disclosure of the SSN and/or PII. Contact the vice president for Institutional Research and Effectiveness for appropriate contractual language.

H. cause a SSN to be printed on any material that is mailed, unless state or federal law requires the SSN to be on the document mailed, except as part of an application or enrollment process, or to establish, amend, or terminate an account, contract or policy, or to confirm the accuracy of the SSN. Whenever the SSN may be mailed under this policy, it must not be printed on a postcard or other mailer, not requiring an envelope, or visible on the envelope or without the envelope having been opened.

I. use SSN as an identifier on forms, lists, databases, or systems unless the use of SSN is necessary to perform a legitimate LC State business function and the director of Information Technology or an LC State vice president or president has determined that there is no reasonable alternative.

J. communicate SSN by e-mail or other electronic means unless it is encrypted or otherwise adequately secured. Contact the director of Information Technology or the vice president for Institutional Research and Effectiveness for advice and assistance.

6. Secure Storage of Protected PII

A. SSN information in electronic form must be stored securely on LC State-owned equipment, including encryption at rest and in-transit. SSN should not be stored on desktop, laptop or other portable devices or media. If SSN is not stored on central servers, it must be encrypted or otherwise secured. Contact the director of Information Technology or the vice president for Institutional Research and Effectiveness for advice and assistance.

B. SSN information in paper form must be stored in locked or otherwise secured areas when not in active use.

C. If the director of Information Technology or the vice president for Institutional Research and Effectiveness determines that an existing practice of storing or communicating SSN and/or PII violates this policy and is not approved, the data custodian must secure or dispose of the SSN and/or PII record within a time period as specified. If the data custodian disagrees with the determination, the individual may appeal to the president or their designee, whose decision will be final.

D. The director of Information Technology or the vice president for Institutional Research and Effectiveness may require additional controls be implemented when approving an existing practice of storing or communicating SSN and/or PII.

E. Possession by LC State persons of records containing SSN that have not been reported to the director of Information Technology or the vice president for Institutional Research and Effectiveness will be considered a violation of this policy and subject to sanctions.

7. Sanctions

Violations of this policy can result in disciplinary action up to and including separation from LC State and/or exclusion from LC State programs and facilities. Violations of Idaho law can lead to fines and injunctions, as well as personal liability.

8. Reporting Unauthorized Disclosure of SSN and PII

A. Prompt reporting of unauthorized disclosure of SSNs and PII is essential for LC State to meet its obligations under law, regulation, and contract. LC State will not take disciplinary action against any person solely because of his or her good faith reporting of a disclosure. Individuals who report violations of this policy will be protected from retaliation resulting from providing information.

B. Immediately report any suspected unauthorized disclosure of or access to SSN and/or PII or material containing SSN and/or PII to the director of Information Technology or the vice president for Institutional Research and Effectiveness. Contacts also can provide more information about the meaning and operation of the policy.

9. Authority

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

B. Gramm-Leach-Bliley Act (GLBA) Compliance – (Federal Regulation 16 C.F.R. Part 314)

C. Health Insurance Portability and Accountability Act (HIPAA) – 45 CFR 164.502

D. The Sarbanes-Oxley Act (Sarbanes-Oxley) – Public Law 107-204

E. Payment Card Industry – Data Security Standard, Version 4.0 (PCI-DSS) – standards found here

F. National Institute of Standards and Technology (NIST) 800-171 Rev. 2 – standards found here

G. Federal Protection of Human Subjects – 45 CFR Part 46 Subparts A-E

H. Idaho Code § 28-51-105

I. Federal Regulation on Controlled Unclassified Information (CUI) – 32 CFR Part 2002

J. Idaho Public Records Act – Idaho Code Title 74, Chapter 1

K. Lewis-Clark State College Policy 1.202 Appropriate Use of Technology

L. Lewis-Clark State College Policy 1.206 Data Governance Policy

10. Additional Information

A. The restrictions described in this policy do not apply to an individual's treatment of their own SSN and PII.

B. Questions, requests for assistance, or other issues regarding this policy should be directed to the director of Information Technology or the vice president of Institutional Research and Effectiveness.

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.

Title: Lost or Stolen Information Technology Equipment Policy

Background: All college-owned computing devices store various forms of Lewis-Clark State College (LC State) information. Some of that information may be considered protected or confidential based on various Federal or State laws, State Board of Education policies, or college policies, rules, or guidelines. Should the devices become lost or stolen, the college may be required to report the data contained on the device as lost which may comprise a breach.

Point of Contact: Director of Information Technology and LC State Risk Manager

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

Date of approval by LC State authority: August xx, 2024

Date of State Board Approval: NA

Date of Most Recent Review: August xx, 2024

Summary of Major Changes incorporated in this revision to the policy: New Policy

1. Philosophy

A. Loss or theft of a device owned by LC State, regardless of the information stored on the device, creates a risk to college systems. A serious risk is created if the lost or stolen device contains restricted/confidential information about students, faculty, staff, alumni, donors, retirees, contractors, or others with whom LC State does business. Therefore, to protect LC State resources, systems, information, and integrity, this policy guides college employees on reporting lost and stolen equipment.

B. Devices covered under these rules and procedures include any device that is college or personally owned and contains LC State information. Information includes but is not limited to work, research, documents, or other information relating to work or services done at LC State; information relating to employees; information relating to any LC State grants or contracts; and LC State student information. Examples of devices include desktops, laptops, tablets, USB storage devices, portable hard drives, and smartphones. This process addresses a device that is lost or stolen from the campus premises, as well as from off-campus locations.

2. Definitions

A. Information

Refers to a body of knowledge or data obtained, produced, organized, shared, or managed throughout its business operations. Information may be shared or stored in a physical or electronic manner. Information is not easily replaced without funding, skill, knowledge, resources, time, or any combination of these factors. Therefore, Information is considered a critical college asset used to build knowledge and sustain and create organizational value.

B. Information Technology equipment

Includes but is not limited to all workstations, laptops, tablets, USB storage devices, portable hard drives, and smartphones.

C. Lost device

Refers to a device that has been misplaced and cannot be located, or the assigned user simply no longer knows where the device is located.

D. Protected Information

Refers to information that is to be protected from improper disclosure or inappropriate use as defined by federal or state law, State Board of Education policy, or by LC State policy requirements. Compliance Standards including but are not limited to Federal Educational Rights Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Idaho Code section § 28-51-104

E. Stolen device

Refers to a device that has been taken without permission or has been taken with permission but not returned in the agreed-upon timeline.

3. Policy

A. If the device is lost or stolen on college property:

The assigned device holder will, as soon as possible:

i. Contact the LC State Department of Public Safety at 208.792.2226 and report the equipment as lost or stolen.

ii. Contact their immediate supervisor in writing (email is the preferred method) and report the device as lost or stolen.

iii. Complete the Missing Technology Asset/Device Report Form found on the LC State Information Technology page under Faculty and Staff Resources and email the completed form to the LC State College Help Desk at helpdesk@lcsc.edu.

iv. If the device is known to be stolen or is reasonably suspected to have been stolen, file a police report with the appropriate legal authorities as directed by the LC State Department of Public Safety.

v. Help Desk staff will contact the Cybersecurity Engineer and college Risk Manager via email.

B. IT Cybersecurity Engineer with the assistance of the Assistant Director of IT will:

i. Contact the director of IT and LC State risk manager

ii. Contact the device owner to determine the type of information stored on the device.

iii. If confidential/restricted data were stored on the device, initiate the Information Security Incident Response Plan.

iv. Follow the Tracking Stolen Computers procedures (an IT internal use document) and, if applicable, Computrace tracking procedures.

v. Work with the LC State Department of Public Safety to ensure police reports are tracked and followed up on as required.

C. If Device is Lost or Stolen Off-Campus:

The device owner will, as soon as possible:

i. Contact the LC State Department of Public Safety at 208.792.2226 and report the equipment as lost or stolen.

ii. Contact local police authorities, provide details on the equipment, and request local police to contact LC State public safety regarding theft/loss.

iii. Contact their immediate supervisor in writing (email is the preferred method) and report the device as lost or stolen.

iv. Complete the Missing Technology Asset/Device Report Form found on the LC State Information Technology page under Faculty and Staff Resources and email the completed form to the LC State College Help Desk at helpdesk@lcsc.edu.

v. Help Desk staff will contact the cybersecurity engineer and college risk manager via email.

D. IT Cybersecurity Engineer with the assistance of the Assistant Director of IT will:

i. Contact the Director of IT and the College Risk Manager

ii. Contact the device owner to determine the type of information stored on the device.

iii. If confidential/restricted data were stored on the device, initiate the Information Security Incident Response Plan.

iv. Follow the Tracking Stolen Computers procedures (an IT internal use document) and, if applicable, Computrace tracking procedures.

v. Work with the LC State Department of Public Safety to ensure police reports are tracked and followed up on as required.

E. FOR ALL INSTANCES WHEN A DEVICE IS LOST OR STOLEN:

If protected information was stored on the device and the Information Incident Response Plan is enacted, the director of IT will monitor the progress of the incident as managed through the Information Security Incident Response Plan and ensure that the college executive team is fully apprised of the incident and progress made as part of the resolution.

Authority:

Idaho Code § 28-51-105 (Security Breaches)

Federal Educational Rights Privacy Act (FERPA)

Gramm-Leach-Bliley Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

Idaho Code section § 28-51-104 (Identity Theft)

Title: Information Technology Change Management Procedure

Background: System and program changes are required to ensure the enterprise resource systems are updated, secure, and aligned to data and process needs. This policy is established to protect Lewis-Clark State College (LC State) data, provide reliable enterprise tools, and reduce the risk of data integrity, data loss, or loss of service information productivity through negligence or intentional harm.

Point of Contact: Director of Information Technology / Chief Technology Officer

Other LC State offices directly involved with the implementation of this policy, or significantly affected by the policy: Office of the President, Vice President for Finance and Administration, Vice President for Academic Affairs, Vice President for Student Affairs, Vice President for Institutional Research and Effectiveness

Date of approval by LC State authority: August xx, 2024

Date of State Board Approval: N/A

Date of Most Recent Review: August xx, 2024

Summary of Major Changes incorporated in this revision to the policy: This is a new policy.

1. Philosophy

Formal Information Technology (IT) Change Management prevents unintended or malicious consequences introduced through system changes and ensures that all changes or alterations to systems are implemented according to an approved framework or model.

2. Definitions

A. Information Technology Change Management

IT Change Management seeks to minimize the risk associated with the additions, modifications, or removal of anything that could affect IT services, including changes to the IT infrastructure, processes, documents, interfaces, etc.

B. Change

Change refers to modifying the current state of a technology-related application, process, or service, which could impact end-user functionality or pose a significant risk to college production technology systems.

Examples of changes include but are not limited to:

i. new system implementations and the launch of new applications that may store or interact with college data;

ii. application modifications or updates such as a Colleague upgrade or new system implementation;

iii. hardware modifications or updates such as data storage system upgrades;

iv. software modifications or updates such as an SIS feature update or implementation;

v. network modifications or updates such as a college firewall upgrade or implementation; and

vi. process modifications or updates such as VPN approval process updates.

Note that data entry and regularly occurring low-risk operational changes are not considered changes subject to this policy.

C. Best Practices

Best Practices refer to change management procedures generally recognized by the industry for assuring secure, reliable, scalable, and efficient system management.

i. Tier 0 Systems

Foundational systems that are the infrastructure services necessary to operate Tier 1 systems.

ii. Tier 1 Systems

Mission-critical applications used by LC State. These are required for operation.

D. Hardware, Software, and Information Systems

Technology-related assets that work together or independently to provide a service to the college

E. Production Systems

Systems critical to the operation of a specific department or the college

F. Significant Risk

A risk that poses an operational concern for a majority of the college or might impair the operation of an entire department or division

G. System Administrator

An analyst, engineer, or consultant who implements, manages, and operates a system or systems at the direction of the System Owner, Data Owner and/or Data Custodian

H. System Owner

The manager responsible for the operation and maintenance of an IT system. IT systems may have only one System Owner. The System Owner manages system risk and develops security policies and procedures to protect the system in a manner commensurate with risk; maintains compliance with State of Idaho Information Security policies and standards; maintains compliance with requirements specified by Data Owners for the handling of data processed by the system; and designates a System Administrator for the system.

3. Policy

A. Review of Changes

All planned or proposed changes to Tier 0 and Tier 1 systems must follow one of the following processes as defined.

i. Standard Changes

Standard Changes are pre-authorized for Tier 0 and 1 Systems. These are low-risk changes associated with well-documented, well-tested projects and department procedures. They are documented in a system of record appropriate to the Tier system. For example, all quarterly updates to Ellucian Colleague are to be documented in Enterprise Applications Change Accounting.

ii. Emergency Changes

Changes for Tier 0 and 1 Systems, that must be implemented immediately or within less than five (5) business days, specifically to resolve a major incident or mitigate a critical security vulnerability. These must be approved by a manager or director from IT leadership, normally the individual responsible for maintaining the affected Tier 0 or 1 System.

iii. Normal Changes

The IT Management team reviews, calendars, and discusses all other changes that are not Standard or Emergency Changes.

iv. Blackout Periods

IT leadership will define blackout periods at the first of the semester, in which all standard and normal changes will follow the emergency change process and must be reviewed and approved by two members of the IT leadership team.

v. Separation of Duties

LC State will maintain a separation of duties and responsibilities. This will be enforced by user and group rights management within the given enterprise system. Group rights will be reviewed by managers twice per year.

vi. Best Practices

Managers of LC State IT services must seek and adopt, whenever possible, Best Practices with regard to change management. The IT Managers Team will review and adopt appropriate standards and procedures representing Best Practices for calendaring, documenting, and testing normal changes.

vii. Responsibilities

The Director of Information Technology / Chief Technology Officer is responsible for administering this policy, including its maintenance and compliance. The IT Management Team consists of all managers within IT and the cybersecurity engineer. In addition, the IT Administrative Assistant or IT Project Coordinator will document the Change Management meetings and requests. Appropriate notification is to be made in a timely manner (prior to the change) for disruptive changes, emergency changes, and any high-risk changes that has a high likelihood to disrupt services.

viii. Exceptions to Policy

A request for exception, along with a risk assessment and management plan, must be submitted for review by the Director of Information Technology / Chief Technology Officer. Non-compliance with these standards may result in revocation of access, notification to the supervisor, and reporting to the individual's manager, Human Resources, or Internal Audit.

ix. Enforcement

Failure to comply with this policy may result in suspending the individual's access to network resources until policy standards have been met.

4. Authority

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

5. Change Management Procedures

Purpose

A. Document the change management procedures used for enterprise systems at LC State

The purpose is to specify the details as referred to by the following policies:

- Policy 1.206 Vulnerability Assessment and Management
- Policy 1.214 Information Technology Change Management Procedures

B. Enterprise systems are governed by a variety of change control methodologies to authorize changes, coordinate change timelines to avoid conflict, and to support a successful implementation change.

6. Standards

A. Changes to our Tier 1 enterprise systems (services that are critical to the function of the college and directly impact the ability to teach and learn) are presented and discussed at the Change Management Team Meeting.

i. This meeting is facilitated by the Assistant Director of Information Technology.

ii. Items are documented on the change calendar.

iii. Items may be discussed and approved out of band through email to the entire team.

B. Technical changes to our Tier 0 systems (services that are required to be running so that other systems can function) need approval from their directors and may have additional reviews for approvals.

One example of additional checks are changes to the network firewall.

i. Requests are made to the cybersecurity engineer who reviews and documents the technical details.

ii. The IT leadership team reviews and approves the change before the network implements it.

iii. Afterwards the change is reviewed by cybersecurity for correctness.

C. A higher level of scrutiny happens the week before and the week of the fall and spring semester.

D. In addition to the change management listed above, specific directors will be assigned to review changes to ensure proper communication and stability have been established before a change in our busiest times.

7. Non-Compliance and Exceptions

A. A Request for exception, along with a plan for risk assessment and management, may be submitted at to the Help Desk at helpdesk@lcsc.edu.

B. Non-compliance with these standards may result in revocation of access, notification of supervisors, and reporting to the Executive Management Team.

Title: One Computer Policy

Background: Computers are essential to fulfill Lewis-Clark State College's (LC State's) mission. Managing and maintaining these computers requires financial and personnel resources.

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:

Date of approval by LCSC authority: August xx, 2024

Date of State Board Approval: N/A

Date of Most Recent Review: August xx, 2024

Summary of Major Changes incorporated in this revision to the policy: This is a new policy.

1. Philosophy

Providing a dedicated computer for each employee of LC State is designed to maximize productivity. This approach emphasizes fiscal responsibility while ensuring data security, consistency of operations, and accommodating flexible work arrangements. By providing the proper hardware and software, LC State will foster a sustainable, supportable, and secure work environment while aligning with the needs and roles of employees.

2. Definitions

Computer: Computers in this policy refer to workstations, desktops, and laptops (notebooks and two-in-one devices).

Computer lifecycle: This refers to the entire usable life a computer system from its initial acquisition and deployment to its eventual retirement and disposal. A computer is required to be retired when it has reached the Original Equipment Manufacturer (OEM) declared end-of-life.

Docking Station: A docking station refers to an external device that allows a laptop computer to be connected to monitor(s) and external devices through a single cable or connection point.

End-of-Life (EOL): This is the point at which a computer will no longer receive system security and operational support or updates and will be replaced. For desktops and laptops purchased and supported by LC State, this is defined as seventy-two (72) months after date of purchase. On rare occasions, as ordered by the OEM, this time limit may be shortened to sixty (60) months.

NOTE: Tablet devices, including Apple iPads, Samsung Galaxy Tablets, Amazon Fire or Kindle, or reMarkable Tablets are not covered by this policy.

3. Policy

A. Acquisition of a Computer

The computer purchase will be decided in consultation between IT and the department supervisor. When mobility may be required, a laptop with a docking station will be issued for the employee's use. In some cases, two docking stations may be issued to an individual employee to allow for a productive work environment across two assigned areas.

B. Replacing a Computer

Employees requesting a new or different computer will return their original computer to the IT department. All computers returned to IT will be evaluated to see if they have reached End of

Life. If the device has remaining life, it may be reallocated in consultation between IT and the Purchasing Department.

C. Exceptions

Vice presidents or the president with agreement of the IT director, may grant exceptions to this policy if they agree it is an appropriate resource allocation. Criteria to be considered in this evaluation include, but are not limited to the following:

- age of the computer and anticipated maintenance of older hardware,
- ability of designated equipment to complete the work tasks required,
- specialized need to retain older hardware to support expensive or critical equipment,
- whether an upgrade can fulfill the projected need for a new computer, and
- increased security vulnerabilities of operating older hardware/software.

NOTE: This policy does not prevent the purchase of a computer using grant funds (if the computer was specifically listed among the expenditures when the grant was approved) and funding provided to faculty or staff pursuant to the signed agreement.

4. Authority

Idaho Technology Authority (ITA)is authorized by Idaho statute, Title 67, Chapter 57.1

ITA's directives are relevant to Lewis-Clark State College because of the definition included in the statute.

Description of ITA: (https://ita.idaho.gov/the-ita/)

List of ITA policies: (https://ita.idaho.gov/resources/)

ITA Policy P1060 – Employee State-Issued IT Device

5. Questions

Requests or questions related to this policy should be directed to the director of Information Technology.