SECTION: 1.0 GENERAL

SUBJECT: SOCIAL SECURITY NUMBERS AND PERSONALLY IDENTIFIABLE INFORMATION

**Title:** Collection and Use of Protected and 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, and Payroll

**Date of approval by LC State authority**: March 2025

**Date of State Board Approval**: N/A

**Date of Most Recent Review:** New

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

**1. Background**

**2.** . The purpose of the policy is to aid in preventing 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, and a policy is needed to guide LC State on the acquisition, storage, and access of this information. In addition to federal law, Idaho Code § 28-51-105 mandates reporting to state agencies and to the individuals affected, whenever a SSN is disclosed in a manner not in compliance with law.

**3. 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, other protected information, and/or PII. Further, the policy is required to ensure compliance with appropriate federal and state laws (outlined in the Authority section).

**4. Definitions**

A. Personally Identifying Information (PII) is information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means (U.S. Department of Labor). Examples of PII include:
   i. an individual's social security number
   ii. student education records protected by FERPA
   iii. home address or telephone number
   iv. personal electronic mail address
   v. passwords
   vi. parent's surname prior to marriage
   vii. drivers' license number or state ID number
   viii. credit or debit card number, or bank account number

B. 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 while mitigating risks

associated with sharing and using these data. More information on specific types of protected data, specific security risks and requirements for handling these data can be found in the LC State Data Security and Appropriate Use Guidelines.

C. Social Security Number

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

**5. Policy**

A. LC State will collect and record SSNs, PII, and protected information 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, unless considered public information or directory information (for student records) as defined by LC State under the Family Educational Rights and Privacy Act (FERPA) and the student has not successfully submitted a Directory Information Restriction Request Form to the LC State Office of the Registrar.

**6. Restrictions and Permissions on Use of Protected information**

No LC State employee who receives, accesses, or records protected information (e.g., SSN) may:

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

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

C. 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.

D. 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.

E. communicate SSN and/or protected information 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 protected information. Contact the LC State Risk Manager for appropriate contractual language.

F. 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.

G. 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 the President has determined that there is no reasonable alternative.
H. 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 LC State Risk Manager for advice and assistance.

**7. Secure Storage of Protected Information**

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 LC State Risk Manager 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.

**8. 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.

**9. Reporting Unauthorized Disclosure of SSN and Protected Information**

A. Prompt reporting of unauthorized disclosure of SSNs and protected information 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 protected information or material containing SSN and/or protected information to the Director of Information Technology or the Vice President for Institutional Research, Planning and Effectiveness.

**10. Authority**

A. Family Educational Rights and Privacy Act (FERPA) – (20 U.S.C. § 1232g)
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

**11. Additional Information**

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