SECTION #: 1.0 General

SUBJECT: Data Security & Classification

Title: Data Security & Classification

Point of Contact: Institutional Research, Planning & Effectiveness Vice President and Information Technology Director at LC State

Other LC State offices directly involved with implementation of this policy, or significantly affected by the policy: Institutional Research, Information Technology Services, Registrar, Student Records, Financial Aid, Human Resource Services, and Finance & Administration

Date of approval by LC State authority: May, 2026

Date of State Board Approval: N/A

Date of Most Recent Review: New Policy

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

---

1. **Purpose & Scope**
   - A. Purpose
     - i. LC State is committed to protecting the security, integrity, and proper use of institutional data. This policy establishes requirements for classifying, handling, and protecting institutional information to maintain secure operations, protect sensitive information, and ensure regulatory compliance.
   - B. Scope.
     - i. This policy applies to all members of the LC State community, including faculty, staff, students, contractors, consultants, and temporary employees who access, use, or maintain institutional data.
2. **Data Classification**

   LC State classifies institutional data into four security levels based on sensitivity and potential impact of unauthorized disclosure:
   - C. Restricted Data:
     - i. The most sensitive classification requiring the strictest security measures. Includes data protected by laws, regulations, or institutional policies where unauthorized access could result in legal liability, financial penalties, or significant harm.
   - D. Confidential Data:
     - i. Personally identifiable information (PII) or proprietary institutional data that LC State is legally, contractually, or ethically obligated to protect. Access is restricted to personnel with legitimate business need.
   - E. Internal Data:
     - i. Information essential for conducting institutional business that is not intended for public distribution. Requires protection due to proprietary, ethical, or privacy concerns.
   - F. Public Data:

i. Information approved for unrestricted distribution that does not require confidentiality protections.

3. Data Reclassification

Institutional data classifications are not permanent and must be reviewed and updated as the sensitivity, regulatory status, or operational context of data changes over time.

A. Triggering Events: Data Owners must initiate a reclassification review when any of the following occur:
   i. A change in applicable law, regulation, or contractual obligation affecting the data.
   ii. A change in the data's intended use or audience (e.g., internal data approved for public release).
   iii. Expiration of a confidentiality period (e.g., a pending personnel action that has concluded).
   iv. Merger, reorganization, or transfer of institutional functions affecting data ownership.
   v. A security incident or audit finding that reveals a classification was inadequate.
   vi. Routine periodic review (see below).

B. Downward Reclassification Caution:
   When the decision to reclassify data is made to a lower sensitivity level (e.g., from Restricted to Confidential), all existing copies, backups, and derivative datasets need to be identified and are subject to the updated controls. Reclassification does not retroactively authorize prior access that was not permitted under the original classification.

4. General Principles

All users must adhere to the following principles when handling institutional data:

A. **Highest Sensitivity Rule**: When handling combined datasets, apply the requirements of the most sensitive data classification present.
B. **Authorization Required**: Obtain approval from appropriate supervisors or Data Owners (defined in section 7) before extracting, processing, or storing sensitive information.
C. **Appropriate Security**: Store sensitive data only in authorized locations with appropriate security controls.
D. **Need-to-Know Access**: Access only data necessary to perform assigned duties.
E. **Prompt Incident Reporting**: Immediately report suspected breaches, unauthorized access, or policy violations to Information Technology Services (ITS).

5. Security Requirements

A. Storage and Access
   i. Confidential and Restricted Data must only be stored in ITS-approved systems with appropriate security controls.
   ii. Personal devices and consumer cloud services are not approved for storing Confidential or Restricted Data.
   iii. Access to sensitive data must be limited to authorized personnel with documented business needs.

B. Encryption and Technical Controls
   i. Confidential and Restricted Data must be encrypted at rest and during transmission.
   ii. Authentication and role-based access controls are required for sensitive data.
   iii. Systems must meet institutional security standards for encryption, access control, and audit logging.

C. Physical Security
   i. Printed materials containing sensitive data must be handled according to their classification level.

ii. Confidential and Restricted materials require secure printing, locked storage, controlled transport, appropriate labeling, and secure disposal.
iii. Sensitive documents must be destroyed via cross-cut shredding, pulping, or secure destruction services in alignment with LC State's Records Retention Schedule.

6. Third-Party Data Sharing

LC State may share institutional data with external parties only under conditions that ensure appropriate protection consistent with the data's classification level and applicable regulatory requirements.

A. General Requirements
   i. All sharing of Confidential or Restricted Data with third parties requires a written data sharing agreement or contract reviewed by the appropriate compliance office prior to disclosure.
   ii. Third parties must demonstrate equivalent or greater data security controls before receiving Confidential or Restricted Data.
   iii. Data may only be shared for the specific purpose stated in the agreement and may not be further disclosed or repurposed by the receiving party without prior written approval.
B. Vendor and Contractor Access
   i. Vendors and contractors accessing LC State data must be bound by confidentiality and security obligations no less stringent than this policy.
   ii. Access must be limited to the minimum data necessary to fulfill the contracted purpose and terminated promptly upon contract conclusion.

7. Role and Responsibilities

A. Data Owners
   Senior decision-makers responsible for classification, protection, and authorized use of data under their oversight. Accountable for ensuring regulatory compliance, defining access permissions, and approving security measures.
B. Data Custodians
   Responsible for technical implementation of data security measures, including storage, management, and disposal of protected information. Ensure availability, security, and compliance for institutional use.
C. Data Stewards
   Subject matter experts responsible for business control, content quality, and proper usage of defined data assets. Ensure data definitions, standards, and quality objectives are established and maintained.
D. Authorized Personnel
   Individuals granted access to Confidential or Restricted Data based on documented business need. Must follow enhanced security requirements and use only approved systems and tools.
E. Users
   All individuals who access or utilize LC State data. Responsible for complying with security practices, protecting data and devices, and following proper storage, transmission, and disposal procedures.

8. Enforcement

Violations of this policy may result in:

A. Temporary or permanent restrictions on access to LC State systems and services
B. Disciplinary action in accordance with institutional policies, employment contracts, and applicable laws

C. Other consequences as determined appropriate by institutional leadership

9. Related Documents

A. LC State Data Use Guidelines (procedural implementation)
B. LC State Cybersecurity Incident Response Plan
C. Policy 1.211, Social Security Numbers and Personally Identifiable Information
D. Policy 1.117, The Family Educational Rights and Privacy Act (FERPA)
E. Policy 4.103, Records Retention; LC State's Records Retention Schedule
F. Applicable federal and state regulations (FERPA, HIPAA, PCI-DSS, etc.)