PURPOSE OF THIS POLICY
Colorado State University collects personal information of a sensitive nature to facilitate and enable its business and academic functions. Unauthorized access to such information may have significant negative consequences, including exposing those associated with the university to risk of identity theft, and adversely affecting the reputation of the University. In addition, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Colorado House Bill 03-1175 (the “non-SSN” legislation), Colorado House Bill 18-1128 (the consumer data privacy legislation), the Family Educational Rights and Privacy Act (FERPA), the Payment Card Industry Data Security Standard (PCIDSS), the European Union’s General Data Protection Regulation (GDPR), and other legislation regulations require various classes of information to be protected from unauthorized access, and treated with the utmost circumspection. The University Policy on IT Security addresses security measures for protecting personally identifying information sensitive data. This policy addresses access to and use of certain sensitive information personally identifying information stored in paper or electronic form.

APPLICATION OF THIS POLICY
These policies encompass best practices that are in general to be applied comprehensively at the University, including third parties accessing University information. Each unit which owns or is responsible for any electronic information record are responsible for implementing their aspects of this policy. All users who access sensitive digital personally identifying information must also conform to this policy.
DEFINITIONS USED IN THIS POLICY

*Personally Identifying Information* means a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver’s license or identification card number; a government passport number; biometric data, as defined in C.R.S. § 24-73-103(1)(a); an employer, student, or military identification number; or a financial transaction device, as defined in C.R.S. § 18-5-701(3); and all such sensitive personal information as defined below.

*Sensitive personal information* includes social security numbers, personally identifiable health information, personally identifiable financial information including credit card information, driver’s license information, personnel employment and student performance information, proprietary research and academic information, third-party proprietary information, FERPA-protected non-directory information and any other information that through disclosure would adversely affect an individual or besmirch the reputation of the University. Includes social security number information, personally identifiable health information, personally identifiable financial information including credit card information, personnel and student performance information, proprietary research and academic information, student and staff ID photos, location including IP address, and any other sensitive personal information that through disclosure may adversely affect an individual and/or the University.

*Family Educational Rights and Privacy Act (FERPA)*: Federal law protecting students’ education records from disclosure by the University to anyone other than the student without the student’s consent, unless a specific exception applies.

*RamCard*: the official student and employee identification card issued by the University, including the official digital photo, the “RamCard ID Photo.”

**POLICY STATEMENT**

It is Colorado State University's policy to collect and store the least amount of personally identifiable information required to fulfill its required duties and responsibilities, or to complete a particular transaction, or as required by law. This policy applies to the collection and storage of all personally identifiable information, regardless of the source or medium.

For website administration functions, information (other than personally identifying information linked to a particular individual) is collected for analysis and statistical purposes of website to support and facilitate navigation. This information is used to help diagnose problems, assess what information is of most interest, determine technical design specifications, identify system performance or problem areas, to maintain a connection as one browses across web pages and web services, and for other administrative functions. Similar information is also maintained on network logs, which we are required to maintain for law enforcement purposes. However, both os of, logging information of these types of information are maintained in highly secure environments, data are disposed of as
allowable under our operational and legal responsibilities, and such data are strictly protected and never shared with anyone or anything outside of CSU. Such two types of Logging information is areis not subject to this policy but is areis covered under by the IT Security Policy.

Students may choose whether or not to provide personally identifying information to Colorado State University via the Internet. If a student chooses not to provide the personally identifying information requested, the student may still visit most of Colorado State University’s websites, but may be unable to access certain options, offers, and services. In certain extreme cases, the student may not be eneablede to enroll at CSU.

The digital student identification picture, the RamCard ID photo, is considered sensitive personally identifiable information within the education record of the student. Student identification photos are provided digitally for use by course instructors and other CSU faculty and staff who have a legitimate educational purpose to view student education records. These photos are not “directory information” under the CSU FERPA policy, and may not be released to anyone without permission of the student, except in accordance with this policy. They must be secured using the same safeguards as other private and sensitive information.

Employees also have a reasonable expectation of privacy with respect to their RamCard ID photos.

**POLICY PROVISIONS**

1. **Principle of Least Privilege De Minimis Access**: The amount of sensitive personally identifying information collected and stored shall be the minimum amount required for the efficient and effective conduct of business and academic functions. Access to sensitive personally identifying information shall be limited to only those needing access for legitimate business or academic purposes, and only to the minimum amount of that which is required for business purposes. Periodically, individual access may shall be reviewed to be in conformance with this policy.

2. Units are responsible for ensuring that all of their paper, non-paper and electronic records containing sensitive personally identifying information are secured as required under the CSU IT Security Policy and protected from unauthorized access.

3. Periodically, units shall review their policies, operations, forms, archives and other associated functions to ensure they are in conformance with this policy.

4. Reasonable and prudent efforts shall be made to isolate and protect sensitive personally identifying information in physical form from unauthorized access, for example in locked filing cabinets, behind locked doors, suitable IT security measures, etc.

5. Social security numbers (SSNs) shall not be used as the primary numeric identifier for individuals. This particular policy applies to all forms of information, both electronic and non-electronic, including identification cards. See the University Policy on Social Security Numbers.

6. RamCard ID Photos:
Access to and use of official RamCard ID photos are permitted for legitimate educational and business purposes only. Access or use for personal reasons, and any unauthorized access or use, or redistribution, is not permitted.

Direct access to the University’s electronic systems that store digital ID photos must be pre-approved in writing by the Vice President for Information Technology, who shall constitute a small, ad hoc committee to review such requests. Requests must be made to the Advisory Committee for Administrative Applications (ACAdA) using the application for such access provided in Appendix A by the Information Systems Department. Considerations for approval shall include the business need for access, especially inherent benefits, a commitment to complying with these policy provisions, including the quality of the protections to be implemented to ensure IT security and privacy, and proper data disposal, and the effort involved in granting access and in implementing such protections.

Before access or use, departments are required to provide relevant employees a copy of this policy and ensure they understand these provisions to ensure protection of the privacy of students and employees.

Access and use shall be controlled via an approved login and password as specified in the CSU IT Security Policy.

Files containing digital ID photos shall not be copied or shared in any manner except as specifically authorized herein in advance.

Viewing digital photographs shall be done in a manner that is discreet, reasonably viewable only by authorized personnel.

Disposal of Records: All records containing personally identifying information held by the University, any department or unit of the University, or any person or entity acting for the University must be properly disposed of when the applicable retention period has ended and the record is no longer needed, in accordance with the CSU Policy on Records Retention. As used herein, “disposed of” includes rendering the personally identifying information in the record unreadable or indecipherable by any means whatsoever.

COMPLIANCE WITH THIS POLICY
Abuse or misuse of RamCard ID photos personally identifying information shall be reported to the Office of the Vice President for Information Technology. Violation of this policy may result in revocation of access without notice, and violators may be subject to disciplinary consequences, and/or legal action. Criminal liability can also arise for violations of applicable laws.

POLICY GOVERNANCE
The Information Technology Executive Committee (ITEC) is responsible for this policy, including initiating modifications and changes as necessary to remain current with technological and legal requirements.
REFERENCES
CSU Privacy Statement and Related Information
CSU Policy on Information Technology Security
CSU Policy on Social Security Numbers
CSU Policy on Records Retention
CSU FERPA policy

APPROVALS
Version 1.0 Approved by ITEC: July 8, 2004

Version 1.1 Approved by ITEC: July 21, 2005

Version 2.0 Approved by ITEC: May 10, 2017 (by Rick Miranda, Provost/Executive Vice President)