	Procedure Number	8.6.2P
	Effective Date	9/25/23

In accordance with IT Security Policy 8.6, the purpose of this procedure is to outline general procedures that ensure the security, integrity, and confidentiality of personally identifiable information (PII), protecting it against anticipated threats, and guarding it against unauthorized access or use. The college recognizes administrative information as a college resource requiring proper management to permit effective planning and decision-making, and to conduct business in a timely and effective manner. Employees are charged with safeguarding the integrity, accuracy, and confidentiality of this information as part of the condition of employment. To that end, Laramie County Community College takes steps to remain in compliance with regulations suCIPA

Adopted on: 9/25/23

This procedure applies to all persons including without limitation: The Board of Trustees, employees, students, guests, and all other individuals and entities affiliated with Laramie County Community College (referred to in this procedure as "users") who access or use the College's E-Resources. Laramie County Community College (LCCC) encompasses Cheyenne Campus, Laramie Campus, and Eastern Laramie County Outreach.

A. *Administrative Computer System* – Ellucian's Colleague ERP.
B. *Administrative information* – any data related to the business of the college including, but not limited to, financial, personnel, student, alumni, and physical resources. It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which they reside.
C. *Mnemonics* – Ellucian's Colleague processes for accessing data entry screens, processing, and reporting.
D. *Personally Identifiable Information (PII)* – nonpublic information relating to an individual that reasonably identifies the individual and, if compromised, could cause significant harm to that individual or to the college. Examples may include, but are not limited to, Social Security numbers, credit card numbers, bank account information, student grades or disciplinary information, salary or employee performance information, donations, patient health information, information that the college has agreed to keep confidential and account passwords or encryption keys used to protect access to confidential college data.

E. *Principle of Least Privilege* – Accounts are not given more access than is necessary to complete their job functions.

F. E-Resources – All information technology and other electronic resources of the College (referred to in this procedure as "E-Resources"), including without limitation:

1) all devices, systems, equipment, software, data, networks, and computer facilities owned, managed, or maintained by the College for the handling of data, voice, television, telephone, or related signals or information
2) any access or use of the College's electronic resources from a device or other system not controlled or maintained by the College
3) the creation, processing, communication, distribution, storage, and disposal of information under the College's control.

In addition, members of the community may have access to third-party electronic resources through their affiliation with the College. Use of these resources by members of the community is governed by this procedure and any applicable policy or restriction of the third-party provider.

G. *College Data* –

2. Creating/Removal of employee AD accounts following the Employee

b. Technical Safeguards

i. According to industry standards, the college relies on the Integrated Technology Services (ITS) department to provide network security and administrative software password access security. This protects student PII that is accessed electronically but stored outside of a department. Departmental desktop computers and other electronic devices storing student PII are protected by physical safeguards and encryption where applicable.

ii. The use of strong passwords with required password changing recommendations are outlined in the Network Password Procedure and Guidelines 8.6.1P.

iii. Appropriate use of E-Resources is outlined in the Acceptable Use Procedure 8.3P.

iv.

h.