Information Technology – Data Access Security Procedure	Procedure Number	8.6.2P
	Effective Date	9/25/23

1.0 PURPOSE

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 such as The Gramm-Leach-Bliley Act of 2000 (GLBA), The Fair and Accurate Credit Transactions Act (FACT Act), the Family Educational Rights and Privacy Act (FERPA), and on a limited basis The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and The Children's Internet Protection Act (CIPA).

2.0 REVISION HISTORY

Adopted on: 9/25/23

3.0 PERSONS AFFECTED

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.

4.0 DEFINITIONS

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* – College data are assets of the college in any form or location that meets one or more of the following criteria:

1) Data that the college has a legal obligation to responsibly manage.
2) Data that is relevant to the operations, planning, management, control, reporting, auditing, and administration of the college.
3) Data that is created, received, maintained, or transmitted as a result of the function of the college.
4) Data that is included in an official college report.
5) Data that is used to derive any data element that meets the above criteria.

H. *Cyber Security Training* – Security awareness training teaches employees to understand vulnerabilities and threats to business operations. LCCC employees need to be aware of their responsibilities and accountabilities when using a computer on a business network.

5.0 PROCEDURES

A. Gramm-Leach-Bliley and FACT Act Requirements

a. GLBA mandates that the college designate information security program representatives to coordinate the information security program, conduct a risk assessment of likely security and privacy risks, institute a training program for all employees who have access to customer information, oversee service providers and related contracts, and evaluate and adjust this program periodically. The FACT Act has similar requirements, including mandating schools to have a program to identify, detect, and respond appropriately to relevant “red flags;” this is further detailed in the Identity Theft Prevention Program Procedure 9.6P and the Privacy Protection and Information Security Procedure 9.8P.

i. LCCC provides mandatory training for all employees on a variety of IT security topics monthly.

ii. College employees are trained when they are hired and are provided training every other year thereafter in reference to the use and security of sensitive and

confidential educational records. Employees are held accountable to know and understand that they are not permitted to access personally identifiable information for unapproved purposes or to disclose it to unauthorized persons. Their access is only to perform their duties for the college. Human Resources policies articulate that violation of LCCC policies and procedures may result in disciplinary action, up to and including termination of employment.

b. GLBA further mandates that a Qualified Individual be designated to overseeing and implementing and enforcing our information security program. LCCC designates the Cyber Security Analyst for this role.

B. IT Security Members

a. Colleague Security Committee

i. The members of the Colleague Security Committee for the college include:

1. Registrar
2. Specialist, HR Information Systems
3. Director, Financial Aid
4. Assistant, Executive Admin I, Academic Affairs
5. Comptroller
6. Project and Application Support Manager

ii. The Colleague Security Committee provides recommendations for the administration and maintenance of the procedures and processes surrounding the Administrative Computer System. This includes:

1. Establishing Colleague security classes based on employee position.
2. Reviewing and assigning and/or removing Colleague mnemonics in security classes.
3. Approving, denying, or modifying Colleague access for employee's positions based on each request. Access to the administrative systems is granted based on employee need to use specific data as defined by job duties and is subject to appropriate approval. As such, this access cannot be shared, transferred or delegated. Failure to protect these resources may result in disciplinary measures being taken against the employee, up to and including termination of employment.
4. Perform a complete security review of all security classes, users, and user access every three (3) years.

b. Active Directory (AD) IT Security

i. The members of the IT Security Team for the college include:

1. Analyst, Cyber Security
2. Director, Systems & Technology Support
3. Chief Information Officer
4. Manager, Network

ii. The IT Security members provide leadership to campus-wide data security efforts and advisory support to ITS staff in these endeavors. This includes the management of the following processes:

1. Determines proper access to the computer systems for AD users. Access is provided based on the principle of least privilege.

2. Creating/Removal of employee AD accounts following the Employee Email Procedure 8.1P and the Student Email Procedure 8.5P.
3. Approves content for the mandatory IT training for all employees on a variety of security topics.
4. Conducts periodic risk assessment on various threats against the computer systems throughout the year. These include various penetration testing, network scanning, phishing tests, etc.
5. Performs assessments that may include National Institute of Standards and Technology (NIST) tests, the Federal Financial Institutions Examination Council (FFIEC) tests, or similar cybersecurity and preparedness assessments.
6. The Qualified Individual prepares an annual monitoring report to present to the LCCC Board of Trustees that includes preventive activities, risk assessment, data breaches, and future initiatives.
7. Participates in the annual LCCC Financial IT Audit.

C. Security Provisions

With respect to the safeguarding provisions of the GLBA Act, this covers all physical, technical, and administrative safeguards used in the collection, distribution, processing, protection, storage, use, transmission, handling, or disposal of customer PII.

a. Physical Safeguards

i. The college uses direct personal control or direct supervision to control access to and handling of all customer PII when an office is open. Whether the information is stored in paper form or any electronically accessible format, departmental PII is maintained, stored, transmitted, and otherwise handled under the direct personal control of an authorized employee of the college.

ii. Departmental PII is collected, processed, transmitted, distributed, and ultimately disposed of with constant attention to its privacy and security. Conversations concerning PII are held in private. Papers with PII are mailed via official campus mail, US mail, or private mail carrier. Departments are encouraged to password-protect electronic files of PII when transmitting electronically. When best practices permit the disposal of PII, it is destroyed; paper containing such information is routinely shredded. Disks containing PII are disposed of by physical destruction or mutilation.

1. Confidential material is kept secure. Most offices have locked doors with restricted access. For those that do not, materials are kept in locked filing cabinets or other locked storage areas. When offices are open, confidential information is kept out of sight from visitors, and computer screens are not visible to visitors. Offices and/or computers are locked when the office is vacant for an extended length of time.
2. Key access is limited to authorized college employees only.
3. Departmental cloud storage and information processing generally conforms to the same practices as onsite storage and is safeguarded under the provisions for outside service providers.

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. College-owned computers and servers have software updates installed on a monthly patch cycle to stay protected from security threats. Critical security patches may be applied out of band if necessary.

v. When using personal computers, laptops, and cell phones to access protected college resources, additional security requirements may be imposed to ensure the security of the device adequately protects college data.

vi. Devices storing customer PII should meet a baseline security standard of:

1. Using full disk encryption if it is a mobile device.
2. Having a compliant password.
3. Being kept up to date on software patches.
4. It has up-to-date malware protection if it is a PC or Mac.
5. It is configured to automatically lock the device to prevent unauthorized access after a period of inactivity.
6. It is not shared with people not authorized to access this information.

vii. PII should only be stored on E-Resources for as long as it is needed and should be promptly removed afterward. This may include, but is not limited to downloaded reports, received emails, exports, etc. from any system used by the college.

viii. PII that is stored on portable media, such as CDs, DVDs, USB flash drives, etc. should use encryption to protect the data in the event of loss or theft.

ix. Only ITS-provided cloud storage should be used to house college data. Use of any cloud storage service other than that which ITS has provided requires written ITS approval. See Cloud-Based Storage Supplemental Guidance.

x. ITS shall establish and maintain an incident response plan outlining actions to be taken during a cyber security incident.

c. Outside Service Providers

i. ITS shall guide the entire purchasing process of third-party software services to manage the contract details pertaining to data ownership, security, stewardship, and backup. All contracts must be reviewed by both the director of the functional area requesting the contract, Director of Contracting and Procurement and the Chief Technology Officer, or designee, prior to the College President's approval. Each area ensures that third-party service providers are

required to maintain appropriate safeguards for PII to which they have access. Contracts with service providers, who within their contracts have access to PII, shall agree to the contract provisions provided by the Director of Contracting and Procurement.

ii. ITS shall establish measures to oversee information system service providers. ITS shall determine the appropriate measures necessary to safeguard college data with regard to each provider and the data they are handling.

d. Assessment, Review, and Reporting Process

i. An assessment of data security occurs at least annually. The assessment includes the review of the procedures to create and remove administrative access to data. The annual review also includes identification and assessment of internal and external risks to the security, integrity, and confidentiality of customer PII and covered accounts, including review of outside contractors and their contracts to ensure that proper safeguards are in place. The results from each department will be included in a comprehensive review of the college. These reports are used to inform improvements to the systems and training priorities. A summary of these reports is provided to the LCCC Board of Trustees in an annual monitoring report.

ii. Regular monitoring, testing, and evaluation of the effectiveness of security safeguards will be conducted. This will either be done periodically or continuously where possible.

D. Violations

a. The College treats misuse of its various data and resources as misconduct and will address employee violations per the Employee Conduct and Discipline Policy 6.10.

b. Anyone aware of possible violations of this procedure must report them immediately to an appropriate person (e.g., his/her supervisor, the system administrator, the HR director, the Dean of Students, the Cyber Security Analyst, the CIO, the ITS Help Desk, etc.).

c. Cases of serious, deliberate criminal conduct will be referred to the appropriate external authorities and may result in civil or criminal proceedings.

E. Resources

a. The Gramm-Leach-Bliley Act of 2000 (GLBA): https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

b. The Federal Trade Commission (FTC): https://www.ftc.gov/

c. The Fair and Accurate Credit Transactions Act (FACT Act): https://www.ftc.gov/legal-library/browse/statutes/fair-accurate-credit-transactions-act-2003

d. Family Educational Rights and Privacy Act (FERPA): https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

e. Health Insurance Portability and Accountability Act of 1996 (HIPAA): https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

f. Children's Internet Protection Act (CIPA): https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

g. National Institute of Standards and Technology: https://www.nist.gov/

h. Federal Financial Institutions Examination Council (FFIEC): https://www.ffiec.gov/
i. Privacy Protection and Information Security Procedure 9.8P
j. Acceptable Use Policy 8.3 and Procedure 8.3P
k. Cloud Based Services Supplemental Guidance 8.3.1P