Information Technology – Data Protection Procedure	Procedure Number	8.6.3P
	Effective Date	

1.0 PURPOSE

In accordance with IT Security Policy 8.6, the purpose of this procedure is to outline general procedures for protecting the information and use of technology resources and facilities to support the College's educational and service missions as well as the administration and operation of the College.

2.0 REVISION HISTORY

Adopted on:

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. *Data* – stored collection of information that may include symbols, words, sounds or images.
B. *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.
C. *Personal Data* – identifiable information such as name, identification number, address, college id number, or specific details of an individual's physical, physiological, genetic, mental, economic, cultural, or social identity.
D. *Proprietary Information* – data, information, or intellectual property in which the college has an exclusive legal interest or ownership right, which, if compromised, could cause significant harm to the college. Examples may include, but are not limited to, business planning information, financial information, trade secrets, copyrighted material, research, or comparable materials from a third party that the college has agreed to keep confidential.
E. *Sensitive Information* – any information whose disclosure could cause harm to the College or its constituents including PII and proprietary information.
F. *Data integrity* – ensure the reliability and trustworthiness of data throughout its lifecycle.

G. *Private Data* – includes information gathered from users by their use or connecting to LCCC resources, including system activity, event logs, browsing history, email/voicemail content, and documentation.
H. *College Data* – College data are assets of the college in any form or location that meets one or more of the following criteria:
    a. Data that the college has a legal obligation to responsibly manage.
    b. Data that is relevant to the operations, planning, management, control, reporting, auditing, and administration of the college.
    c. Data that is created, received, maintained, or transmitted as a result of the function of the college.
    d. Data that is included in an official college report.
    e. Data that is used to derive any data element that meets the above criteria.
I. *Administrative Computer System* – Ellucian's Colleague ERP.
J. *E-Resources* – All information-technology and other electronic resources of the College (referred to in this procedure as "E-Resources"), including without limitation:
    a. 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;
    b. any access or use of the College's electronic resources from a device or other system not controlled or maintained by the College; and,
    c. the creation, processing, communication, distribution, storage, and disposal of information under the College's control.

5.0 PROCEDURES

A. Information Collected/Use of Collected Information
    a. LCCC collects data that is considered sensitive information, personal data, PII, and private data from students, employees, and other community members as necessary in the exercise of its legitimate interests, functions, and responsibilities as an institution of higher education.
    b. LCCC has data that is considered proprietary and is necessary in the exercise of its legitimate interests, functions, and responsibilities as an institution of higher education.
    c. LCCC's web server recognizes the referring domain, IP (Internet Protocol) address, operating system and browser used. That information is used for internal research. Some PII provided by website users may be used to fulfill requests to participate in our programs and activities, receive services, and to respond to requests for information and so may be used to communicate with the user. LCCC does not collect any PII about users (e.g., names, email address, etc.) unless specifically provided.
    d. Third-party service providers who have entered into contracts with the college to support its operations and policies may receive personal information of students, employees, and other community members for specific authorized purposes. Information shared with such third-party service providers will be subject to safeguards approved by LCCC to prevent unauthorized disclosure.
B. Protection and Guidelines for Collected Information

a. LCCC has implemented appropriate physical, electronic and managerial procedures to safely maintain and help prevent unauthorized access, maintain data security, and ensure proper usage of the information collected, including secure information transmission, storage, and retrieval.

b. Controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users is in place.

c. LCCC uses industry-standard security technology to guarantee the confidentiality of transactions made on our website. This technology helps protect online transaction information from access by unauthorized parties.

d. LCCC may use and disclose de-identified information without limitation. An example of this would be state-wide reporting with the Wyoming Community College Commission.

e. Users need to adhere to the Policies and Procedures listed below when collecting and using College Data:

i. Privacy, Access to, and Amendment of Student Record Procedure (3.4.2)
ii. Acceptable Use Procedure (8.3P)
iii. IT Security Policy (8.6) and Procedures
iv. Records Retention Procedure (9.5P)
v. Identity Theft Prevention Program (9.6P)
vi. Privacy Protection and Information Security Procedure (9.8P)

f. LCCC attempts to protect the information of minors and children under age 13 by adhering to the Children's Internet Protection Act (CIPA) where applicable. LCCC does not knowingly collect personal information of children under age 13 except when related to LCCC's activities or programs.

g. LCCC provides protection to students by adhering to the Family Educational Rights and Privacy Act 1974 – 'Buckley Amendment' – PL 93-380 (FERPA). LCCC provides protection to students and employees by adhering to the Health Insurance Portability and Accountability Act (HIPAA) of 1996 where applicable.

h. LCCC is committed to protecting the security and privacy of personal and sensitive information collected from individuals in the European Union (EU). The General Data Protection Regulation (EU 2016/679) (GDPR) is legislation of the EU that is intended to protect the privacy of individuals in the EU by establishing how data controllers and data processors must address the collection and processing of personal information about those individuals. This policy is applicable to the processing of personal data received from individuals about those individuals. This policy is applicable to the processing of personal data received from individuals who are physically in the EU at the time data is initially collected in connection with the offering of goods or services by the College. This policy is in addition to and does not replace other College policies and procedures, such as policies regarding the protection of student information, employee information, health record information or other data.

i. LCCC provides protection to the sensitive data stored on databases through the implementation of data encryption. This is designed to encrypt and decrypt the systems

databases containing sensitive information and PII. PII data is encrypted while at rest and while in transit on any external network.

j. LCCC shall evaluate and adjust its information security program in light of the results of required testing and monitoring, material changes to its operations or business arrangements, results of risk assessments, or any other circumstances that may have a material impact on the information security program.

k. LCCC requires that any in-house developed software that transmits, accesses or stores customer information utilize current secure development practices. Externally developed software that transmits, accesses, or stores customer information is subjected to evaluation, testing, or assessment of security before implementation.

l. Access to PII is protected by multi-factor authentication requirements when possible and other mitigating technical measures are employed where multi-factor authentication is not possible.

C. Data Integrity

a. Data integrity can be compromised through human error or through malicious acts. To that end, LCCC has guidelines in place to gather and enter consistent data into the Administrative Computer System. See Data Quality Committee: Guidelines for advancing and maintaining data integrity and consistency at LCCC document for details.

b. Data validating methods are implemented to ensure that LCCC is able to report accurately and process data accurately. This is a statewide initiative with the Wyoming Community College Commission.

D. Backup of Computer Systems

a. Servers are backed up nightly using a combination of full, differential, and incremental backup methods. Because they are nightly, our Recovery Point Objective is less than 24 hours. Servers identified as being critical to the operation of the college are backed up in four locations, three of them being offsite, and backups are considered immutable to protect against ransomware and tampering. All backups are stored in an encrypted format to prevent unauthorized access. Our Recovery Time Objective for critical servers is eight hours. Restoration from cloud backup may add additional time due to the unpredictable nature of large data transfers occurring over the Internet. Backups are tested for viability every six months.

E. Disaster Recovery

a. In addition to nightly server backups, redundant offline copies of critical servers are maintained in a separate offsite datacenter. This is designed to be a short-term solution in the event of a disaster that prevents the use of our normal production infrastructure. Our Recovery Point Objective for these instances is less than one hour and our Recovery Time Objective is eight hours. In the event of a disaster, an assessment of our situation will be conducted by ITS, and a determination is made as to whether use of the offsite datacenter is warranted or not. If the decision is made to failover to the offsite datacenter, services are restored in a limited capacity to only a limited number of college employees. ITS will provide any software required to access these instances of our servers. Employees may also require a separate Internet connection, depending on

the status of onsite infrastructure. Our disaster recovery strategy is tested for viability every six months.

F. Employee Workstations
   a. It is the responsibility of each employee to adequately safeguard their own data from loss. To protect against most common data-loss scenarios, ITS advises that all data on employee computers be stored within the OneDrive account provided by the College. Data stored in OneDrive is highly available, protected from hardware failure, and secure. It can be recovered in the event of accidental deletion or restored to previous versions in the event of ransomware. Employees should avoid storing data to any place on their computer's hard drive not synced by the OneDrive Sync Client.

G. 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. Student violations will follow disciplinary procedures according to the Student Code of Conduct Policy 3.15 and Student Rights and Responsibilities Policy 3.17.
   c. 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.).
   d. Cases of serious, deliberate criminal conduct will be referred to the appropriate external authorities and may result in civil or criminal proceedings.

H. Resources
   a. Children's Internet Protection Act (CIPA): https://www.fcc.gov/consumers/guides/childrens-internet-protection-act
   b. Family Educational Rights and Privacy Act (FERPA): https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html
   c. 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.
   d. General Data Protection Regulation (GDPR): https://gdpr.eu/tag/gdpr/
   e. Data Quality Committee: Guidelines for advancing and maintaining data integrity and consistency at LCCC. https://lccc.wy.edu//Documents/About/accreditation/2018/5-1/5P1d_IR_DQC_Guidelines_p-2_20170510.pdf
   f. Privacy Protection and Information Security Procedure 9.8P
   g. Privacy, Access to, and Amendment of Student Records Procedure 3.4.2
   h. Records Retention Procedure 9.5P
   i. Identity Theft Prevention Program Procedure 9.6P
   j. Acceptable Use Procedure 8.3P
   k. Video Conferencing Software Supplemental Guidance 8.3.3P
   l. Cloud-Based Services Supplemental Guidance 8.3.1P

REQUIRED APPROVALS	NAME/SIGNATURE	DATE
Originator(s) Name(s)		
Approval by President's Cabinet		
Ratified by College Council		
Approval by President (Signature)		