Privacy Protection and Information Security Procedure	Procedure Number	9.8P
	Effective Date	September 30, 2019

1.0 PURPOSE

In order to meet Laramie County Community College's multi-faceted mission, LCCC must function in an increasingly information-dependent and privacy-regulated environment. Safeguarding both the institution's business information assets, and the personal information of all stakeholders, is vital to operational processes and public trust. All affected persons are expected to respect and maintain the confidentiality of LCCC information and the privacy of individuals whose records they access.

The Privacy Protection and Information Security program, procedures, and operating practices will incorporate requirements of all applicable state and federal regulations, including the Family Educational Rights and Privacy Act, Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act. The assumed practices of institutions of higher education and the standards of practice for the professions within higher education will serve as resources for additional privacy and information security practices.

In accordance with Laramie County Community College's Integrity and Standards of Practice Policy 9.8, the purpose of this procedure is to set forth the procedures for ensuring LCCC protects and correctly manages all personal and proprietary information and data collected, stored or reported by the college, in any format. Any regulation or standard required of LCCC is enforceable as part of this procedure.

2.0 REVISION HISTORY

Adopted on: 8/2/19 by Temporary Executive Order through 12/4/19; 9/30/19

3.0 PERSONS AFFECTED

Persons affected by this policy include all individuals with access to Laramie County Community College non-public data in any capacity. This includes those volunteering for, or on behalf of, the college.

4.0 DEFINITIONS

A. *Personal Information* – Any information that can be used to identify an individual or with other information to identify, contact, or locate an individual. This includes Personally Identifiable Information (PII) and Protected Personally Identifiable Information (PPII).

1) 2 *CFR §200.79 Personally Identifiable Information (PII)* – PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly

available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

2) 2 *CFR §200.82 Protected Personally Identifiable Information (Protected PII)* – Protected PII means an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. This does not include PII that is required by law to be disclosed.

B. *Business Information Assets* – Any information that is critical to the operation of the college or protected by LCCC through regulation or legally binding agreement (e.g., NDAs, copyrights, or sponsored awards), of which a compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on college interests or operations, or the privacy to which LCCC stakeholders are entitled (e.g., intellectual property or proprietary information).

C. *Data/Information Breach* – Any event when the potential for non-authorized access to PII, business information assets, or protected information occurs.

D. Freedom of Information Act (FOIA) – A federal freedom of information law that allows for the full or partial disclosure of previously unreleased information and documents controlled by the federal government.

E. *Governing Regulation* – Regulations with which LCCC must comply as a course of business, including but not limited to FERPA, GBLA, and HIPAA.

F. *Information Technology Resource (IT Resource)* – A resource used for electronic storage, processing or transmitting of any data or information, as well as the data or information itself. This definition includes but is not limited to electronic mail, voice mail, local databases, externally accessed databases, CD-ROM, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio, electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

G. *Protected Information* – includes PII and business information assets, and anything deemed sensitive by policy or law, in the custody of LCCC's non-public information systems whether in electronic, paper, or other forms. Examples of such data would include that data protected by the Health Insurance Portability and Accountability Act (HIPAA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data or data that has been deemed by the college as requiring protective measures.

H. Wyoming Public Records Act – A state-level information access law that provides the public with access to public records, books, and files of state governmental agencies (subject to exceptions). The Public Records Act defines "public records" as "the original and copies of any paper, correspondence, form, book, photograph, photostat, film, microfilm, sound recording, map drawing or other document, regardless of physical form or characteristics that have been made by the state of Wyoming and any counties, municipalities and political subdivisions thereof and

by any agencies of the state, counties, municipalities and political subdivisions thereof, or received by them in connection with the transaction of public business, except those privileged or confidential by law."

5.0 PROCEDURES

A. Meeting Regulatory Requirements

LCCC's President's Cabinet will establish the necessary compliance areas and assign responsibility for the oversight and day-to-day management of those functions. Responsible areas are tasked with prescribing the operating procedures to identify protected information, prevent any compromise of LCCC's information security, and detect and report any misuse of protected information.

B. Support of the Privacy Protection and Information Security Program

LCCC will maintain a working group of subject matter technical experts from the major compliance areas to support the campus community in issue identification and resolution.

C. Policies Maintained and Acknowledged

Each compliance area is tasked with ensuring policies and procedures remain current and reflect applicable regulations and laws. Employee acknowledgement of receipt of policies will be included in the Human Resources onboarding process.

D. Training and Awareness

All LCCC employees will complete basic information security training. Employees in areas with protected information functions will have additional training as determined by their function.

E. Use of IT Resources

ITS will establish the security protocols and technological protections necessary to identify and prevent the system compromise of protected information and overall information system security, including determining penalties or prescribing access limitations for the misuse of LCCC IT resources.

F. Collecting, Managing and Storing Protected Information

Protected information will only be collected, managed, or stored by areas with an operation need for such information and only using ITS approved systems.

G. Access to Protected Information

Access to protected information will be granted on the principle of least privilege and restricted to those users that have a legitimate business need and appropriate approvals for access to such information. All persons with access to systems containing protected information or locations where protected information is stored will receive an orientation and training and will be responsible for safeguarding this information and related systems at all times.

H. Securing Protected Information

The physical security of protected information will be accomplished utilizing current industry standards and appropriate methods as determined by ITS and the compliance area.

I. Transmitting Protected Information

Users will ensure protected information is secure and the integrity of records is safeguarded in storage and transmission. Users of protected information are responsible for the proper management of this data while under their control.

J. Requests for Reports under FOIA or WPRA

The purpose of the FOIA and the WPRA is to promote disclosure of publicly-funded records. The law does not require the college to create or compile a record that does not exist at the time of the request. LCCC maintains a designated point of contact for FOIA and WPRA requests.

K. Reporting data/information breaches.

All suspected or actual breaches of protected information must be reported immediately to LCCC's designated Cybersecurity Coordinator. The Coordinator and breach reporter will respond according to Incident Response Guidelines maintained by ITS.

L. Notification to Regulatory Agencies

Each compliance area oversight authority will report and/or publicize unauthorized information disclosures as required by law or specific industry requirements.

M. Notification to President's Cabinet and Board of Trustees

Data breaches, incidents and metrics for LCCC's Privacy Protection and Information Security program will be reported to the President's Cabinet and the Board of Trustees on an annual basis.

N. Misconduct and Misuse of Individual or Institutional Information

The unauthorized addition, modification, deletion, or disclosure of protected information is expressly forbidden. Penalties and enforcement of this procedure will be in accordance with LCCC policies. Appropriate disciplinary and/or legal action will be taken when warranted in any area involving violations of this procedure.

REQUIRED APPROVALS	NAME/SIGNATURE	DATE
Originator(s) Name(s)	Victoria Steel, Sponsored Awards and Compliance Director on behalf of the Privacy Protection and Information Security Working Group	8/2/19
Approval by President's Cabinet		
Ratified by College Council		
Approval by President (Signature)		8/2/19