**Policy Number:** 7.2
**Effective Date:** 2003
**Last Reviewed:** 6/25/2018
**Approved by Trustees:** (*Pending*)

**Policy Owner:** Chief Information Officer
**Policy Implementation:** Chief Information Officer

# Student Information Security and Privacy

## I. Privacy

Lander University complies with the Family Educational Rights and Privacy Act of 1974 (FERPA), which is designed to protect the privacy of student education records maintained by the university. Any student who is or has been in attendance at Lander University has FERPA rights. The rights parents exercise with respect to their children's education records transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Lander University may discuss information about a student's educational records with the parents if the student completes the Student Information Release Form in the Registrar's Office.

The following student rights are covered by the Act and afforded to all eligible students of the university:

A. The right to inspect and review information in the student's educational records.
B. The right to request amendment of the contents of the student's educational records if believed to be inaccurate, misleading or otherwise in violation of the student's privacy or other rights.
C. The right to prevent disclosure without consent, with certain exceptions, of personally identifiable information from the student's informational records.
D. The right to file complaints with the U.S. Department of Education concerning alleged failures by the university to comply with the provisions of the Act.

The name and address of the Office that administers FERPA is:
Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202-8520

The act further provides that certain information designated as directory information may be released by the university about the student unless the student has informed the university that such information should not be released. Lander University designates the following items as Directory Information: the student's name, address, telephone number, electronic mail address, date and place of birth, classification, major and minor field of study, athletic participation, participation in Lander organizational memberships, weight and height of athletes, dates of attendance, honors conferred, degrees conferred, awards and scholarships received, admission status (date of acceptance), enrollment status (full/part-time), and the most recent previous educational agency or institution attended by the student.

Students have the right to request that directory information not be released to outside parties. To request non-disclosure, students must complete the Student Privacy Request Form in the Registrar's Office. Requests to withhold directory information will remain in effect until the student completes another Student Privacy Request Form in the Registrar's Office to reverse the decision.

According to the provisions of the Family Educational Rights and Privacy Act of 1974 and with the exception of directory information, student records, files, documents, and other materials which contain information directly related to a student and are maintained by Lander should be accessed for internal use only on a legitimate, educational NEED TO KNOW basis. Data which is part of the student's record, but which is not considered directory information, may not be disclosed to a third party without the written consent of the student. The Act further provides that directory information may not be released if the student has informed the institution, via Student Privacy Request Form, that such information should not be released. The regulations governing the release of student information apply to that which is contained in the hard (paper) copy as well as that which is available using online computer files. Any questions pertaining to the release of student information should be directed to the Registrar's Office.

For more information regarding FERPA, please visit the U.S. Department of Education's website: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html?src=ft

## II. Security

In addition, Lander University is committed to safeguarding student information. The impetus for creating this security plan originates with the final regulations issued by the Federal Trade Commission (FTC) under 16 CFR Part 314, as published in the May 23, 2002 Federal Register, p. 346484). These regulations stem from the Gramm-Leach Bliley Act (GLB Act) enacted in 2000. All colleges and universities in the United States participating in financial aid fall under the GLB Act and are therefore required to develop and maintain an information security plan.

A. Objectives

1. To ensure the security of student information;
2. To protect against any anticipated threats to the security or integrity of such information;
3. To guard against the unauthorized access to, or use of, such information that could result in substantial harm or inconvenience to any student.

## III. History

Since its design in 2003, most of the original steps and recommendations for the Student Information Security and Privacy Procedure have been implemented or modified to meet the changing needs of Lander University students as well as changes in technology. Of particular concern since the origins of this Procedure is the privacy of student information in an online setting; whether students are traditional or distance/online learners (or a combination of the two), much of their class work and even advising can take place online. Lander University has continuously found ways to control the security and privacy of this information, from requiring that faculty, staff, and students use their password-protected official Lander email accounts in online communications to implementing, for all university classes, the Blackboard course administration program, which contains specific privacy policies and

settings carefully monitored by Information Technology Services (ITS). Since the Student Information Security and Privacy Procedure is actually more of an ongoing process, it is up to everyone—faculty, staff, and students—to help safeguard student information and to alert the appropriate office, such as the Registrar, Financial Aid, or ITS, of security or privacy issues. Thus, the Procedure has operated as one of constant internal self-assessment and review. When formal changes to this Procedure are deemed necessary by the Chief Information Officer (CIO) and Registrar, the CIO will submit the revised Procedure to the Policy Administrator, who will arrange for the document to be reviewed and approved by the President's Cabinet and the Board of Trustees.

## IV. Information security and privacy safeguards

The following are safeguards currently in place at Lander University for maintaining the security and privacy of student information:

A. Employee training as part of new hire orientation
    1. Information security procedures are discussed as part of new hire orientations.
    2. Before being granted access to online student data via Banner, all employees sign a compliance/confidentiality statement acknowledging the sensitivity of nonpublic student information, reading of Lander University's information policy, and noting FERPA and Federal Trade Commission penalties for unauthorized disclosures.

B. Completion of annual security awareness training is required of all employees (faculty and staff) to educate them on new information security threats and remind them of current University policies and procedures regarding student privacy;

C. Access to information is limited to offices and employees within those offices on a "need- to-know" basis;

D. Student information screens, reports, files, or forms are restricted to employees on a "need- to-know" basis;

E. All hard drives of employees having access to non-public student information are physically destroyed upon retirement from active use. These PCs are no longer made surplus to the state for reuse or resale with the hard drives intact;

F. ITS regularly manages, updates, and maintains information systems, including detecting, preventing, and responding to online attacks, intrusions, or other system failures;

G. Computers in offices are positioned so that they cannot be seen from the front, or polarized screens are in place to prevent side viewing, primarily in offices such as The Office of the Registrar, in which computers are in close proximity to students;

H. The student information system (MyLander portal, Bearcat Web, and/or Blackboard) and Lander email require authentication through the use of user names and passwords, which is particularly important for protecting the privacy of online/distance learners;

I. All students (traditional and/or online) are identified through the use of internally- generated identification numbers instead of Social Security Numbers;

J. Web firewall and virus protection are in place for all computers, servers, and internet connections on campus, and student computers cannot connect to the network without virus protection;

K. Security agreements are in place with outside vendors having access to student information, including the National Student Clearinghouse or Aramark Food Service;

L. An automated session timeout of the student information system (MyLander portal, Bearcat Web, and/or Blackboard) is set for all employee, student, and faculty computers without activity;

M. Paper documents such as registration forms, rosters, and Add/Drop forms are secured when work stations are unattended;

N. Lander University regularly conducts on-site confidential shredding of documents, containing student information ready for destruction, by a third-party vendor. Certain offices on campus also have purchased cross-cut shredders for additional safety; and

O. To protect student data, an email encryption feature is available for all Lander accounts, and its use is mandatory when transmitting student information and/or education records via email.

## V. Procedure

To control access to protected student information and ensure compliance with federal and state security and privacy regulations:

A. All requests for access to student information must be submitted to the Office of the Registrar.

B. Any known or suspected compromise of student information must be reported immediately to the Information Security Officer (ISO) and/or CIO.
   1. Any confirmed compromise of student information ("data breach") must be reported to South Carolina's Enterprise Privacy Office.
   2. The ISO will carry out the incident response and remediation process, which includes determining if there is a way to stop the spread of compromised information and/or prevent access by unauthorized personnel.
   3. After the scope of the compromise is determined, the ISO will provide all relevant information to the University's Privacy Officer, who will evaluate whether the data breach warrants student notification or other actions.

## VI. Summary

The Student Information Security and Privacy Procedure is designed to help avoid risks common to any online learning situation, including the misuse, theft, or unauthorized viewing of information displayed on computer screens, accessed online, or printed to reports, files, or forms.

As an ongoing process, this Procedure will undergo certain changes and improvements, including the following:

A. The Procedure will be subject to frequent formal reviews of its contents to keep its measures and processes up-to-date;

B. Management/Administration will include discussion or reminders of information security and privacy procedures more frequently as a part of normal staff and faculty meetings;

C. While initial faculty "new hire" orientations provide this information, all employees will be

reminded about the need to keep unattended and unsecured computers – including classroom computers—logged off so that screens available for recall or update of student information are not compromised with regard to privacy or security; and

D. Initial faculty "new hire" orientations will include more thorough training in regards to securing student privacy, particularly in online/distance learning situations.

Overall, the Student Information Security and Privacy Procedure has provided both traditional and online/distance learners with safe and secure information, from personal data to midterm and final grades, and has also worked to maintain the privacy and confidentiality of this information in a variety of forms, whether online, on paper, or on a computer screen.