



founded in 1872

LANDER UNIVERSITY

Office of Information Technology Services

PRIVACY AND SECURITY

OF

STUDENT INFORMATION:

LANDER UNIVERSITY'S PLAN

JULY 2003

TABLE OF CONTENTS

1. PRIVACY	3
2. SECURITY	4
A) OBJECTIVES.....	4
B) FIRST STEPS.....	4
C) COMMON RISKS	5
D) SAFEGUARDS.....	5
E) ADDITIONAL SAFEGUARDS RECOMMENDATIONS.....	5
3. SUMMARY	7

1. PRIVACY

Lander University's firm commitment to the privacy of student information is practiced through strict adherence to the Family Educational Rights and Privacy Act (FERPA) as shown in the following chart:

Information contained in the permanent educational record of each Lander University student follows the professional guidelines set forth by the American Association of Collegiate Registrars and Admissions Officers (AACRAO) in the *Academic Record and Transcript Guide*.

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 Vice President for Student Affairs, in writing, 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 on-line computer files.

Any questions pertaining to the release of student information should be directed to the Office of the Registrar.

GUIDE FOR RELEASE OF STUDENT INFORMATION	Employers	General Public	Government Agencies (except Military Recruiters)	Lander Faculty/Staff	Other Educational Institutions	Parents/Spouse/Guardian	Other Students	Military Recruiters (in compliance with "Solomon Amendment")
TYPE OF INQUIRY								
General Information.....								
*Address/Telephone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Athletic participation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Country of citizenship	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Date and place of birth	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Height and weight of athletes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Lander organizational memberships	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Name of student	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Parents' names/address/telephone	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Personal Identification Number (PIN)	No	No	No	No	No	No	No	No
Public Safety Reports	No	No	No	Yes	No	No	No	No
Race/Ethnicity	No	No	No	No	No	No	No	No
Student ID number	No	No	No	Yes	No	No	No	No
Veterans Status	No	No	Yes	Yes	No	Yes	No	No
Academic Information.....								
*Awards and scholarships	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Class level (freshman, sophomore...)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Class schedule	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Dates of attendance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Degrees (dates) conferred	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Enrollment status (full/part-time)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Honors conferred	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Major and minor field of study	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
*Most recent school attended	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Academic status (probation/suspension)	No	No	No	Yes	No	No	No	No
Admission status (accepted, rejected...)	No	No	No	Yes	No	No	No	No
Admission status (date of acceptance)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
FALS events attended	No	No	No	Yes	No	No	No	No
Grades/GPA/hours earned	No	No	No	Yes	No	No	No	No
Test scores (SAT,ACT...)	No	No	No	Yes	No	No	No	No
List of Drop Out/Stop Out Students	No	No	No	Yes	No	No	No	No

* indicates information considered to be "directory information" at Lander University. That is, information that would not generally be considered harmful or an invasion of privacy if disclosed.

NOTE: Lander may disclose educational records without the written consent of students 1) to persons in an emergency if the information is necessary to protect the health or safety of students or other persons, 2) upon subpoena by a court or tribunal of competent jurisdiction, 3) to authorized representatives of the U. S. Attorney General, 4) to parents and legal guardians of students under the age of 21 of information regarding student's violation of laws or policies governing the use or possession of alcohol or a controlled substance, 5) regarding final results of a disciplinary proceeding against a postsecondary student.

2. 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

- i) To ensure the security of student information;
- ii) To protect against any anticipated threats to the security or integrity of such information;
- iii) To guard against the unauthorized access to, or use of, such information that could result in substantial harm or inconvenience to any student.

b) FIRST STEPS

Because information security covers a broad area affecting many departments, a step-by-step process is needed to implement the program. The following steps are considered essential to developing an ongoing security program:

- i) Designate an employee or team to coordinate the security information program, make suggestions and recommendations on an ongoing basis to the President's Council, and maintain a database of departmental risks and safeguards.
- ii) Complete a risk assessment to identify reasonable, foreseeable internal and external risks to the information provided by students. The assessment will be updated periodically but not less than once every five years. The risk assessment will specifically cover the following general areas:
 - (1) Employee training and management;
 - (2) Information systems management, including detecting, preventing and responding to attacks, intrusions or other system failures;
 - (3) University operations as regards the obtaining, processing, accessing, or reporting of student information including but not limited to: Admissions, Advising, Student Accounts, Financial Aid, Instructors, Counseling, and Tutoring;
 - (4) Service providers such as bookstore vendors relating to graduating students and other educational organizations such as the National Student Clearinghouse and the South Carolina Commission on Higher Education.
- iii) List common risks and safeguards noted from the risk assessment.
- iv) Identify and address individual risks and safeguards for each department processing student information.
- v) Apply suggestions for improvements resulting from the assessment, through specific recommendations to the President's Council.
- vi) Test safeguards for effectiveness through internal audits conducted as a part of the regular cycle of internal audits.

- vii) Review progress of the implementation of suggestions and recommendations and initiate new suggestions and recommendations periodically but not less than once a year.

c) COMMON RISKS

The following common risks are noted for all departments:

- i) Information displayed on PC screens or printed to reports, files or forms is misused by employees, contractors, or agencies;
- ii) information on PC screens or printed to reports, files or forms is viewed by unauthorized persons;
- iii) Information is stolen by outside attackers, such as hackers, etc.

d) SAFEGUARDS

Safeguards currently in place:

- i) Student information system requires authentication through the use of user names and passwords;
- ii) Employees, including student workers, are required to sign confidentiality statements regarding the release of student information;
- iii) Access to information is limited to offices and employees within those offices on a “need-to-know” basis;
- iv) Student information screens, reports, files or forms are restricted to employees on a “need-to-know” basis;
- v) Counter and desk designs are positioned so that PC screens face away from students or visitors;
- vi) Security agreements are in place with outside vendors having access to student information;
- vii) Automated shut down time of student information systems for PC’s without activity for 60 minutes;
- viii) Paper documents such as registration forms, rosters and Add/Drop forms are secured when work stations are unattended;
- ix) On-Site shredding of documents containing student information and that are ready for destruction by a third-party vendor;
- x) Unused hard drives from offices that retain student information on PC’s and are no longer in use are reinitialized;
- xi) Web firewall and virus protection for all PC’s, servers and internet connections.

e) ADDITIONAL SAFEGUARDS RECOMMENDATIONS

Safeguards to be initiated:

- i) Employee Training
 - (1) Information security procedures such as using encryption technology for e-mailing student non-public information, securing paper documents containing non-public information, etc. should be a part of the “New hire” packages as a separate information sheet. The sheet should reflect FERPA (Family Education Rights and Privacy Act) and HIPAA (Health

- Insurance and Portability Accountability Act) regulations and examples of violations;
- (2) A compliance/confidentiality statement should be developed for all employees to sign acknowledging the sensitivity of nonpublic student information, reading of Lander University's information policy, as well as noting FERPA and Federal Trade Commission penalties for unauthorized disclosures;
 - (3) Information security, while not a large enough subject for separate seminars, should be worked into an expansion of Human Resources' recently developed HIPAA medical information;
 - (4) Management should periodically include discussion of information security procedures as a part of normal staff and faculty meetings.
- ii) Student Information System Procedures
- (1) Sensitize employees about the need to keep unattended and unsecured PCs logged off so that screens available for recall or update of student information is not compromised with regard to privacy or security;
 - (2) Identify students through the use of randomly-generated identification numbers rather than through the use of Social Security Numbers;
 - (3) Know the information security plans of outside agencies and vendors that receive Lander University's nonpublic student information or have access to our database. Contractual security agreements with vendors such as the National Student Clearinghouse or Aramark Food Service need to be initiated to ensure they implement and maintain appropriate information safeguards.
 - (4) All hard drives of employees having access to non- public student information should be physically destroyed upon retirement from active use. These PCs should no longer be surplus to the state for reuse or resale with the hard drives intact. If required new University procedures and /or policies should be developed.
 - (5) Existing Student/Employee ID cards contain social security numbers in bar code for use with the library ID system. Adding the randomly-generated student identification number to the student ID card would protect students from having their social security numbers viewed unintentionally.
 - (6) Scrap paper needs to be screened by those who generate before it is turned into scratch pads to guard against the unauthorized access to, or use of, such information that could result in substantial harm or inconvenience to any student.
- iii) Existing Safeguards - Changes and Improvements
- (1) The Cashier and Office of the Registrar PC's are in close proximity to students and require managers in those offices to sensitize their employees of the need to position of PCs so they cannot be seen from the front of the counter or to purchase a Polarized screen to prevent side viewing;
 - (2) Where not in practice, all areas should participate in the campus-wide confidential shredding that occurs once every four weeks and/or purchase

cross cut shredders. Strip cut shredders are not secure due to inexpensive advanced software with the ability to reconstruct strip-shredded documents, after being scanned into a PC.

3. SUMMARY

Once decisions have been reached on the initial recommendations, the information security program will be in place.

The ongoing security information program will consist of:

- a) Periodic internal application and effectiveness audits of risks and safeguards in departments processing student non-public information;
- b) Periodic risk assessments to update the list of risks and safeguards;
- c) Periodic reviews to continue awareness of risks and safeguards with resulting suggestions and recommendations sent to the President's Council.