SUNY Student Loan Service Center
Gramm-Leach-Bliley Act
Safeguard Plan

The SUNY Student Loan Service Center (SLSC) is committed to protecting the confidential information that the SUNY campuses and their current and former students entrust to us. In that regard, the SLSC collects and shares information only for the purpose of administering the Federal Grant and Loan Programs as required by Federal and/or State Law.

This document describes our standards relating to the Administrative, Technical, and Physical Safeguards, as they pertain to the collection, use and disclosure of personal information pertaining to current and former SUNY students. The objectives of these standards are to:

- Ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records; and
- Protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience to any customer.

Employee and Management Training:

All staff members, including temporary staff and students, will be provided with a copy of the Safeguard Plan and trained on the contents.

Third Party Agencies:

The SLSC may share information with third parties as necessary to meet the requirements of servicing the Title IV and Title VII federal aid programs. Third parties include, but are not limited to:

- Contracted Collection Agencies
- Educational Computer Systems, Inc.
- Law Enforcement Agencies
- National Credit Bureaus
- National Student Clearinghouse
- National Student Loan Database System (NSLDS)
- New York State Attorney General's Office
- New York State Department of Taxation and Finance
- United States Department of Education
- United States Department of Health and Human Services

The information we share with outside agencies is strictly limited to the information needed to perform the specific service they provide and shall be used by them only for that purpose. All contracted third party service agents are required to implement and maintain a written Information Security Program in order to protect such customer information.

Customer Information Disposal:

All customer information is retained and disposed of in accordance with all applicable federal, state and SUNY records retention and disposal policies. Specifically, the State University of New York erases all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contains customer information.

All obsolete confidential documents shall be shredded, and not disposed of directly in waste receptacles. The documents to be shredded shall be placed in recycling containers or shall be otherwise tagged for shredding. The SLSC contracts with Mobile Shredding to conduct on-site mass shredding once per month, or as needed, to securely dispose of all sensitive and personal information, including paper documents, diskettes and microfiche. Mobile Shredding agrees to maintain the SLSC's high standards of information security.

Staff Access and Protection of Personal and/or Private Information:

The SLSC authorizes access to personal student/borrower information only to those staff members who have a legitimate need to know such information in order to carry out their specific job responsibilities. Employees who have access to this information are required to keep the information secure and confidential. Specific safeguards exist with regard to the following areas:

File Room: Only those employees who need access to borrower files are allowed to review such information. Employees removing a borrower file from the file room are required to sign the file out with their name and date of removal.

Promissory Note Room: All campus-based loan documentation (entrance interview, promissory note, exit interview, etc.), signed by the borrower while attending a SUNY state campus, is transferred to the SLSC upon the separation of that borrower. The SLSC maintains this information in locked, fireproof file cabinets within a locked room. Access to this room is limited strictly to those who work directly with this information.

Building and Office Access: Staff access to the building is controlled through card access during non-business hours. Entry to specific offices within the SLSC is controlled through a very limited distribution of office keys. All office doors are locked when the office is not occupied.

Confidentiality of Hard Copy Data: Staff members are to lock any confidential data in desks or file cabinets when they leave for the day. All confidential information that needs to be discarded must be discarded through the shredding containers that are kept in a secured and locked area of the office.

Computer Information Systems: Staff access to account information through our student loan database is controlled through security sign-on containing user name, user initials, and a

password. The SLSC will follow the University at Albany's Policy on the Responsible Use of Information Technology. Attached to and made a part of the Safeguard Plan is a copy of the Policy. The following are some of the key aspects of the Policy as the Policy applies to the SLSC:

- All user data is to be stored on secure network drives and not on personal hard drives. Access to these drives is allowed or denied based upon the University's Network Login;
- Information stored or accessed through the computer information system shall not be used, disclosed or destroyed without authorization;
- Information shall only be used for its intended purpose, and not for private purposes;
- Privacy of information shall be respected. Information shall not be shared except with other employees who need to know to perform their official work duties and assignments;
- Passwords may not be shared or distributed in any way, and they should not be written anywhere near the PC;
- Workstations shall not be left unattended without engaging the password protected screen saver or logging off the system entirely;
- Circumventing or breaching security is prohibited at all times;
- Employees who violate the policy may be subject to suspension or termination of access privileges to the system;
- System managers shall ensure the security of the systems;
- Security incidents are to be reported promptly to the supervisor and to ITS; and
- ITS has not only the right, but the responsibility, to remove computers from the network for violation of the security policy, and the responsibility for reconnecting computers to the network when the security risk no longer exists.

Removable Media: All removable media (floppies, zip disks, etc.) with data on them, are to be stored in a secure and locked location.

This Plan may be amended from time to time by the SLSC as required by changes in law and regulation, as well as in the sole discretion of the SLSC and the University to meet the demanding evolution of technology and changes to the industry's best business practices.

University at Albany

Information Security Program

(As it pertains to FTC Regulated Activity)

POLICY

University at Albany
Information Security Program
(As it pertains to FTC Regulated Activity)

Purpose:

- Ensure the security and confidentiality of customer records and information.
- Protect against anticipated threats to the security and/or integrity of such customer records and information.
- Guard against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.
- Comply with the Gramm-Leach-Bliley Act and the rules promulgated thereunder by the Federal Trade Commission.

OUTLINE

I. Program Coordination

A. A Designated representative from Office of the Provost shall coordinate the Information Security Program (the "Program").

B. The Program includes input from other University departments, including, but not limited to, University Counsel and Information Technology.

C. The Program will be reviewed and evaluated annually, during the month of June. Selected aspects will be tested periodically, and adjustments to the Program will be made as needed.

II. Risk Assessment & Safeguards

There is an inherent risk in handling and storing any information that must be protected. Identifying areas of risk and maintaining appropriate safeguards can reduce risk. Safeguards are designed to reduce the risk inherent in handling customer information. The Federal Trade Commission has identified four areas to address:

A. Employee Management & Training
B. Information Systems
C. Managing System Failures
D. Service providers

III. Appendices.

A. Legal References
B. FERPA Policy

C. Rules Governing Access to and Release of Student and Employee Data

D. Access to Employee and Student Data Confidentiality Agreement
E. Maintaining the Security, Confidentiality and Integrity of Customer Information
F. Policy on the Responsible Use of Information Technology
G. Sample Office Safeguarding Practices
H. Policies Governing Student Use of Computing and Networking Facilities
I. ResNet Policies
J. Service Providers under the FTC Safeguards Rule
K. Helpful Resources

PROGRAM DETAILS

I. Designated Information Security Program Coordinator

A. The **Chief Information Officer**, or designee, is the designated University official charged with the responsibility for coordination of the University's Information Security Program.

B. Assessing Risk to and Safeguarding Customer Information
The following offices have been identified as those among the relevant offices to be considered when assessing the risks to customer information possessed or maintained by the University, and these offices also shall have primary responsibility for safeguarding such information: Human Resources, Information Technology, SUNYCard, Admissions, Registrar, Financial Aid, Student Affairs, Student Accounts, Advancement, Controller, Facilities and Residential Life. Each relevant area is responsible to secure customer information in accordance with all relevant security guidelines.

II. Risk Assessment & Safeguards

A. Definitions

Covered data and information for the purpose of this policy includes student and other customer financial information required to be protected under the Gramm-Leach-Bliley Act (GLB). Covered data and information includes both paper and electronic records.

Customer financial information is that information the Campus has obtained from a student or other customer in the process of offering a financial product or service, or such information provided to the university by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of customer financial information include addresses, phone numbers, bank and credit card account

numbers, income and credit histories and social security numbers, in both paper and electronic format.

B. Employee Management & Training

Employees handle and have access to customer information in order to perform their job duties. The term "employee" includes permanent and temporary employees and work-study students and student assistants, whose job duties require them to access customer information or work in a location where there is access to customer information.

1. Hiring Employees

The University at Albany exercises great care in trying to select well-qualified employees. Hiring supervisors review applications, carry out interviews and check references and verify college degrees before making their final selection. All newly hired employees participate in individual or group orientation sessions which include information on the privacy and safeguarding of confidential information.

2. Work-Study Students and Student Assistants

Work-Study students are referred by the Financial Aid Office and Student Assistants apply for part-time positions as available. Individual offices interview the students referred or applying and make the final decision before a student is placed. Confidentiality and safeguarding of information is covered in an individual orientation session conducted prior to the first day of work.

Furthermore, under the Higher Education Act the University annually must and does distribute to all enrolled students and posts on the University website a notice of the availability of financial assistance and institutional information required to be disclosed pursuant to the Act including information regarding the Family Educational Rights and Privacy Act (FERPA) which governs access to student educational records maintained by educational institutions and the release of information from those records. **(See Appendix B)**.

3. Permanent Employees

Before receiving access to the University's administrative systems, all employees are provided information on information privacy and security **(See Appendix C)** and must sign confidentiality agreements acknowledging their obligations to ensure the security of confidential information. **(See Appendix D)**. Furthermore, each year the Office of Human Resources distributes to all employees information on maintaining the security and confidentiality of customer information. **(See Appendix E)**.

4. Ongoing Training

Periodically, employees with access to protected customer information will take part in FERPA and Safeguards training, as a refresher.

5. Access to Customer Information
Only employees whose job duties require them to access customer information shall have access, and such access is limited to that necessary and consistent with job responsibilities.

6. Disciplinary Measures for Breaches
Breaches of information security may result in appropriate disciplinary action, depending upon the nature and severity of the breach. All breaches should be reported in accordance with the University's Policy on the Responsible Use of Information Technology **(See Appendix F)** and rectified as soon as possible. Employees, work-study students and student assistants are encouraged to report any suspected intentional and/or malicious breaches to an appropriate University official or supervisor.

C. Information Systems

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal.

1. Paper Storage Systems
Access safeguards best practices are outlined in the document "Maintaining the Security, Confidentiality & Integrity of Customer Information."

Additional Safeguards:
Each University off will be responsible to develop security practices designed to ensure the safeguarding of paper storage systems and securing storage and work areas. Such practices may include, but shall not be limited to storing critical customer documents in fireproof file cabinets and storing files so as to minimize damage in the case of flooding. An example of such office practices is attached as **Appendix G**.

2. Computer Information Systems
The Office of Information Security serves as the central electronic information security office. The following information security policies and practices that protect against unanticipated threats to the security or integrity of electronic customer information and guard against the unauthorized use of such information apply:

Policy on the Responsible Use of Information Technology **(See Appendix F)**

- prohibits use of IT for non-university purposes, for financial gain, etc.
- prohibits unauthorized use, disclosure of, or destruction of information
- prohibits sharing of passwords
- requires users to respect privacy of information and use it only for its intended purposes
- prohibits circumventing or breaching of security

- provides for the suspension or termination of user access privileges for violations of the policy
- requires System managers to ensure that systems are secure

Campus IT Security Procedures

- security incidents are to be reported promptly to supervisor and to ITS
- ITS has the right/responsibility to remove computers from the network
- departments/offices have responsibility to bring their computers into compliance with campus standards and security
- ITS reconnects computers to the network when they no longer pose a security risk
- UA “enterprise” IT systems housed in campus data center with controlled physical access, and back-up storage procedures
- users with access to IAS systems required to sign a data confidentiality agreement
- users with multiple netIDs reconciled so that each user has one netID
- NetIDs and e-mail addresses are issued based on entry into PeopleSoft Student or Employee record system
- all users will be issued PINs to safeguard lost or forgotten passwords (June ’03)
- sets forth policies and procedures to ensure secure remote connections to the University's computing network

Policy Governing Student Use of Computing and Networking Facilities at the University at Albany **(See Appendix H)** prohibits students from :

- Lending computing user ID or account to another person.
- Using a computer user ID or account assigned to another person.
- Compromising the privacy of electronic networks or information systems.
- Damaging or destroying the integrity of electronic information or computer hardware or software.
- Attempting to interfere with, or disrupt the use of electronic networks, information systems or the legitimate work of another user.
- Attempting to circumvent system or network security.
- Attempting to access the computer files belonging to another user without permission.
- Sending messages that cause an interruption in the work of others.
- Chain letters.
- E-mail bombs.
- Using computing or network facilities to harass or intimidate any other person or group.
- Using University computing/network facilities for personal profit.

- Unauthorized copying and, or distribution of software or other intellectual work such as music, images, logos and speeches. All proprietary computer software is legally protected by copyright, patent, or trade secret law.
- Misrepresenting the ownership or source of files and messages.
- Providing unauthorized users with access to University systems and resources, or assisting unauthorized users in accessing University systems and resources.
- Abusing specific computer and network resources, as described in other University documents

University's Residential Network Policies require all systems connecting to the University's network to be running current and active antivirus software which is made available by the University to all students free of charge. Additional security practices guidance and recommendations, including the ResNet Participants Agreement, which sets forth the terms and conditions of use of the residential network, are provided on the ResNet website **(See Appendix I).**

3. Customer Information Disposal

The University at Albany will develop a program that provides for the confidential disposal of documents. Under the program obsolete confidential documents will be placed in recycling containers or are tagged for shredding in secure areas and marked confidential before being transferred for recycling/shredding and disposal.

The University at Albany erases all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information.

The University archives customer transaction information as necessary**.**

All customer information is retained and disposed of in accordance with all applicable federal, state and SUNY records retention and disposal policies.

D. Managing System Failures

1. Written Contingency Plans

2. Centralized Protection from E-Invasion

See paragraph C.2. above.

3. System Back-ups

System back-ups are performed on a regular basis and are stored in a secure offsite location.

4. Security Breaches

In the event that information security is compromised, a prompt disclosure will be made to any customers that may have been impacted. (**See Appendix F).**

E. Service Providers

1. Contracts

All contracts with service providers are reviewed by the Offices of Institutional Services and Counsel to ensure that external service providers agree to observe the University's high standards of information security. Contracts will not be approved with providers that will not agree to maintain appropriate safeguards as provided in **Appendix J**.

2. Relevant Current Contracts

- Contracts with vendors for shredding, recycling services, etc;.
- Contracts with collection agencies;
- Contracts with software vendors having access to financial transactions and related information;
- Contracts with campus-related entities, such as Auxiliary Service Corporations, Campus Foundations and Alumni Associations

3. Monitoring

The University at Albany will periodically evaluate providers to ensure that they have complied with the information security requirements of the contract.

Appendices

A. Legal References
B. FERPA Policy
C. Rules Governing Access to and Release of Student and Employee Data
D. Access to Employee and Student Data Confidentiality Agreement
E. Maintaining the Security, Confidentiality and Integrity of Customer Information
F. Policy on the Responsible Use of Information Technology
G. Sample Office Safeguarding Practices
H. Policies Governing Student Use of Computing and Networking Facilities
I. ResNet Policies
J. Service Providers under the FTC Safeguards Rule
K. Helpful Resources

University at Albany

Information Security Program

(As is pertains to FTC Regulated Activity)

APPENDICES

A-K

Appendix A

Legal References

15 USC, Subchapter I, sec. 6801-6809 (Gramm-Leach-Bliley Act)
16 CFR, Part 313 (Privacy Regulations, see reference to FERPA)
20 USC, Chapter 31, 1232g (FERPA)
34 CFR, part 99 (FERPA regulations)
16 CFR, part 314 (Safeguard Regulations, as published in the Federal Register, 5/23/02)

Appendix B

Family Education Rights and Privacy Act Information

The Family Educational Rights and Privacy Act (FERPA) sets forth requirements designed to protect the privacy of student educational records. The law governs access to records maintained by educational institutions and the release of information from those records. FERPA affords parents and students over 18 years of age ("eligible students") certain rights with respect to their education records. These rights include:

- The right to inspect and review the student's education records within 45 days of the day the University receives a request for access. Students should submit to the registrar, dean, head of the academic department, or other appropriate official, written requests that identify the record(s) they wish to inspect. The University official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the University official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.
- The right to request the amendment of the student's education records that the student believes are inaccurate or misleading. Students may ask the University to amend a record that they believe is inaccurate or misleading. They should write the University official responsible for the record, clearly identify the part of the record they want changed, and specify why it is inaccurate or misleading. If the University decides not to amend the record as requested by the student, the University will notify the student of the decision and advise the student of his or her right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.
- The right to consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent. One exception that permits disclosure without consent is disclosure to school officials with legitimate educational interests. A school official is a person employed by the University in an administrative, supervisory, academic or research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the University has contracted (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility. Upon request, the University discloses education records without consent to officials of another school in which a student seeks or intends to enroll.
- The right to file a complaint with the U.S. Department of Education concerning alleged failures by State University to comply with the requirements of FERPA.

The Office's address is: Family Policy Compliance Office, U.S. Department of Education, Washington, D.C. 20202–4605.

Release of Student Information by Registrar

The following is the policy of the Office of the Registrar with respect to the release of student academic information:

1. Only the following information may be released to any outside source not officially connected to the State University of New York or one of its agents:
    a. Any information listed as "directory information" by the University.
    b. Dates of attendance
    c. If the student received a degree, and if so, which degree.
    d. Any office of the State University of New York or its agent may have released to it any information kept on a student on a "need-to-know" basis
    e. No further information will be released without the written consent of the student. Absolutely no transcript of students' records will be released outside the University without their signed authorization.

    The University, in accordance with FERPA, has designated the following information about students as public (directory) information:
    - Name
    - Address (local and permanent)
    - Academic Status (Undergraduate, Graduate, General Studies)
    - Dates of attendance
    - Degrees Completed

    Students have the right to have this directory information withheld from the public if they so desire. Each student who wants all directory information to be withheld (including items to be published in the Student Directory) shall so indicate by completing a Change of Information Form which can be obtained from the Office of the University Registrar or at the back of the Schedule of Classes for each semester. At least 10 days should be allowed for processing of these requests. The University receives many inquiries for "directory information" from a variety of sources, including friends, parents, relatives, prospective employers, other institutions of higher education, honor societies, licensing agencies, government agencies, and the news media. Each student is advised to carefully consider the consequences of a decision to withhold "directory information." The University, in all good faith, will not release directory information requested to be withheld, and any requests from persons or organizations outside the University will be refused unless the student provides written consent for the release.

    Prospective or current students may request a paper copy of information covered by the federal right-to-know legislation by sending a written request identifying each specific piece of information requested to:

RTK
Institutional Research, UAB321
University at Albany
1400 Washington Avenue
Albany, NY 12222

Appendix C

RULES GOVERNING ACCESS TO AND RELEASE OF STUDENT DATA

Family Educational Rights and Privacy Act Information

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education, and thus is applicable to the University at Albany. FERPA gives students certain rights with respect to their education records. There is nothing in the Act that is intended to restrict the use of student information by University officials in the normal exercise of their duties involving the educational interests of the student. **With very limited exceptions, student information, except for directory information described below, must not be transmitted by these officials to anyone outside the University without either the express written release by the stude**nt or pursuant to lawfully issued subpoena or other legal mandate. Release of records pursuant to subpoena or other legal mandate must be coordinated through the Office of University Counsel (442-5919).

Under FERPA:

- Students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for eligible students to review the records. Schools may charge a fee for copies. Students, however, must **NOT** be allowed access to:
    - Education records that contain information on more than one student (the student may review only the specific information about himself or herself);
    - Financial records of the student's parents;
    - Letters of recommendation or reference received after January 1, 1975 for which the right of inspection has been waived.
- Generally, schools must have written permission from the student in order to release any information from a student's education record. There are exceptions, including school officials with legitimate educational interest; other schools to which a student is transferring; specified officials for audit or evaluation purposes; in connection with financial aid to a student; to comply with a judicial order or lawfully issued subpoena; and by appropriate officials in cases of health and safety emergencies.

Schools may disclose, without consent, ONLY **"directory information."** However, schools must tell eligible students about directory information and allow students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify students annually of their rights under FERPA. The actual means of notification is left to the discretion of each school. The University at Albany, in accordance with FERPA, has designated the following information about students as **directory information**:

- Name
- Address (local and permanent)
- Academic Status (Undergraduate, Graduate, General Studies)
- Dates of attendance
- Degrees Completed

Students have the right to have this directory information withheld from the public if they so desire. Students who wish to have all directory information withheld (including items to be published in the Student Directory) shall so indicate in writing to the Office of the University Registrar. At least 10 days should be allowed for processing of these requests.

Parents should not be provided with information about students, including grades and grade point average, unless the student has expressly approved release of information to parents.

****

Student Records

Reference Chart: Release of Student Education Records Under the Family Educational Rights and Privacy Act

The following FERPA Reference Chart, which is reprinted here with the permission of the Campus Legal Information Clearing House at The Catholic University of America, is provided to assist you in complying with the Act's requirements.

Actions to be Taken by Record Custodian

REQUESTER	THE STUDENT REQUESTING HIS/HER OWN RECORDS	PARENT OR GUARDIAN	FACULTY OR OTHER SCHOOL OFFICIAL	OTHER PARTIES SEEKING INFORMATION
DEFINITION	Any person who attends or has attended the university.	Natural parent, guardian, or individual acting as parent in the absence of a parent or guardian.	University administrator, academic or research employee.	Includes media, courts, lawyers, educational authorities, lending institutions, educational agencies or institutions, and alleged victims of crimes of violence.
ASK TO SEE ID	Yes, check ID. Also, have student sign and date request form.	Check to verify that the student has provided 'release' to Registrar.	No, unless doubt as to the official's identity.	Yes, if release of record depends on identity/role.
VERIFY NEED TO KNOW	N/A	N/A	Yes, even for an official, verify their legitimate educational interest.	Yes, unless they have student's written permission.
CONSULT WITH UNIVERSITY COUNSEL	No, unless questions arise regarding the request.	No, unless questions arise regarding the request.	No, unless questions arise regarding the request.	Yes, for subpoenas, IRS summons or other legal process, or if it involves student disciplinary records.
OBTAIN WRITTEN PERMISSION FROM STUDENT	Yes, to the extent that the student is required to provide a signed request form.	Yes, unless student has provided release to University Registrar. Exception for under 21 student with alcohol/drug or legal violation.	Not necessary if official has a legitimate educational interest.	Yes, unless the request falls within exceptions to release of information or is directory information.
EXPLAIN RE-DISCLOSURE LIMITS	No	No	Yes	Yes
RECORD REQUEST & ACTION TAKEN IN STUDENT FILE	No	Yes	Keep a record in the student's file only when the request for access was denied.	Yes, unless written consent from student or directory information or subpoena prohibiting disclosure of the request to student.
MISCELLANEOUS	Student has no right to confidential letters of recommendation, confidential financial information of parents, or those items not defined as education records	Check to see if the student is a tax dependent of either parent. If the student has filed for federal financial aid, the Financial Office will have this information. Both parents have equal access, even if divorced/separated, unless a court order states otherwise.	Consult with supervisor or Registrar if doubt as to legitimate educational interest. Office of General Counsel can provide guidance.	For directory information, be sure to check whether student has requested non-disclosure of such information.

If record contains personally identifiable information on other students, delete that information before disclosing the record. Written consent must specify: 1) records to be disclosed; 2) purpose of disclosure; and 3) party or class of parties to whom disclosure may be made.

RULES GOVERNING ACCESS TO AND RELEASE OF EMPLOYEE DATA

New York State Personal Privacy Protection Law

- The Personal Privacy Protection Law (Public Officers Law, Article 6-A, sections 91-99) is intended to protect individual privacy by regulating the manner in which the state collects, maintains and disseminates personal information it maintains.

Protection of Privacy

Under the **Personal Privacy Protection Act**, State agencies may not disclose personal information about individuals, except under carefully defined circumstances. The Office of University Counsel should be consulted before any information about individual employees is released.

Use of Social Security Numbers

The Social Security Number ("SSN") is generally collected for use as an identifier for record keeping and matching purposes.

Federal Law

The Social Security Act protects as confidential, SSNs and related records that are obtained or maintained by authorized persons pursuant to any provision of law enacted on or after October 1, 1990 **and provides that they shall not be disclosed.**

State Law

In addition to federal restrictions on the disclosure of SSNs, New York State **Freedom of Information Law** and the **Personal Privacy Protection Law** prohibit the release of SSNs to the public unless specifically authorized, on the ground that such disclosure would result in an unwarranted invasion of personal privacy. However, State agencies may re-disclose SSNs collected directly from individuals to another governmental agency, but only to the extent permitted by the **Personal Privacy Protection Act** [See above]. Finally, section 2-b of the **Education Law** prohibits the display of any student's SSN to identify such student for the posting of grades or on class rosters or other lists provided to teachers.

The above are interpretative guidelines only. For clarification and further detail or any specific questions you may have, please contact either the Office of University Counsel or the University Registrar.

UNIVERSITY AT ALBANY
STATE UNIVERSITY OF NEW YORK

INTEGRATED ADMINISTRATIVE SYSTEM
ACCESS AND COMPLIANCE FORM

SUPERVISOR/ADMINISTRATOR:

My signature below certifies that the employees named below, who are under my supervision, require access to the University at Albany Integrated Administrative System (IAS) because such access is relevant and necessary in the ordinary course of performing their job duties at the University at Albany.

I understand my obligation to provide, and have so provided, information to this employee regarding the state and federal laws and University policies that govern access to and use of information contained in employee, applicant, and student records. I have also obtained a signed "Access and Compliance" form from these individuals.

EMPLOYEE:	DEPARTMENT
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

_____ _____
Supervisor Signature *Title*

_____ _____
Name (please print) ***Date***

EMPLOYEE ACCESS AND COMPLIANCE AGREEMENT

Required of all employees granted access to the IAS system

I certify that I have received and read the attached information regarding the state and federal laws and University policies that govern access to and use of personally identifiable information about employees, applicants, and students.

I understand that I am being granted access to student and employee information and data based on my agreement to comply with the following terms and conditions:

- **I will comply with the state and federal laws and University policies that govern access to and use of information about employees, applicants, and students.**

- **My right to access the University at Albany Integrated Administrative System (IAS) is strictly limited to the specific information and data that is relevant and necessary for me to perform my job-related duties.**

- **I am prohibited from accessing, using, copying or otherwise disseminating information or data that is not relevant and necessary for me to perform my job-related duties.**

- **I will maintain the privacy and confidentiality of the information and data that I access.**

- **I will share information or data only with those authorized to receive such information.**

- **I will sign off the IAS when I am not actively using it.**

- **I will keep my password(s) to myself, and will not disclose it/them to others.**

I understand that violations of this agreement may result in the revocation of my access privileges to the IAS, may result in appropriate administrative action, including, but not limited to, disciplinary action, and may also subject me to prosecution by state or federal authorities.

I certify that I have read this "Access and Compliance Form," and the attached information pertaining to access to and use of information contained in employee, applicant, and student records, that I understand both, and that I agree to comply with the above terms and conditions.

_____	_____	_____
Signature	Name (Please print)	Date

A. SUPERVISOR SIGNATURE

Consult with Dean or Vice President to determine if supervisor signature is required.

I certify that the above employee requires access to the student records system in order perform duties necessary to the employee's job.

_____	_____	_____
Signature	Department Title	Date

Appendix E

SAMPLE

Maintaining the Security, Confidentiality & Integrity of Customer Information

The University at Albany and its faculty and staff control access to rooms and file cabinets where paper records are kept.

- We lock doors to our office areas during non-business hours.
- Work areas where customer information is processed are behind locked doors.
- Guests are escorted in areas where customer information is being processed.
- Guests are restricted to areas that do not have customer information in plain view.
- File cabinets used to store customer information are secured in locked areas.
- The fireproof cabinets used to store promissory notes are locked during non-business hours.
- Documents no longer needed are disposed of in designated recycling/shredding containers.

The University at Albany and its faculty and staff control access to information stored electronically

- Workstations are behind locked doors.
- We minimize screens not in use, to prevent inadvertent breaches.
- Employees are encouraged to lock their workstations when not in use. However:
    - Tellers may not lock their workstations except for short breaks
    - Management covering the front line must have access to workstations
    - Tellers are encouraged to close their sessions and email when not in use.
- We use strong passwords, in accordance with ATN guidelines.
    - Network and email access (at least eight characters, alphanumeric, special character)
    - Mainframe access (at least eight characters, alphanumeric)
    - Second password for LMS & SIS
- We change passwords every ___days, in accordance with ATN guidelines.
- We do not post our passwords near or on our computers.

We protect our customers' information.

- We encrypt sensitive customer information when it is transmitted electronically over networks or stored online

- We respond to requests for customer information in accordance with FERPA.
- We refer to the appropriate security policies as needed to ensure our compliance.
- We report any fraudulent attempts to obtain customer information management, who then report the attempt to the appropriate law enforcement agencies.

Appendix F

University at Albany Policy for the Responsible Use of Information Technology

This policy was formulated to provide a secure and reliable computing environment at the University at Albany that will facilitate and encourage the exchange of ideas and information as well as protect the freedom of speech rights of the members of the University community. It establishes basic rights for all users and describes expectations for responsible use to ensure those rights.

I. General Principles

This section sets forth the ten basic policy principles. Situations or behaviors not specifically mentioned in sections II and III may be addressed through application of these basic principles.

II. User Rights and Responsibilities

This section highlights policy specifics related to privacy, copyright, software, harassment, defamation, accessing computing resources, abuse of computer resources, reporting unauthorized use, and the web.

III. System Administrator Rights and Responsibilities

This section describes system administrators and highlights specific expectations for system administrators, whether they be professional staff, faculty or student administrators.

Comments and suggestions regarding these policies may be sent to the Computer Usage Committee via email to the Committee Chair at LISC-CU@uamail.albany.edu.

III. General Principles

Access to modern information technology is essential to the University at Albany's mission of providing the students, faculty and staff with educational services of the highest quality. The pursuit and achievement of the mission of education, research, and public service require that the privilege of using computing systems and software, internal and external data networks, as well as access to the World Wide Web, be made available to the entire campus community.

The preservation of that privilege for the full community requires that each faculty member, staff member, student, and any other user comply with institutional and external policies for appropriate use. To assist and ensure such compliance, the University at Albany establishes the following policy which supplements all applicable SUNY wide policies, including sexual harassment, patent and copyright, and student and employee disciplinary policies, as well as applicable federal and state laws.

1. Use of University at Albany computing and network resources shall be consistent with: the education, research and public service mission of the State University of New York; all federal and state regulations; and this policy document.

2. This policy applies to all University at Albany computing and network resources, including host computer systems, campus-sponsored computers and workstations, software, data sets, and communications networks, whether accessed directly or indirectly.
3. This policy applies to all users of campus computing and network resources including faculty, staff, and students.
4. Information technology provides an important means for both public and private communication. Users and system administrators will respect the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers, graphics and television to the fullest extent possible under applicable law and policy. The principle of academic freedom will apply to public communication in all these forms.
   Specifically, the University respects freedom of expression in electronic communications on its computing and networking systems. Although this electronic speech has broad protections, all University community members are expected to use the information technology facilities considerately with the understanding that the electronic dissemination of information, particularly on the computing and networking systems, makes it accessible to a broad and diverse audience. The University expects all users to respect the Principles for a Just Community when communicating via the University information technology facilities.
5. Other than publicly designated official University sites, the University at Albany does not generally monitor or restrict content residing on campus systems or transported across its networks.
6. If there is reasonable cause to believe that a user has violated this responsible use policy, state or federal laws, or contractual obligations, the University reserves the right to take any of the following actions:
   - to have staff access the computer systems and networks including individual login sessions
   - limit an individual's access to its networks
   - remove or limit access to University computers and/or materials posted on University computers.
7. In the normal course of system maintenance, both preventive and troubleshooting, staff members operating the computer systems may be required to view files. Staff are required to maintain the confidentiality and privacy of information in such files unless otherwise required by law or University policy.
8. Campus servers and computing services should be properly configured so as not to pose a security risk or otherwise adversely affect existing University servers and services. All University system and network administrators are expected to implement practices to satisfy "due diligence" in respect to security requirements.
9. The University recognizes and acknowledges employee *incidental use* of its computing and network resources within the guidelines (see appendix) established for such use.
10. This policy may be supplemented with additional guidelines by units that operate their own computers or networks, e.g., University Libraries or ResNet, provided such guidelines are consistent with this policy.

II. User Rights and Responsibilities

1. **Privacy:** The University will make every effort to respect the privacy of an individual's computer files. Each user must respect the privacy and integrity of other computer users. No user should view, copy, alter or destroy another's personal electronic files without permission (unless authorized or required to do so by law or policy). Although users are prohibited from using computing resources to monitor electronic communications, all users should be aware that personal computer files are distributed on a public network which cannot guarantee absolute privacy or security.

2. **Copyright:** Original works of authorship and creative expressions that are more than ideas or facts and which are fixed in a tangible medium of expression (print, artwork, visual images, music, electronic materials) may be protected by copyright unless they are in the public domain. When duplicating copyrighted materials for educational use, it is advisable to secure the permission of the copyright holder in advance of the act of duplication.
3. **Software:** Most software that the University provides to its students, employees, and other users is licensed by the University, or third parties, and is protected by copyright and other laws, together with licenses and other contractual agreements. Users are required to respect and abide by the terms and conditions of software use and redistribution licenses. Such restrictions may include prohibitions against copying programs or data for use on the University network or for distribution outside the University; against the resale of data or programs, or the use of them for non-educational purposes or for financial gain outside of the academic mission; and against public disclosure of information about programs (e.g., source code) without the licensee's authorization.
   All University business will be conducted using legally licensed software. Managers are responsible for ensuring that only licensed software is installed on department computers. Managers are required to maintain documentation regarding purchases of software and conduct departmental self-audits to assure continued compliance with applicable agreements.

   University employees who knowingly and/or intentionally make, acquire or use illegal copies of computer software shall be considered to be acting outside the scope of their employment and as such may not be eligible for legal defense by the Office of the Attorney General under the Public Officers Law.
4. **Harassment, Defamation:** As in other aspects of behavior in campus life, civility is expected at all times. No user should, under any circumstances, use campus computers or the University network to harass any other person. Similarly, users may not use computing resources to defame, slander, or libel.
5. **Accessing Computing Resources:**
   This section outlines guidelines on the use of computer accounts, user room facilities, and the campus network. At all times, users are expected to practice reasonable conservation measures (such as regularly cleaning up their mail files and practicing efficient file management).

III. Accounts:

Computer and network access accounts are to be used for the University-related activities for which they are assigned.

- ***Sharing of access:*** Computer accounts, passwords, and other types of authorization are assigned to an "owner," who is then responsible for the account and all activities generated by the account.

- ***Unauthorized access:*** You may not run or otherwise configure software or hardware to allow access by unauthorized users.
- ***Termination of access:*** When you cease being a member of the campus community (e.g., withdraw, graduate, terminate employment, or otherwise leave the university), or if you are assigned a new position and/or responsibilities within the State University system, your access authorization must be reviewed. You must not use facilities, accounts, access codes, privileges or information for which you are not authorized in your new circumstances.

B. User Room Facilities

User rooms on campus are primarily provided for the use of the University at Albany community. User rooms are a limited communal resource, and, therefore, users must abide by certain restraints and courtesies, including all rules and guidelines posted in each facility. For example, the use of some programs may be limited to off-peak hours in the public facilities.

III. The Campus Network

The rules that govern the use of the University at Albany's network are based on the premise that the network is a communal resource. The people who use it agree to abide by certain restraints and courtesies. These are detailed in various documents, including the University's Community Rights and Responsibilities document, the ResNet Participants' Agreement incorporated into the Residence Hall License, and this policy.

6. **Abuse of Computer Resources:**

Abuse of campus computer resources is prohibited and includes, but is not limited to:

- ***Circumventing Security:*** Users are prohibited from attempting to circumvent or subvert any system's security measures. Users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.
- ***Breaching Security:*** Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized personnel of resources or access to any University at Albany computer or network is prohibited. Breach of security includes, but is not limited to, the following:
    - · Creating or knowingly propagating viruses.
    - · Hacking
    - · Password cracking
    - · Unauthorized viewing of other's files

- ***Chain Letters:*** The propagation of chain letters (e-mail requesting that the reader send on the message to multiple others) is prohibited. Virus hoax announcements generally fall in this category.
- ***Unauthorized Servers:*** Initiating and operating unauthorized servers (e.g., gaming, IRC, FTP, file sharing applications, e-mail) on University servers or systems, particularly those that extend University network and computing resources to non-affiliates of the University, is prohibited.
- ***Unauthorized Monitoring:*** A user may not use computing resources for unauthorized monitoring of electronic communications.
- ***Flooding/E-Mail Bombs:*** Sending massive e-mail in a deliberate attempt to overwhelm a system is prohibited.
- ***Private Commercial Purposes:*** The computing and networking resources of campus shall not be used for personal or private commercial purposes or for financial gain outside the academic mission.
- ***Violations of Copyright:*** Written permission from the copyright holder may be required to duplicate for educational use or any other purpose copyrighted material. This includes duplication of audio tapes, videotapes, photographs, illustrations, images, audio files, computer software, and all files or other information, whether in digital format or otherwise.
- ***Political Advertising or Campaigning:*** The use of campus computers and networks shall be in accordance with University policy on use of University facilities for political purposes (SUNY Administrative Procedures Manual Policy 008, See Appendix A.).

7. **Web Policy**
   This policy exists to help the creators of Web pages at the University at Albany take advantage of this powerful communications tool, yet avoid the pitfalls that can lead to confusion and complaints. Individual schools and colleges, as well as departments and programs, may have their own guidelines for publishing professional, organizational, and instructional web pages. However, these are supplemented and superseded by this University-wide policy.
   A. **Official Home Pages**
      i. The University at Albany home page is an official publication of the University. All materials, including text and photographs, appearing on the home page or subsequent official home pages of specific departments are copyrighted and may not be reproduced without written permission from the copyright holder.

      ii. Home pages linked to the University at Albany home page may be created by academic departments, programs, centers or institutes, governance groups, and administrative departments.

      iii. Official home pages are a reflection of the University. It is important for all contributors to ensure that their information is well-organized, accurate, and timely, and the web pages presentation complies with NYS Technology Policy 99-3: Universal Accessibility for NYS

Web Sites.

A primary contact person must be identified for the creation and maintenance of all official home pages. The contact is designated by the department or unit head. The contact for an official page must be a University at Albany faculty or staff member, and an email address for the contact person must be included on the organization main page. The contact person is responsible for periodically reviewing and updating the web page information.

iv. Recognized student groups may create home pages that are linked to the University at Albany home page with the approval of the Office of Student Life.
v. Developers of University at Albany official pages may include the University logo in its original form on the main page of the site; contact the Office of Media & Marketing for an original logo file.
vi. Subordinate official home pages must contain a path back to the home page of the University (http://www.albany.edu).

B. **Personal Home Pages**
   i. Personal home pages are posted without prior review by University administrators. Authors of web pages are expected to use good judgment with respect to the effect of their page content on the broad and diverse audience that accesses the University web site.
   ii. Personal pages may *not* contain any of the University at Albany logos or any other University copyrighted materials or images.
   iii. When individual or personal home pages are linked from official pages, the University requires that there be a clear and explicit indication at the point of transition from official to personal Webspace. This indication must explicitly state that any opinions, views or endorsements of any kind encountered on personal pages are not the policy of the University but are of a personal nature.
   iv. No material included in personal home pages may violate any laws, including but not limited to those regarding obscenity, harassment of others or copyright.
   v. Personal web pages may not be used for commercial purposes or financial gain outside of the academic mission.

8. **Limitations**
   A. The issuance of a password or other means of access is to assure appropriate confidentiality and does not guarantee privacy for personal or improper use of university equipment or facilities.
   B. The University at Albany provides reasonable security against intrusion and damage to files stored on the central facilities. The campus also provides some facilities for archiving and retrieving files specified by users, and for recovering files after accidental loss of data. However, the

campus is not responsible for unauthorized access by other users or for loss due to power failure, fire, floods, etc. The University at Albany makes no warranties with respect to Internet services, and it specifically assumes no responsibilities for the content of any advice or information received by a user through the use of the University at Albany's computer network or email systems.

C. Users should be aware that campus computer systems and networks may be subject to unauthorized access, tampering, or generation of fraudulent email messages.

III. System Administrator Rights and Responsibilities

System administrators are those individuals who directly support the integrity and operations of computing systems. As users of the system they administer, they have the same rights and responsibilities as any other user of the system including respect for the privacy of other users' information. In addition, they have a primary responsibility to ensure the availability, usefulness, integrity and security of the systems they manage. In this capacity their rights exceed those of other users of the systems. They generally have access rights that allow them the ability to read, write, or execute any/all files on the system(s) under their purview. Because of this, the professional ethics of system administrators must be at the highest level and their professional ethical conduct must be beyond reproach. The following itemizes specific rights and responsibilities of the system administrator.

1. **Adequate Hardware and Software:** Before any server is installed and placed on the campus network, the system administrator should ascertain that the machine is in an appropriate state to be placed on a shared network. The system administrator should also ascertain that the resource requirements (hardware and software) and system management requirements (people) for both current and future needs are either in place or planned for, to keep the machine in "top running order."
2. **Legal Licensing:** The system administrator must ensure that hardware and software products are installed consistent with license agreements.
3. **Monitoring:** The system administrator monitors for performance and capacity planning. The system administrator monitors to ensure that the system resources are not being misused. Multi-user systems are by definition and design shared resources. One user can either intentionally or inadvertently take over the system thereby rendering the resources unavailable for others. The system administrator is responsible for monitoring and interceding where needed to prevent misuse or misappropriation of system resources.
4. **Security Alerts and Updates:** The system administrator is responsible for monitoring sources of system alerts and for applying operating system and software product "patches" and security upgrades in a timely manner.
5. **Precautionary Scans:** System administrators must take precautions to safeguard systems against "corruption, compromise or destruction." This includes performing scans for diagnostic problem resolution purposes of the systems they maintain or assessing network traffic into or out of systems they maintain.

6. **Confidentiality and Privacy of User Files:** In the course of carrying out their duties, the system administrator must avoid viewing the contents of a user's files or messages. If such content becomes known to the system administrator, it should be treated as confidential and private.
7. **Security Breaches:** If the system administrator, in the performance of duties, uncovers information that indicates a breach of security has occurred, the system administrator must take action. System administrators cannot capriciously shut down user accounts, services, or systems. However, in those instances where a security incident is suspected that will endanger the security and integrity of both the system and the files and data of others, the system administrator may shut down specific accounts or close access to services or systems that appear to be associated with the problem. These may include possible perpetrators as well as victims of the security breach. Immediately after such an action, the system administrator should notify his or her supervisor and initiate appropriate review processes to follow up on such an action.
8. **Policy Violations and Criminal Activity:** If the system administrator, in the performance of duties, uncovers information that an individual is acting inconsistent with this policy, or discovers evidence of criminal activity, the system administrator must report such findings to the appropriate authority.

Sanctions and Reporting of Policy Violations

Violators of this policy are subject to the existing student or employee disciplinary procedures. Sanctions may include the loss of computing privileges. Illegal acts involving University at Albany computing and networking resources may also subject users to prosecution by state and federal authorities.

University employees learning of misuse of computing resources shall notify the appropriate supervisor, system manager, department manager, or area Vice President.

Appendix: Incidental Use of Information Technology

Incidental personal use of computing resources at the University at Albany is an exception to the general prohibition against the use of University equipment for anything other than official state business.

The parameters of the exception are:

- the incidental personal use of computing resources facilitates the user's proficiency; or
- there is no additional cost to the state; or
- an analogy to incidental use of telephones can be made; or
- an analogy to personal use of library resources can be made.

Incidental personal use must not:

- result in financial gain for the user;
- be for business purposes where the business is owned by the employee or the work is done for another business (including consulting); faculty/staff who do extensive paid consulting are expected to obtain services through an Internet Service Provider that handles the bulk of such correspondence and associated research.
- interfere with assigned job responsibilities; or

- be in violation of existing security/access rules.

This policy was developed by the Computer Usage Committee of the University at Albany's University Senate's Council on Libraries and Information Systems (LISC). The policy was approved by LISC on December 4, 2000 and by the University Senate on December 11, 2000. The Computer Usage Committee continues to meet regularly to execute its responsibilities of continual review, development, and maintenance of the University at Albany computer usage policies.
The development of this policy was expedited by the extant policies of several other institutions including the University at Buffalo, the State University of New York at Stony Brook, Cornell University, University of Texas, SAGE (the Systems Administrator Guild Special Technical Group of USENIX), University of Hawaii, Georgetown University, Rensselaer Polytechnic Institute, Pennsylvania State, Rochester Institute of Technology, and Auburn University.

Appendix G

Sample Office Safeguarding Practices

Appendix H

Policies Governing Student Use Of Computing and Networking Facilities at the University at Albany

As a member of the University community, you are given the privilege of using the computing facilities administered by Computing and Network Services.
While the use of computers, electronic information and computer networks is important for research, instruction, and administration within the academic community, use of the University computing and network is a privilege that comes with the responsibility for appropriate usage. Because the electronic environment is easily disrupted and electronic information is readily reproduced, respect for the work and rights of others is especially important. Therefore the University establishes the following policy to ensure respect for the work and rights of all members of the University community which supplements all applicable University policies and federal, state and local laws.
Any behavior with respect to the electronic environment that interferes with the mission or legitimate activities of the University or its members will be regarded as unethical and may lead to disciplinary action under standard rules for misconduct and existing disciplinary procedures defined in Community Rights and Responsibilities, and may lead to the suspension or loss of computing privileges. In addition, conduct which violates criminal codes, or local, state or federal laws may result in criminal prosecution and University judicial review and disciplinary action. The following activities are examples, but not an exhaustive list, of activities prohibited with respect to the University's electronic environment:

1. Lending computing user ID or account to another person.
2. Using a computer user ID or account assigned to another person.
3. Compromising the privacy of electronic networks or information systems.
4. Damaging or destroying the integrity of electronic information or computer hardware or software.
5. Attempting to interfere with, or disrupt the use of electronic networks, information systems or the legitimate work of another user.
6. Attempting to circumvent system or network security.
7. Attempting to access the computer files belonging to another user without permission.
8. Sending messages that cause an interruption in the work of others.
9. Chain letters.
10. E-mail bombs.
11. Using computing or network facilities to harass or intimidate any other person or group.
12. Using University computing/network facilities for personal profit.
13. Unauthorized copying and, or distribution of software or other intellectual work such as music, images, logos and speeches. All proprietary computer software is legally protected by copyright, patent, or trade secret law.
14. Misrepresenting the ownership or source of files and messages.

15. Providing unauthorized users with access to University systems and resources, or assisting unauthorized users in accessing University systems and resources.
16. Abusing specific computer and network resources, as described in other University documents.

Home Pages and Electronic Mail

The University at Albany World Wide Web Home Page is an official publication of the University at Albany. Personal Home Pages residing on University owned systems or served through the University network are permitted but shall include the disclaimer that the University at Albany does not monitor, review, or endorse the personal Home Pages or link identifiers of personal Home Pages residing in the University domain. The University is not responsible for the contents of personal Home Pages or electronic mail communications. Views and opinions expressed in e-mail or on personal Home Pages are strictly those of the authors.

CONSERVE RESOURCES

As a computer user, you are expected to conserve system resources. Everything you do on the system uses a portion of limited, shared resources, including printers, processor time, and communications ports. Disk storage and machine cycles are exhaustible and should not be wasted.

Appendix I

ResNet Policies

ResNet Policies can be found on the University at Albany website at:

http://www.resnet.albany.edu

Appendix J

SERVICE PROVIDERS UNDER THE FTC SAFEGUARDS RULE

A service provider is defined in the Safeguards Rule "as any person or entity that receives, maintains, processes or otherwise is permitted access to customer information through its provision of services directly to a financial institution." (16 CFR §314.2(d)). Campuses must require service providers by contract to implement and maintain safeguards of nonpublic personal information they possess. Although subcontractors of a service provider are not required to maintain their own safeguards, the FTC has cautioned that a service provider should address the practices of its subcontractors and their employees in implementing its required safeguarding measures.

Relevant contracts that campuses have entered into after **June 24, 2002** with service providers must include the required safeguarding provision. Contracts entered into before **June 24, 2002** will be interpreted as having such language, whether they do or not, provided all such contracts are amended by **May 24, 2004** to explicitly include that language

Language For Service Provider Contracts:

In performing this contract you will receive, maintain, process or otherwise will have access to confidential information on students and/or customers of (Name of Campus). Pursuant to the Gramm-Leach-Bliley Act (P.L. 106-102) and the Federal Trade Commission's Safeguards Rule (16 CFR Part 314), you must implement and maintain a written Information Security Program in order to protect such customer information. Customer information is defined in relevant part under the Safeguards Rule as "any record containing nonpublic personal information as defined in 16 CFR §313(n)" (the FTC's Privacy Rule) "about a customer of a financial institution, whether in paper, electronic, or other form" (16 CFR §314.2). Examples of nonpublic personal customer information include, but are not limited to, name, address, phone number, social security number, bank and credit card account numbers and student identification numbers.

The safeguards that you implement under the Program must comply with the elements set forth in 16 CFR §314.4 and must achieve the objectives enunciated in 16 CFR §314.3, namely to: 1) insure the security and confidentiality of student and/or campus

customer records and information; 2) protect against any anticipated threats or hazards to the security or integrity of such records; and 3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any student and/or campus customer.

If you subcontract with a third party for any of the services that you are required to undertake in furtherance of this contract, you must ensure that such third parties implement practices, which protect nonpublic personal information of students and/or campus customers with which they receive, maintain, process or otherwise are permitted access.

You are required to (return) or (destroy) (Campus to choose method) all customer information in your possession upon your completion of this contract. Furthermore, the safeguarding requirements set forth above shall survive termination of this contract.

Appendix K

HELPFUL RESOURCES

Statute and Regulations:

FTC Privacy Rule can be accessed at http://www.ftc.gov/os/2000/05/65fr33645.pdf

FTC Safeguards Rule can be accessed at http://www.ftc.gov/os/2002/05/67fr36585.pdf

Text of Title V of the GLB can be accessed at
http://www.ftc.gov/privacy/glbact/glbsub1.htm (Subtitle A)
http://www.ftc.gov/privacy/glbact/glbsub2.htm (Subtitle B)

Other Resources:

Campus Legal Information Clearinghouse (CUA OGC web page on Gramm-Leach-Bliley) http://counsel.cua.edu/fedlaw/glb.cfm (updates and sample policies will be posted here as they become available)

Helpful FTC links:
http://www.ftc.gov/privacy/glbact/index.html
http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm (includes practices that might be considered in developing an Information Security Program)
http://www.ftc.gov/privacy/glbact/glboutline.pdf

System Administration, Networking and Security Institute (SANS) http://www.sans.org
http://www.sans.org/rr/legal/gramm.php

International Association of Privacy Professionals
http://www.privacyassociation.org/

http://www.nacubo.org/nacubo_reports/
Compliance with GLB NACUBO Jan. 13, 2003 report
http://www.nacubo.org/public_policy/
Click on “Information Security Template” to see a Model Information Security Program