The State University of New York at SUNY Fredonia
Information Security Program
Adopted by the President's Cabinet on June 2, 2004

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. Designated representatives from Offices of ITS and Internal Control shall coordinate the Information Security Program.

B. The Program includes input from other SUNY at Fredonia departments, including Human Resources, Admissions, Financial Aid, Student Accounts, Registrar, Faculty Student Association, Internal Control, Payroll Services, College Services, University Advancement and Foundation, Residence Life, and the Banner SIS Security Committee.

C. The Program will be reviewed and evaluated annually, during the month of May. Selected aspects will be tested. 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:

Employee Management & Training
Information Systems
Managing System Failures
Service providers

III. Appendices

A. Legal References
B. FERPA Policy at http://www.ed.gov/policy/gen/reg/ferpa/index.html
C. Federal Work Study Manual located in SUNY Fredonia Financial Aid Office, 215 Maytum Hall
D. Social Engineering Security Policy
E. Student Employee Security Responsibility and Confidentiality Agreement
F. State Employee Confidentiality Agreement
G. Physical Information Security Policy
H. Electronic Information Security Policy
I. Telephone and Fax Security Policy

PROGRAM DETAILS

I. Designated Information Security Program Coordinators

A. Representatives

Karen S. Klose Associate Vice President for ITS 712 Maytum Hall SUNY College at Fredonia Fredonia, NY 14063 (716) 673-4670	Jennifer Burke Internal Control Coordinator 502 Maytum Hall SUNY College at Fredonia Fredonia, NY 14063 (716) 673-4761

B. Offices Possessing Customer Information

The following have been identified as among the relevant offices to be considered when assessing the risks to customer information: Human Resources, Admissions, Financial Aid, Student Accounts, Registrar, Faculty Student Association, Internal Control, Payroll Services, College Services, University Advancement and Foundation, Residence Life, and the Banner SIS

Security Committee. Each relevant area is responsible to secure customer information in accordance with all relevant privacy guidelines.

C. Offices Having Responsibility in Safeguarding Customer Information
Human Resources, Admissions, Financial Aid, Student Accounts, Registrar, Faculty Student Association, Internal Control, Payroll Services, College Services, University Advancement and Foundation, Residence Life, and the Banner SIS Security Committee.

II. Risk Assessment & Safeguards

A. Definitions

Covered data and information for the purpose of this policy includes student and other customer financial information are 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. This includes permanent and temporary state and student employees, whose job duties require them to access customer information or work in a location where there is access to customer information.

1. Hiring Employees
SUNY Fredonia exercises great care in trying to select well-qualified employees. Hiring supervisors review applications, carry out interviews, check references, and verify educational credentials before making their final selection. Recruitment policies and procedures are available at http://www.fredonia.edu/aaoffice/index.htm.

2. Work Study and Temporary Service Student Employees
Work-Study students are assigned by the Office of Financial Aid, and must comply with the Federal Work Study Manual (see appendix C.). Confidentiality and safeguarding of information is covered by each hiring office during an individual orientation session conducted by the first day of

work. All student employees and supervisors sign the ”Security Responsibility and Confidentiality Agreement” (Appendix E.), during the orientation session. One copy is retained in the employee’s office, and one copy is retained by Payroll Services. Once e-sign is instituted, the electronic agreement will be maintained in the Campus Information System (CIS).

3. State Employees (Permanent, Term, Part-time, Graduate Assistants)

All employees take part in Information Security and FERPA training at the time of new employee orientation. In addition, the ITS Help Desk Coordinator includes FERPA requirements during Basic Banner Navigation Training and administrative offices review FERPA during student records orientation.

All employees receive a copy of the Information Security Policy Documents (Appendices D-I of the SUNY Fredonia Information Security Program), which includes the Social Engineering and Telephone/Fax Security Policies, and sign a “Confidentiality Agreement” form (Appendix F). The Confidentiality Agreement form is maintained by the Office of Human Resources in each employee file.

Once e-sign is instituted, the electronic agreement will be maintained in the Campus Information System (CIS).

4. Ongoing Training

"The Information Security Program and Policies will be available as a link from the Human Resources website. In addition, Human Resources will annually send a confidentiality and FERPA regulation reminder via e-mail to all state employees."

5. Access to Customer Information

Only employees whose job duties require them to access customer information shall have access.

6. Disciplinary Measures for Breaches

Breaches of information security may result in appropriate disciplinary action by the immediate supervisor depending upon the nature and severity of the breach. All accidental breaches should be reported and rectified as soon as possible. Employees are encouraged to report any suspected intentional and/or malicious breaches. Human Resources will be notified of any breach of information security by state employees. State employees may be subjected to disciplinary actions for the violation

of this policy. Student breaches will be dealt with by the immediate supervisor and abuse flagged by the Office of Student Payroll.

C. Information Systems

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

1. Paper Storage Systems

Access and handling safeguards are outlined in the Physical Information Security Policy, appendix F. The Office of Internal Control maintains the Record Retention policy.

2. Computer Information Systems

The Office of Computing Services in ITS serves as the central electronic information security office and as such provides or terminates access based on employee status information from Human Resources. Access to the Campus Information System (CIS) is determined by position description with roles and access maintained by the Database Administrator. Access to employee data is maintained by SUNY System Administration. Desktop connection to the Internet is accomplished via static IP, allowing ITS intervention as necessary in the event of network security breaches. Additionally, the network administration tool tracks network connections by desktop hardware address.

Electronic security safeguards are outlined in the Electronic Information Security Policy, appendix G.

3. Customer Information Disposal

SUNY Fredonia provides for confidential disposal of documents through its Office of College Services. Obsolete confidential documents are placed in recycling containers or are tagged for shredding in secure areas and marked confidential before being transferred to the recycling/shredding center. Two paper shredders are available for use in the Thompson Copy Center and Fenton Hall copy room. Offices disposing of confidential documents must notify the Internal Control Officer, as logs of disposal must be maintained.

(Or, campus contracts with an outside agency to perform the above service. The outside contractor does provide secure recycling containers.)

SUNY Fredonia erases all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information. (Computers swapped to new owners are completely re-formatted following old user's sign-off.

Computers designated as obsolete equipment are wiped clean by AIT personnel following procedure created in conjunction with Office of College Services.)

SUNY Fredonia archives customer transaction information as necessary.

SUNY Fredonia disposes of obsolete customer information in accordance with applicable records retention policies (maintained by the Office of Internal Control).

D. Managing System Failures

1. Written Contingency Plans—in development

2. Centralized Protection from E-Invasion

SUNY Fredonia has implemented a tiered approach to protect from e-invasion that incorporates port blocking at the network firewall level, intrusion detection management, regular application of patches and upgrades, and managed antivirus protection at the e-mail gateway and desktop levels. Protection from e-invasion is dependent on timely definition updates and alerts from numerous advisory agencies (e.g. CERT, Infragard, Microsoft, SUNY System Administration, and SANS Institute), as well as educated and cautious computer users.

3. System Back-ups

Systems and databases controlled by ITS are backed up to tape on a daily basis Monday-Friday and stored in a fireproof vault with a 1500 4-hour rating (internal temperature remains below 125 degrees for 4 hours in a 1500 degree fire). Tapes are moved to an off-site location on a monthly basis.

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.

E. Service Providers

1. Contracts

All contracts with service providers are reviewed by the Office of University 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 cannot maintain appropriate safeguards.

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, Alumni Associations

3. Monitoring

SUNY Fredonia will periodically evaluate providers to ensure that they have complied with the information security requirements of the contract.

Appendices

A. Legal References

1. 15 USC, Subchapter I, sec. 6801-6809 (Gramm-Leach-Bliley Act)
2. 16 CFR, Part 313 (Privacy Regulations, see reference to FERPA)
3. 20 USC, Chapter 31, 1232g (FERPA)
4. 34 CFR, part 99 (FERPA regulations)
5. 16 CFR, part 314 (Safeguard Regulations, as published in the Federal Register, 5/23/02)
6. NACUBO Advisory Report 2003-01, issued 1/13/03
7. FTC Facts for Business: *Financial Institutions and Customer Data: Complying with the Safeguards Rule,* published September 2002.

B. FERPA Policy
http://www.ed.gov/policy/gen/reg/ferpa/index.html

C. Federal Work Study Manual, see SUNY Fredonia Financial Aid Office

D. Social Engineering Security Policy

E. Student Employee Security Responsibilities and Confidentiality Agreement

F. State Employee Confidentiality Agreement

G. Physical Information Security Policy

H. Electronic Information Security Policy

I. Telephone and Fax Security Policy

Appendix D.

SOCIAL ENGINEERING SECURITY POLICY

The purpose of this policy is to emphasize that information security (the protection of confidentiality and the integrity of confidential student and employee information) is the responsibility of each and every SUNY employee. "Social Engineering" is the term that describes non-technical ways by which hackers obtain information, usually by fooling people into giving up their own security.

Policy

It is the policy of SUNY Fredonia to ensure confidential physical information is protected.

Procedure

The following guidelines should be followed:

- Include the review of FERPA regulation and the SUNY Fredonia Information Security Program and Policies during new employee orientation, with the policies included in orientation packets.
- Require completion of the Confidentiality Agreement Form, appendix E of the SUNY Fredonia Information Security Program.
- During annual evaluations, supervisor and employee shall review information security confidentiality requirements and procedures.
- The Office of Human Resources will annually remind employees of information security and FERPA regulations.
- Eliminate use of social security number for customer identification in campus-wide office procedures. Use the Your Connection ID when verifying customer identification.
- Practice vigilance in how and where each employee shares information. Hackers can overhear conversations and build up information over time that can then be used to obtain confidential information.
- Never write passwords down, or share with anyone (even system administrators, account managers, or friends). Most cases of unauthorized access to information is through the use of compromised passwords. Use of strong passwords following the guidelines in appendix G. is recommended.

Prepared by: Karen Klose, SUNY Fredonia
Reviewed by: President's Cabinet
Adopted on: 6/02/2004
Revision dates: 6/02/2004

Appendix E.

STUDENT EMPLOYEE

SECURITY RESPONSIBILITY AND CONFIDENTIALITY AGREEMENT

The information contained in the various databases and print files used by SUNY at Fredonia is confidential in nature and is only to be used in connection with University, SUNY, and State business following the SUNY Fredonia Information Security Program and the Family Educational Rights and Privacy Act of 1974 (FERPA) regulations. Access to the data is granted to selected offices with the understanding that the information and any reports generated from the system will be accessible only to appropriate personnel for legitimate business purposes.

As an employee of the State University of New York at Fredonia, I recognize that I may have access to or be required to handle certain information that is confidential, private, and proprietary for the performance of my duties.

I am aware that:

- Data should be accessed and made available only to authorized persons for College business by authorized departmental personnel following approved departmental procedures;
- Assigned functional capabilities (user codes, access to equipment, data or restricted areas) are to be used **ONLY** to perform my assigned duties;
- Any breach of confidentiality or abuse of my position will result in dismissal from my job and possible judicial action.

I agree to follow departmental policies and procedures with respect to confidentiality of records, equipment, user codes and general practices as outlined by my employer, and recognize that failure to do so will be grounds for disciplinary action by SUNY at Fredonia Judicial Office for violations to the Student Code of Conduct.

I have discussed this policy with my immediate supervisor.

Employee Printed Name

_____ _____

Employee Signature Date

_____ _____

Supervisor Signature Date

This signed form should be forwarded to Payroll Services, Maytum Hall, with a copy retained in the employee's hiring department personnel file.

Prepared by: Banner Security Committee, SUNY Fredonia
Revised by: Karen Klose, SUNY Fredonia
Reviewed by: President's Cabinet
Adopted on: 6/02/2004
Revision dates: 6/02/2004

Appendix F.

STATE EMPLOYEE

CONFIDENTIALITY AGREEMENT

The information contained in the various databases and print files used by SUNY Fredonia is confidential in nature and is only to be used in connection with University, SUNY, and State business following the SUNY Fredonia Information Security Program and FERPA regulations. Access to the data is granted to selected offices with the understanding that the information and any reports generated from the system will be accessible only to appropriate personnel for legitimate business purposes.

As an employee of the State University of New York at Fredonia, I recognize that I may have access to or be required to handle certain information that is confidential, private, and proprietary for the performance of my duties.

I am aware that personal information not included in a public directory, such as social security number, date of birth, disability status, bank account #, or other such information may not be released to any individuals outside the office to which access has been granted without the express permission of the Director of the particular area. Failure to maintain confidentiality or misuse of the information contained in the system may subject an employee to discipline up to and including termination

As an employee of SUNY Fredonia, I hereby understand and agree to abide by the above confidentiality statement.

_____
Printed Employee Name

_____
Employee Signature

_____
Signature Date

Prepared by: Michael Daley, SUNY Fredonia
Revised by: Karen Klose, SUNY Fredonia
Reviewed by: President's Cabinet
Adopted on: 6/02/2004
Revision dates: 6/02/2004

Appendix G.

PHYSICAL INFORMATION SECURITY POLICY

The purpose of this policy is to protect the security of physical information and to protect the confidentiality and integrity of confidential student and employee information.

Policy

It is the policy of SUNY Fredonia to ensure confidential physical information is protected. In addition, physical assets that provide access to confidential information must be secure.

Procedure

The following guidelines should be followed when maintaining physical information.

- File cabinets containing confidential information must be locked or in an area that can be secured from the public.
- Fireproof cabinets used to store promissory notes are locked during non-business hours.
- Confidential information should not be left on desks or open areas accessible to the public. This includes but is not limited to paper, floppy disks or CD's.
- Private or confidential information should not be discussed in person or over the phone where it can be overheard. Where confidentiality/privacy is required, special accommodations will be made.
- All mobile devices, including PDA's and laptops, will be password protected.
- All confidential information no longer needed must be properly destroyed (i.e., crosscut shredded) so as to ensure its confidentiality. (Office of Internal Control maintains the Record Retention policy.)
- Idle-time implementation for Banner forms access is in review by the Banner Security Committee. Idle-time, if activated, would end a work session after a specific amount of "idle" time.
- Database and system logoffs are required whenever the user is away from the computer desktop for an extended period of time.
- Computer screens should not be visible to the public and will utilize a password protected screen saver. Desktop locking instructions for Windows and Macintosh users are located on the ITS website.

Prepared by:	Deborah Putnam, Director of Computing Services/Informational Technology Security Officer at Alfred State College
Adopted w/revisions by:	Karen Klose, SUNY Fredonia
Reviewed by:	President's Cabinet
Adopted on:	6/02/2004
Revision dates:	6/02/2004

Appendix H.

ELECTRONIC INFORMATION SECURITY POLICY

The purpose of the policy/procedure is to protect the security of electronic information and to protect the confidentiality and integrity of confidential information. All individuals who are authorized to use the e-mail systems of SUNY Fredonia must be familiar and compliant with this policy.

POLICY/PROCEDURE STATEMENT

No Right to Privacy

Email

SUNY Fredonia encourages the business use of e-mail for the efficiency of operations. The e-mail system and all the messages generated by e-mail, including backup copies, are part of the business infrastructure of SUNY Fredonia, are owned by SUNY Fredonia, and are not the property of the individuals who use the system.

Right to Monitor, Audit, Read

In keeping with provisions outlined in the SUNY Fredonia Computer and Network Usage Policy, SUNY Fredonia reserves the right to monitor, audit, and read e-mail messages.

Request for Confidential Information

The transmission of an individual's own personal information via electronic mail (e-mail) to an external network is permitted only when the requester has been advised of the campus e-mail policy stating "SUNY Fredonia cannot guarantee that electronic communications will be private." If, after advisement, the requester agrees, the personal information may be e-mailed.

The transmission of confidential information requested by another individual (other than self) via electronic mail is not permitted to off-campus locations.

On-campus electronic mail transmission are reasonably secure, due to the higher level of security provided by switched network interfaces and the dual-level anti-virus security built into the SUNY Fredonia e-mail gateway and managed anti-virus desktop systems, as well as user compliance with the Physical Information Security Policy.

The transmission of confidential health information via electronic mail (e-mail) is not permitted.

Websites

Sites, such as Banner, that accept confidential information input must be password protected and allow for encryption/secure communications. The servers hosting confidential information must be protected with SSL (Secure Sockets Layer) certificates, such as Verisign.

Confidentiality and Information Security

- All provisions of the SUNY Fredonia Computer and Network Usage Policy must be observed with regard to access, use, modification, creation, disclosure, storage, copying,

transmission, or destruction of information in any way related to online communications or interactions.

- Access to and disclosure of online confidential information is subject to the same restrictions that apply to non-electronic campus records.

File Transfer Protocol (FTP)

Transferring information to an external third party such as New York State Higher Education Services Corporation, the Federal Government, M&T Bank, and Standard Register, among others, will always utilize an encrypted and secure transmission method either outlined by Information Technology Services (ITS) or specified by the provider and approved by ITS.

Passwords

Passwords are access keys, help to prove you are who you say you are, and help to ensure your privacy. Compromised passwords provide access to systems for unauthorized personnel. For that reason, SUNY Fredonia computer users are encouraged to create and use strong passwords in accordance with the following password integrity guidelines:

- Initial password is randomly generated and displayed for each user in the secured "Your Connection" web interface. This interface is secured with a PIN that is specific to each new user.
- Your Connection PIN change is forced after initial login. User may change initial password if desired following the guidelines below.
- Use at least seven characters whenever possible.
- NOT ALLOWED to use any portion of user's first name, last name, or userid.
- A mixture of three of the following is required: English uppercase characters, English lowercase characters, base 10 digits (0-9), non-alphanumeric characters (!,$,#,%).
- Make password easy to remember but difficult for someone to guess. Do not reveal yourself in developing a password (don't use social security number, birth date for yourself or a significant individual in your life, address or telephone number). Using a "pass phrase" is a good way to develop a password. This example of using the pass phrase "Do you know the way to San Jose?" to develop the password D!Y!KtwTSJ? comes from the Duke University guidelines.
- Never share your password (this includes system administrators, account managers, and friends). Never provide access to systems for other individuals using your logon identity.
- Never write your password down.
- Change your password if you have shared it with anyone else or if you wrote it anywhere. It is also advisable to change the password if you logged into the Fredonia system from a remote location without using an encrypted login program.
- Password aging is the act of changing a password on a regular basis and is required for users logging into the Campus Information System (CIS) forms or Dec Alpha hardware due to the confidential nature of data stored in this system. (As recommended by the Banner Steering Committee following review of state audit guidelines.) Password aging is recommended but not forced for all other access to Fredonia electronic resources.

Prepared by:	Deborah Putnam, Director of Computing Services/Information Technology Security Officer at Alfred State College
Adopted w/revisions by:	Karen Klose, SUNY Fredonia
Reviewed by:	President's Cabinet
Adopted on:	6/02/2004
Revision dates:	6/02/2004

Appendix I.

TELEPHONE AND FAX SECURITY POLICY

To establish a policy and procedure for transmission of protected information via telephone or fax machine that complies with Federal and State regulations.

POLICY

It is the policy of SUNY Fredonia to protect the confidentiality and integrity of student, employee, and campus private information as required by State and Federal law, union contracts, professional ethics and accreditation agencies. This policy applies to both internal and external telephone requests for confidential information.

Circumstances- The following circumstances outline when information may be released via telephone, following verification of the caller's identity.

- Situation where the original results or mailed copy will not meet the immediate needs of the requester.
- For internal requests, during system downtime, when information cannot be accessed via the computer systems.
- Only the Offices of Student Accounts and Financial Aid will disclose information to parents, and in those offices only financial information will be discussed.

Verification of Identity- The identity of the internal or external individual requesting information and the authority of the individual to have access to the information, if unknown, must be verified.

- Students will provide their Your Connection ID.
- Employees will identify themselves by name, title, department, home address, and home telephone number. Personnel will verify the information in the most recent publication of the Faculty/Staff Directory or through the Human Resources Office.
- Parents will provide their son or daughter's date of birth, Fredonia ID, or other verifiable identifying information. (OFFICE OF STUDENT AFFAIRS IS VERIFYING THIS.)
- If the request is from an external organization (i.e., financial institution, government office, police department), the requestor should be informed that the request for confidential information must be documented on official agency letterhead and faxed using SUNY Fredonia's fax policy to the appropriate number.
- Requestors deemed unauthorized to receive confidential information will be directed to the Vice President for Student Affairs for further review of the request.

Sensitive Information- Personnel should not disclose sensitive information via telephone unless the conditions stated above (circumstances and verification of identity) and requirements under the Family Educational Rights and Privacy Act are met. Examples of sensitive information include, but are not limited to:

- Health information
- Academic grades or assessments
- Financial information
- Social Security number

In cases where students have restricted their directory information, no information related to that individual may be released.

Voice/Answering Machines

- Protected information shall not be left on voicemail/answering machines.

Fax Machines

The following guidelines should be followed when faxing information.

- Place fax machines in areas with less traffic. Fax machines should not be placed in public areas where there is faculty, staff, or student traffic.
- A confidential fax cover sheet should be used indicating "Confidential Information Enclosed".
- A warning should be placed on the bottom of the fax cover sheet. "Important Warning: This message is intended for the use of the person or entity to which it is addressed and may contain information that is privileged and confidential, the disclosure of which is governed by applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this information is strictly prohibited. If you have received this message by error, please notify us immediately and destroy related message."
- Make sure the fax cover sheet includes: Date and time, sender's name, authorized recipient's name, number of pages transmitted, information regarding verification of receipt.
- Make sure the fax transmittal has received the proper authorization.
- Limit the faxing of confidential information to urgent or non-routine situations when mail or other delivery is not feasible.
- Regularly empty the fax tray so confidential information does not remain exposed on the fax machine for long periods of time.
- Confirm the accuracy of fax numbers. All commonly used fax numbers should be programmed into the fax machine to prevent misdialed numbers.
- Verify confirmations of outgoing faxes to prevent information being sent to the incorrect recipient.
- In the event of a misdirected fax, ensure improperly faxed documents are either immediately returned or destroyed by the recipient.

Prepared by: Deborah Putnam, Director of Computing Services/Informational Technology Security Officer at Alfred State College
Revised by: Karen Klose, SUNY Fredonia
Reviewed by: President's Cabinet
Adopted on: 6/02/2004
Revision dates: 6/02/2004