Fayette Institute of Technology Information Security Plan

Program Adoption
The Fayette Institute of Technology developed this Information Security Plan pursuant to the Federal Trade Commission's Safeguards Rule, from the Financial Services Moderation Act of 1999 (the Gramm-Leach-Bliley Act).

Purpose
The purpose of this plan is to establish an Information Security Plan designed to protect student information. The plan includes reasonable procedures to:

1. Designate one or more employees to coordinate the safeguards;
2. Identify and assess the risks to student information in each relevant area and evaluate the effectiveness of the current safeguards;
3. Define the safeguards program, and regularly monitor and test it;
4. Select appropriate service providers and contract with them to implement safeguards;
5. Ensure the plan is regularly monitored and tested to reflect changes in academic and financial practices, or as the result of testing and monitoring of safeguards.

The plan shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Definitions

Student Information is typically gathered in connection with obtaining federal/state/local financial assistance and enrollment in one of our academic programs to include names, demographic data, addresses, phone numbers, income and credit histories, and Social Security numbers.

Relevant Areas

The following have been identified as relevant areas to be considered when assessing the risks to student information:

Information Technology Services
Student Financial Aid Office
Student Financial Services Office

Identification of Risks
The following risks have been identified:

1. Documents containing personal information are accessed by unauthorized individuals;
2. Documents containing personal information are stolen;
3. Electronic data bases containing personal information are accessed by unauthorized individuals;
4. Personal information stored in an electronic format is stolen (i.e. laptop; disc).

Safeguards

Employee Management and Training

Adherence to FERPA laws is central to this plan; the Financial Aid office will provide guidance in complying with all FERPA regulations.

- Fayette County Schools will check references prior to hiring employees who will have access to student information;
- Require all employees to complete FERPA training to ensure they understand confidentiality and security standards for handling student information;
- FIT has written policies for securing electronic and paper files. Each relevant area will be trained on and will follow school policy. We recognize data may also exist in areas that are not official repositories of student data and that security of student data is the responsibility of every department. Accordingly, we will train staff in all departments on this policy.
- Employees at FIT should be mindful of their responsibility to maintain and ensure the security and confidentiality of documents that relate to students. This includes documents that involve class work, financial transactions, grades, enrollment status, and other confidential activities that may transpire. The following guidelines should be adhered to, as closely as possible, in all departments and offices at the school that retain student records:
    1. Paper records should be stored in an area that is secure and not accessible to unauthorized individuals;
    2. Each office or department should specifically determine individuals who have authorized access to files, filing cabinets and student records;
    3. Unauthorized access to records should be reported immediately to a supervisor;
    4. If records cannot be secured in a separate room or locked office, locking filing cabinets should be used and locked when unattended;
    5. File storage areas should be protected against destruction or potential damage from physical hazards, like fire or floods;
    6. Official records or reports, or copies thereof, may not be removed from an office where it is maintained except in the performance of a person's duties;
    7. Documents and files, especially with confidential information, should not be left in an "open area" and unattended;
    8. Employees should be encouraged and trained to notice unsecured documents and take reasonable steps to secure them without incident or reprimand;
    9. Confidential paper documents that are no longer needed should be disposed of in a secure manner, preferably shredded;
    10. Refer calls or other requests for student information to designated individuals who have had safeguard training; and

11. Recognize fraudulent attempts to obtain student information and report it to appropriate law enforcement agencies.

Information Systems

The Information Technology Services office will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic student information and that guard against the unauthorized use of such information.

Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal. Security should be maintained throughout the life cycle of student information – that is, from data entry to data disposal:

1. Store electronic student information on a secure server that is accessible only with a password – or has other security;
2. Use password-activated screensavers;
3. Use strong passwords (at least eight characters long requiring a capital letter, number, and special symbol);
4. Change passwords periodically, and do not post passwords near employee computers;
5. Encrypt sensitive student information when it is transmitted electronically over networks or stored online;
6. Limit access to student information to employees who have a business reason for seeing it;
7. Maintain secure backup media and keep archived data secure, for example, by storing off-line or in a physically-secure area;
8. Provide for secure data transmission: If sensitive data is transmitted by electronic mail, ensure that such messages are password protected so that only authorized employee have access.
9. Erase all data when disposing of computers, hard drives or any other electronic media that contains student information; and
10. Effectively destroy hardware.

Managing System Failures

Effective security management includes the prevention, detection and response to attacks, intrusions or other system failures:

1. Follow a written contingency plan to address any breaches of your physical, administrative or technical safeguards;
2. Back up all student data regularly;
3. Check with software vendors regularly to obtain and install patches that resolve software vulnerabilities;
4. Use anti-virus software that updates automatically;
5. Maintain up-to-date firewalls;
6. Provide central management of security tools and communication updates about security risks or breaches; and

7. Notify students promptly if their nonpublic personal information is subject to loss, damage or unauthorized access.

Oversight of the Program

Responsibility for developing, implementing and updating this Plan lie with the Aries instructor. He will be responsible for Plan administration dealing with technology infrastructure and electronic safety protocols, and he will be responsible for the protection of student data and ensuring appropriate training of the school's staff on the Plan. All correspondence and inquiries should be directed to theAries instructor

Updating the Program

This information security plan shall be evaluated and adjusted in light of changing circumstances, including changes in the school's business arrangements or operations, or as a result of testing and monitoring the safeguards. Periodic auditing of each relevant area's compliance shall be done within each department. Evaluation of the risk of new or changed business arrangements will be done within each department.

Staff Training

FIT provides FTC Safeguard Rule training to its staff and faculty under the umbrella of FERPA training. Fayette County has conducted FERPA training sessions with all academic departments and employees.

FERPA compliance training of new staff, as well as annual review and training of current employees of the FIT, is handled by safe schools online training.

Oversight of Service Provider Arrangements

FIT will, in the normal course of business, periodically select and contract with service providers that are given access to student information. In the process of choosing a service provider that will have access to student information, the evaluation process shall include the ability of the service provider to safeguard student information. Contracts with service providers shall include the following provisions:

1. Explicit acknowledgment that the contract allows the contract partner access to confidential information;
2. Specific definition of the confidential information being provided;
3. Stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
4. Guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;

5. Provision for the return or destruction of all confidential information received by the contract partner upon completion of the contract;
6. A stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles Mercer County Technical Education Center to immediately terminate the contract without penalty;
7. A provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and
8. A provision ensuring that the contract’s protective requirements shall survive any termination agreement.

Currently, vendors who may have data access through this policy include a contracted Financial Aid Administrator approved by the state.