AIKEN TECHNICAL COLLEGE

INFORMATION SECURITY PLAN

ATC'S PLAN TO SECURE NONPUBLIC STUDENT INFORMATION

Table of Contents

AIKEN TECHNICAL COLLEGE INFORMATION SECURITY PLAN

PURPOSE AND ORIGIN

The purpose of this plan is to develop, implement, and maintain a comprehensive written information security program containing safeguards appropriate to Aiken Technical College's (ATC) size, mission and sensitivity of student information.

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

OBJECTIVES

- To ensure the security and confidentiality of student information
- To protect against any anticipated threats to the security or integrity of such information
- To guard against the unauthorized access to, or use of, such information that could result in substantial harm or inconvenience to any student

ONGOING IMPLEMENTATION

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

1) Maintain a security information coordinator position and a related team to coordinate the security information program, make suggestions and recommendations on an ongoing basis to the executive staff, and maintain a database of departmental risks and safeguards. The team will be queried at least annually for new suggestions and recommendations.

2) The coordinator, utilizing the team, will complete a College wide risk analysis to identify reasonable, foreseeable internal and external risks to the information provided by students at least once every five years.

3) The five year risk analysis will specifically cover the following general areas:

- Employee training and management
- Information systems management, including detecting, preventing and responding to attacks, intrusions or other system failures
- College operations obtaining, processing, accessing, or reporting student information including but not limited to: Admissions, Finance, Planning, Financial Aid, Instructors, Training and Business Development, Counseling, and Tutoring.
- Service providers such as bookstore vendors relating to graduating students, forms printing vendors, and educational organizations

4) List common risks and safeguards noted from the risk analysis.

5) Update the data base of individual risks and safeguards for each department processing student information

6) Apply suggestions for improvements resulting from the analysis, through specific recommendations to the Executive Staff

7) Testing of the database safeguards for effectiveness through internal audits conducted as a part of the regular cycle of internal audits. (See Appendix for checklist example)

RECOMMENDATIONS AWAITING IMPLEMENTATION

All initial recommendations from the original plan in 2003 have been implemented.

COMMON RISKS

The following common risks were gleaned from all the risks reviewed for all departments involved in the risk analysis:

1) That employees, contractors, or agencies misuse information on PC screens;

2) That unauthorized persons view information on PC screens;

3) That information printed to reports, files, or forms are seen by unauthorized persons;

4) That information printed to reports, files, or forms are misused by employees, contractors or other agencies;

5) That information is stolen by outside attackers, such as hackers, etc.;

SAFEGUARDS

Appropriate safeguards for the College are listed below.

1) Datatel system passwords and user names
2) Blank cover sheets or envelopes for printed materials
3) Employee information security signed agreements, such as a confidentiality statement
4) Information security training for employees
5) Offices with limited access (especially Human Resources, Payroll and Student records)
6) PC screen restrictions within Datatel
7) Student information reports restricted to necessary users
8) Student information screen access restricted to necessary users
9) Counter & desk designs to position PC screens away from student populated areas
10) Polarized screen covers to limit side viewing where PC's are in use in public areas
11) Security agreements with outside vendors having access to student information
12) Automated shut down time of Datatel system for PC's without activity
13) Securing paper documents such as registration forms, rosters and Add/Drop forms when work stations are unattended
14) Cross-cut shredding of documents containing student information that are ready for destruction
15) Published procedures forbidding faxes or e-mails with grades, social security numbers or other non-public student information.
16) Physical destruction of hard drives on PC's no longer in use from offices that retain student information on their hard drives.
17) Web firewall and virus protection for all PC's, servers and internet connections
18) Reference checks for all new employees
19) Exercise due diligence in authorizing access to College computing facilities (i.e. allowing access for computer maintenance staff)

ORGANIZATIONAL CONTROLS

Organizational controls provide that no one individual has access to or knowledge of an information system enabling them to process data without authority. Controls to safeguard administrative systems and their related data include:

1) Access to non-public data residing on any computer system, fileserver or workstation is granted only to authorized employees for areas related to their responsibilities.

2) Student employees may access nonpublic data only after initial information security indoctrination and only under the direct supervision of an authorized employee.

3) An authorized employee is a full time ATC employee who has read and become familiar with the College's information security procedures and so documented that action by a signed statement retained in the Human Resources department files and further has received permission from his or her supervisor to access non-public data, as well as completing the College Access Form, retained by the ISM department.

4) The Human Resource Director will:

   a. Maintain a New Hire package information sheet containing accountability details of both the Family Education Rights and Privacy Act (FERPA) and the Health Insurance and Portability Act (HIPPA) regulations.

   b. Maintain a compliance/confidentiality statement for all employees' signature that acknowledges: the sensitivity of non-public student information; reading of the sheet in a. above; and FERPA and HIPPA penalties for unauthorized disclosure.

   c. Include ATC's information security procedures, FERPA and HIPPA requirements in ongoing personnel training and professional development efforts.

ACCESS CONTROLS

Access or possession of system data resources is restricted to authorized individuals with the need to access that data. Users of ATC's systems are assigned user id(s) and password (s) granting them access to those systems. Users are responsible for the security of their password(s). The following procedures ensure the security of user accounts:

1) All requests for the creation, modification and deletion of system user accounts will be forwarded to ISM via the appropriate data access system request form.

2) If a user forgets their password they must request a new one from ISM.

3) ISM will review the access capabilities granted to each employee periodically. Managers and supervisors are responsible for requesting changes to an employee's computer access following from job function and responsibility changes.

4) Managers and supervisors are to use their professional judgment in allowing student employees access to non-public data.

5) Unauthorized log-in attempts that threaten system security will be reported to the respective Vice Presidents or President for resolution.

6) System documentation shall be current and secured.

7) The Cashier and Financial Aid PC's in close proximity to students will attach polarized screens or take alternative measures to prevent side viewing of non public student information.

DISTRIBUTION CONTROLS

Data extracted from the College's various systems must be carefully protected. Managers and supervisors must recognize and support the following responsibilities:

1) Determining which administrative data is appropriate for distribution, the audience for that data, the methods and timing of both data distribution and disposal.

2) Ensuring that the methods of distribution provide adequate security for the non-public information contained on the particular media utilized.

3) Keeping all individuals with access to non-public data aware of the importance of maintaining confidentiality and motivated to protect that data from improper disclosure.

4) Staying abreast of technology improvements that affect information security. For example being aware that simple shredding is no longer secure, but proper protection requires at least cross cut shredding.

5) Academic Divisions will choose only the ATC student ID when producing reports involving student data and not social security numbers. For example: attendance, grade and section rosters.

6) Campus Security will use an ATC student id number instead of social security numbers for rosters used in issuing parking decals.

7) Purchasing will request acknowledgement of information security plans in place, in contractual agreements with agencies and vendors receiving non public student information.

8) Outgoing faxes or e-mails containing non public student information must not be sent without verification and reasonable control that the proper recipient is the only viewer of the information.

9) Cross cutting shredders are to be used in disposing of paper documents containing non-public information.

10) Electronic files or media ready for disposal and containing non-public information must be destroyed or erased so that the information cannot be read or reconstructed. Media ready for disposal should be turned in to the ISM department for overwriting or physical destructions and a record maintained of the transfer. (See also Resource Controls item 6).

11) If an outside document destruction contactor is used to dispose of non-public information the College will conduct due diligence in selecting the vendor. Due diligence could include:

    i. Reviewing an independent audit of the contractor's operations and/or it's compliance with the FTC Disposal Rule.
    ii. Obtaining information from several references
    iii. Requiring certification by a recognized trade association
    iv. Reviewing and evaluating the contractor's information security policies and procedures

RESOURCE CONTROLS

Managers and supervisors should control computing resources by addressing the following concerns:

1) ISM will maintain effective protection from exterior and interior web net attacks.

2) Both onsite and offsite data backups should be controlled in a secure manner.

3) Workstations and PC's in areas with screens available to students or the public, are not to be left unattended while logged onto a College networked system or with non-public data displayed on the screen.

4) Telephone numbers for dial-up access to College systems shall not be posted, advertised, printed in directories or otherwise made public.

5) Inactive Datatel screens will time out after one hour

6) ISM and the equipment coordinator will identify and effect multiple overwriting of surplus PC hard drives to produce unrecoverable data.

7) The Bookstore cash register system will track charges by ATC student ID number and not social security number.

INCIDENT RESPONSE PLAN

In the event of a highly suspected or actual theft or loss of personally identifiable credit card data the following priorities should be followed:

(1) Notification of the Bursar

(2) Bursar will immediately notify Visa USA Fraud Control

(3) Bursar notifies and consults with the VP for Administrative Services (VPAS)

(4) If deemed necessary by the nature or the size of the loss the VPAS will convene the Incident Response Team.

(5) The Incident Response Team will limit to the extent possible the effect of a security breach, verify compliance requirements, and recommend actions to the VPAS.

(6) The Incident Response Team at a minimum will include the ISM Director, ISM Mgr. Operations, assigned to Business Office, Bursar, Financial Support Services Director, and the Registrar. Other members could include the Information Security Coordinator, the Public Safety Director and the Purchasing Director.

Response to noncredit card student non-public information exposure

(1) Upon knowledge of exposure all members of the Executive Staff should be notified

(2) Appropriate notice given to law enforcement if the exposure could result in harm to a student, employee or business. Typically this would occur if social security numbers were stolen or accessed by hackers.

(3) VP assigned to develop the response to all exposed parties, based upon the model letter from the Federal Trade Commission website business section under Identity Theft, Dealing with a Data Breach. Elements of the paragraph Notifying Individuals in the same section should be incorporated in the letter.

END OF PLAN