

THE CITADEL
The Military College of South Carolina
171 Moultrie Street
Charleston, SC 29409

MEMORANDUM
NUMBER 4

18 August 2006

INFORMATION SECURITY PLAN FOR STUDENT RECORDS

1. PURPOSE:

- A. The Citadel protects the privacy and confidentiality of all student records that it maintains in accordance with the provisions of South Carolina and federal statutes and regulations. The purpose of this memorandum is to outline the policies and procedures that the college follows to accomplish its security requirements.
- B. The Citadel's security plan accounts for the provisions of the following statutes and regulations:
- 1) The Family Educational Rights and Privacy Act (FERPA) of 1974, as amended.
 - 2) The Health Insurance Portability and Accountability Act (HIPAA) of 1996.
 - 3) The Gramm-Leach-Bliley Act of 1999.
 - 4) USA Patriot Act of 2001
 - 5) Campus Security Act of 1990, 20 U.S.C. § 1092.
 - 6) 42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records.
 - 7) SC Code 19-11-95, Confidences of Patients of Mental Illness or Emotional Conditions.
 - 8) SC Code 30-1-10, *et. seq.*, Public Records, Reports and Official Documents.
 - 9) S.C. Code § 30-2-10. *et. seq.*, SC Family Privacy Protection Act of 2002.
 - 10) S.C. Code § 30-4-10, *et. seq.*, SC Freedom of Information Act.
 - 11) S.C. Code § 40-75-190 Confidentiality of client communications of professional counselors, exceptions.
 - 12) S.C. Code . § 44-7-325, Hospitals, Fee for Search and Duplication of Medical Records.

- 13) S.C. Code § 44-22-90, Communications with mental health professionals privileged; exceptions
- 14) S.C. Code § 44-22-100, Confidentiality of records; exceptions, violations and penalties
- 15) S.C. Code § 44-115-40, Physicians' Patient Records Act.

2. RESPONSIBILITIES:

- A. Privacy Officer. The General Counsel is responsible for the coordination and execution of the Information Security Plan for Student Records. He has an additional duty that includes the responsibility for all policies dealing with the confidentiality of student records under the provisions of the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA) of 1996, and the Gramm-Leach-Bliley Act of 1999. He also is responsible for policy matters dealing with all requests for documents at The Citadel under the South Carolina and Federal Freedom of Information Acts. He will also ensure compliance with The South Carolina Family Privacy Protection Act of 2002. The Privacy Officer will coordinate with The Citadel vice presidents to maintain the information security program. The Privacy Officer will provide policy guidance for complying with all applicable privacy regulations. All correspondence, complaints, and inquiries concerning the confidentiality of student records should be directed to that office. The phone number of the Privacy Officer is (843) 953-5252.
- B. Vice Presidents and Records Custodians: Each vice president is responsible for maintaining the security and confidentiality of student records maintained in areas that they supervise. The vice presidents may appoint one or more of their subordinates as record custodians (see Annex A). This practice is most appropriate in those offices that maintain unique student records. However, the vice president maintains overall responsibility for student record security. To the extent that their offices and subordinates maintain student records, they are responsible for their entire area of supervision and assume the following responsibilities:
 - 1) Safeguarding of all student records maintained in their offices.
 - 2) Appointment of a Privacy Officer for the records maintained in their areas of responsibility. This officer has the same responsibilities as The Citadel's Privacy Officer, except the scope of his/her duties are limited to the student records maintained in their areas of responsibility. The Privacy Officer may also be the custodian of records for that office.
 - 3) The development of internal policies for the security and confidentiality of student records maintained in their office or departments. The policies will incorporate this policy and be supplemented to include local requirements based on the types of records maintained, local facilities, and requirements for access.

- 4) Determination of who has access to the student records maintained in their areas of responsibility. In this capacity the custodian is responsible for determining who (to include students, staff, and faculty) has “legitimate educational interest” as defined in this memorandum and FERPA.
 - 5) Education/training in student records security for the personnel assigned to their areas of responsibility who have access to student records.
 - 6) Controlling the release of student records to those outside of their area.
 - 7) The proper disposal of student records which are no longer required.
- C. The Director of Information Technology Services (ITS) will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information.
3. INTERNAL OFFICE STANDING OPERATING PROCEDURES:
- A. Each office is responsible for securing student information in accordance with all privacy guidelines. A written security policy that details the information security policies and processes will be maintained by each relevant area and will be made available to the Privacy Officer or the Internal Auditor upon request.
 - B. Each office that maintains student records at The Citadel must have the following documents on file or available within the office:
 - 1) General Order 8, dated 11 June 2003 (the college regulations that govern security of student records),
 - 2) The Citadel’s FERPA policy as outlined in the current college catalog,
 - 3) The office’s current Standing Operating Procedures for maintaining the security of student records, and
 - 4) The current Annual Notification of FERPA Rights as outlined on the college web site.
 - C. The office must have access to any statutes, regulations, or guidelines pertaining to the security of the specific type of student records that the office maintains *in addition to* the college’s policies (Example: policies or guidelines of accrediting agencies and professional organizations; and any federal or state laws that apply specifically to the operation of your department based on the types of records that are maintained).
 - D. The office’s internal Standing Operating Procedure for maintaining the security of student records must be in writing and accessible to everyone who has access to student records and must contain the following information:
 - 1) The methods used to maintain routine physical security of student records (*i.e.*, keeping files and rooms locked).

- 2) The procedure used to prevent unauthorized access to student electronic records (i.e., the positioning of computer monitors so that student records will not be visible to persons in your office who do not need to see them; having software that closes on-screen files after a certain period of inactivity; and, the limiting of access to electronic student files to only those who have a legitimate educational interest, etc.).
- 3) The method used to determine which personnel in the department have the need for access to student records.
- 4) The procedure used to educate personnel about departmental policies and requirements governing security of student records, including regular updates.
- 5) The procedures used to control the release of student records to those outside the department.
- 6) The procedure used to dispose of student records in paper format (vs. electronic format), including guidelines for how long the paper records are kept.

E. The departmental policy should be available through the college's web site as a link to FERPA.

4. EXTERNAL SUPPORT AGENCIES TO THE CITADEL:

A. The Citadel will select appropriate service providers that are given access to customer information in the normal course of business and will contract with them to provide adequate safeguards. In the process of choosing a service provider that will have access to customer information, the evaluation process shall include the ability of the service provider to safeguard customer information.

B. Contracts with service providers shall include the following provisions:

- 1) An explicit acknowledgment that the contract allows the contract partner access to confidential information;
- 2) A guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards but no less rigorously than it protects its own customers' confidential information;
- 3) A provision requiring the return or destruction of all confidential information received by the contract partner upon completion of the contract;
- 4) A stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;
- 5) A stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles The Citadel to immediately terminate the contract without penalty;

- 6) A provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and
- 7) A provision ensuring that the contract's protective requirements shall survive any termination agreement.

5. REVIEW REQUIREMENTS:

- A. This information security plan shall be evaluated and adjusted in light of relevant circumstances, including changes in The Citadel'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 pursuant to the internal auditing schedule. Annual risk assessment will be done through the Internal Auditor's office. Evaluation of the risk of new or changed business arrangements will be done through the respective vice president's office.
- B. The Internal Auditor or his / her designee will conduct a risk assessment periodically and audit each area's compliance. The risk assessment will include analysis of risks in each of the following operational areas:
 - 1) Employee training and management.
 - 2) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal, and detecting, preventing and responding to attacks, intrusions, or other systems failures.

FOR THE PRESIDENT:

OFFICIAL

JOSEPH W. TREZ
Colonel, USA, Retired
Executive Assistant to the President

ATTACHMENTS:

Annex A – Records Custodians

CITADEL STUDENT RECORD CUSTODIANS

The following offices have been identified as areas that maintain student educational records. (This includes records maintained by the college that may contain confidential information on a student or a student's parents.) The custodian of records in these offices and the responsible vice president are identified in the table below. Those Record Custodians identified with an * are designated as The Citadel's Record Custodian for that type of student record. As the custodian of the record, they or the responsible VP have the responsibility and the authority to designate those individuals or positions that have a legitimate educational interest in the record.

OFFICE/DEPT.	TYPE OF STUDENT RECORDS	RECORD CUSTODIAN	RESPONSIBLE VP
Accounts Payable	Financial Records	Director of Financial Services	VPBA
Admissions	Admissions Records	Director of Admissions	Assoc. Provost
Archives	Archived Records	Director of Records Management	VPBA
Infirmary	Medical Records	Citadel Physician	VPBA
Cadet Store Gift Shop	Charges and Financial Records	Manager, Cadet Store	VPBA
Treasurer	Financial Records	Treasurer	VPBA
Telecommunications	Phone Records and Directories	Director of Telecommunications	VPBA
Academic Departments	Academic Records	Academic Dept. Heads	Assoc. Provost
CGPS	CGPS Student Records	Assoc. Dean of CGPS	Assoc. Provost
Counseling Center	Student Counseling Records	Director of the Counseling Center	Assoc. Provost
Intramural Club Sports	Intramural Club Sports Records	Director of Intramural Club Sports	Assoc. Provost
Multicultural Affairs	Multicultural Counseling Records	Director of Multi-cultural Affairs	Assoc. Provost
Information Technology Services	Electronic Transmission Records	Director of ITS	Assoc. Provost
Library	Library Records	Director of the Library	Assoc. Provost
OASIS	OASIS Tutor Records ADA Records	Director of OASIS	Assoc. Provost
Planning Assessment	Assessment Records	VPAA	Assoc. Provost
Registrar	Academic Records	Registrar	Assoc. Provost
Writing Center	Tutor Records	Director of Writing Ctr.	Assoc. Provost
Athletics	Student Athlete Records	Assoc. Dir. of Athletics for Compliance	Director of Athletics
Commandant's Department	Disciplinary Records	Assist. Commandant for Administration	Commandant
Cadet Activities	Activity Records	Director of Cadet Activities	Commandant
Chaplain	Religious Records	Chaplain	Commandant
Office of The President	Student Records that Require Action by the President	Admin. Asst. to The President	Exec. Asst. to the President
Public Affairs	Photographs and Hometown Press Releases	VP for Communications	VP for Communications
President's Support Office	Legal Actions, Complaints Reports that Identify Cadets by Name, SSN or student ID	Admin. Asst., President's Support Office	General Counsel