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

MEMORANDUM 30 July 2009
NUMBER 3-6

ELECTRONIC INFORMATION SECURITY POLICY

1. PURPOSE

The Citadel does not routinely monitor individual usage of its computing resources or the privately owned computing devices used to access The Citadel network beyond the back up and caching of data and communications required in the normal operation and maintenance of the College's computing resources. When there is sufficient justification to do so (upon the occurrence of certain events for example), the College may access and / or monitor the accounts of specific individual users of college computing resources. The purpose of this Memorandum is to announce the college policy governing the monitoring of computing resources at The Citadel. This Memorandum applies to all users of Citadel computing resources, whether affiliated with the college or not, and whether on campus or from remote locations.

2. REFERENCE

Federal Rules of Civil Procedure
Computer Fraud and Abuse Act, 18 USC §1030
Computer Crime Act, S.C. CODE ANN. § 16-16-10 (1976)

3. POLICY

A. POLICY

The Citadel follows standard, widely accepted computer operation and data security procedures that include the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other similar activities. The Citadel does not consider these normal operations an invasion of individual privacy and carries out these operations routinely without notification. When there is reasonable cause to do so, the College may, without notice, access and monitor the accounts of individual users of college computing resources, including individual login sessions and communications. Furthermore, when the College "reasonably anticipates" litigation, through the receipt of notification

or other information identifying the possibility of a lawsuit or upon the actual service of a summons and complaint ("notification"), the College must take actions to preserve all electronically stored information that may be relevant to the claim.

B. PROCEDURES – GENERAL

1) The college may, without notice, access and monitor the accounts and equipment of individual users of college computing resources, including individual login sessions and communications when there is reasonable cause to do so. Such causes include, but are not limited to the following:

a. the user has voluntarily made them accessible to the public, as by posting to the College's website or any webpage, whether affiliated with the College or not;

b. it reasonably appears necessary to do so to protect the integrity, security, or operation of college or other computing resources or to protect the College from liability;

c. an account appears to be engaged in unusual or unusually excessive activity, as indicated by the monitoring of general activity and usage patterns;

d. it reasonably appears that the account could have a detrimental impact on the operation of the College or the safety of faculty, staff, or students;

e. it reasonably appears necessary to do so as part of an audit conducted internally at the College or by outside auditors or governmental agencies; or

f. it is otherwise required by law.

2) Any access or monitoring of accounts and equipment, other than that specified in part 1) a. (above) or required in response to perceived emergency situations, must be authorized in advance by the Director of Information Technology Services or his designee and General Counsel, following consultation with appropriate College officials.

3) The college will maintain documentation of the authorizations to access or monitor individual user activity or information stating the purposes for which authorization is given. Activities associated with accessing, monitoring, and investigating users' activity and

information shall be limited to the purposes for which such College and/or third party activity is authorized.

4) When the contents of a current employee's or student's College owned computer or communications associated with an individual's College computing account are accessed or monitored under this policy, the individual will be notified as soon as practicable that the access or monitoring occurred, provided the notification is permitted by law and will not interfere with any investigation by the College or other outside agency. Notification is not required when the access or monitoring was conducted under part 1) a.

5) The College, in its discretion, may disclose the results of any such general or individual access or monitoring, including the contents and records of individual communications, to appropriate College personnel or law enforcement agencies and may use those results in appropriate College disciplinary processes.

6) On an annual basis, General Counsel and the Director of Information Technology Services shall provide a report to the President regarding: the number of times the authorization required by this policy was requested to monitor the accounts of group or individual users of College computing resources; the number of times such authorization was given; and a general description of the purposes for requests and authorizations. The report shall be made in a manner that does not directly or indirectly identify the individual users involved or reveal any confidential or private information.

B. PROCEDURES – BEFORE AND DURING LITIGATION

1) Pre-Litigation Data Retention: When the College "reasonably anticipates" litigation, through the receipt of notification or other information identifying the possibility of a lawsuit or upon the actual service of a summons and complaint ("notification"):

a. As soon as practicable after notification, the General Counsel (GC) will notify the Director of Information Technology Services (DITS) of a new potential or actual claim and provide parameters for the information to be preserved. These parameters will be based on the known relevant parties and witnesses (i.e., those who may control or possession or potentially relevant data), the departments of the college which are involved, and the timeframe of the incident or incidents alleged.

b. DITS will take immediate steps to preserve all data held by central services (mail, calendar, etc.).

c. As soon as practicable, the GC and the DITS will meet to discuss the case and develop an initial course of action. Together they will:

i. Identify the set of data that must be preserved;

ii. Discuss mechanisms, process and other circumstances that may be particular to the specific lawsuit; and

iii. Prepare individual and department questionnaires for use by college personnel to identify the location of electronic and paper data implicated by the threatened or potential lawsuit.

d. The GC and DITS, or his designee, will meet with local representatives to discuss immediate needs, identify data unique to the local department, and create a plan to preserve all required data (and to reiterate need to preserve “paper” data as well).

e. DITS will send out end user questionnaires to all affected individuals for completion and return to DITS so that DITS can identify all potential locations of data.

f. DITS will work with the individual departments (involving HR as appropriate) to implement preservation

g. The GC will send specific information handling instructions to all affected individuals to ensure future data are appropriately preserved and easily retrievable. These instructions may provide that:

i. All future documents created that may be relevant to the case be stored in a specific directory;

ii. All future mail correspondence be appropriately stored in a specific mail folder; and

iii. All systems used for future creation of data potentially relevant to a claim be backed up on a regular schedule by DITS.

h. DITS will store all collected data centrally for future potential retrieval and discovery.

2) Discovery: Discovery is the formal process by which parties exchange information after a lawsuit has been filed. Upon receipt of a discovery request for information and data pertaining to a lawsuit, the College must take action to develop and produce a response to this request. The General Counsel, in consultation with the Senior Staff, the DITS, and other college officials, serves as the lead college official for The Citadel's response to discovery requests. The Citadel's response may be to supply the requested information, attempt to obtain a modification of the request as to a different set of data or search terms, or to decline to provide some or all of the requested data based upon expense or some other basis. During the discovery phase:

a. The GC will meet with DITS to discuss the specific requirements of discovery requests.

b. If the college has previously preserved information, as described in Paragraph 1) g, above, the DITS will determine whether the set of preserved data is sufficient to meet the requirements of the discovery request. DITS will also notify the GC of any extraordinary circumstances, costs of compliance, or other concerns.

c. If DITS determines that the preserved data is not sufficient to meet the requirements of the discovery request, the GC and DITS will work to retrieve additional electronic data, whether from central or local data repositories.

d. DITS will perform searches on the preserved data specific to the discovery requirements.

e. DITS will supply the retrieved data to the GC.

f. GC will review the retrieved data to determine legal relevance, privilege or other protected status, and will handle discovery.

4. COMPLIANCE

Failure to adhere to these procedures can result in significant civil penalties to The Citadel. Therefore, individual failure to cooperate with these policies may result in one or more of the following:

1. Exposure of the individual to civil liability,
2. Disconnection of the user's computer from the Citadel network,
3. Suspension of the user's network account, and
4. Referral to the appropriate supervisor or disciplinary body

5. NOTES

A. Dates of official enactment and amendments:

Approved by Director of Citadel Staff on 30 July 2009

B. Responsible Department:

Information Technology Services

C. Responsible Official:

Director of Information Technology Services

D. Cross References

Memorandum No. 3-2 Computer and Networking Use
Memorandum No. 3-3 Computer Security
Memorandum No. 3-4 Access to Electronic Mail Services
Memorandum No. 3-5 Appropriate Use of Mass Electronic Mail

6. RESCISSION

Information Security Policy, published 23 October 2007, is rescinded.

FOR THE PRESIDENT:

OFFICIAL

JOSEPH W. TREZ
Colonel, USA, Retired
Director of The Citadel Staff