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

MEMORANDUM 10 FEBRUARY 2022
NUMBER 3-607

INFORMATION TECHNOLOGY USE POLICY (NON-STUDENT)

1. PURPOSE

This policy establishes the requirements for the use of The Citadel's information technology resources to ensure the appropriate confidentiality, integrity, and availability of the College's data and information technology systems.

2. REFERENCES

N/A

3. DEFINITIONS

The Citadel's information technology resources include, but are not limited to, computers, computer systems, networks, electronic and mobile communications systems, telephone and data systems, internet connections, software, and related hardware and infrastructure that are owned, leased, acquired, developed or maintained by the college.

4. POLICY

All members of The Citadel community must use information technology and electronic communications in a responsible manner and in compliance with college regulations and applicable state and federal laws. Information Technology Services (ITS), on behalf of the college, may restrict the use of information technology systems in response to complaints presenting evidence of violations of college policies, or state or federal laws.

A. Policy Violations

Examples of behavior in violation of this policy include, but are not limited to, use of information technology to:

Harass, threaten, or otherwise cause harm to a specific individual(s) or classes of individuals;

Impede or interfere with the activities of others;

Transport material that is illegal, proprietary, in violation of college contractual agreements, or otherwise is damaging to the institution;

Deliberately send, post, view, or reply to indecent, obscene, pornographic, offensive, threatening, harassing, libelous, slanderous or fraudulent content, or content that is otherwise a violation of state or federal law.

Deliberately circumvent access control mechanisms;

Use credentials assigned to another individual in order to gain that person's access rights or to masquerade as that individual;

Purposefully expose or carelessly handle confidential, privileged or private information;

Intentionally make unauthorized changes or deletions of information stored in College information technology systems;

Install and/or use unlicensed or illegally obtained software.

Uninstall, or otherwise disabling software required by ITS to protect its systems;

install communications devices such as modems, hubs, routers and switches, or network monitoring tools such as sniffers and port scanners, without the explicit approval of ITS.

Posting information to Citadel listservs or email groups (eg. DogNews, All_Faculty, All_Staff, etc.) that is outside of their intended purpose.

B. Administration

The Citadel follows information technology operation and data security procedures that include the storage of data and communications, the logging of activity, the monitoring of general usage patterns, and other similar activities. When there is reasonable cause to do so, the College may, without notice, access and monitor the accounts of individual users of college information technology resources. 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 will take actions to preserve all electronically stored information that may be relevant to the claim.

The college may, without notice, access and monitor the accounts and equipment of individual users of college information technology 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:

1. It reasonably appears necessary to do so to protect the confidentiality, integrity, or availability, of the College's information technology resources or to protect the College from liability;

2. An account appears to be engaged in unusual activity, as indicated by the monitoring of general activity and usage patterns;

3. 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;

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

5. It is required by law.

6. Any access or monitoring of users, other than that specified in section 5a. (above) or required in response to perceived emergency situations, must be authorized in advance by the Chief Information Officer or their designee and General Counsel, following consultation with appropriate College officials.

7. The Citadel will maintain documentation of the authorizations to access or monitor individual user activity or information stating the purposes for which authorization is given.

   When the contents of a current employee's Citadel 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 section 5a. above**

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

C. 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"):

   As soon as practicable after notification, the General Counsel (GC) will notify the Chief Information Officer (CIO) 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 possess potentially relevant data), the departments of the college which are involved, and the timeframe of the incident or incidents alleged.

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

Identify the set of data that must be preserved;

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

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.

The GC and CIO, or their 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.

The CIO will send end user questionnaires to all affected individuals for completion and return. Information from the questionnaires will be used to identify potential locations of data.

The CIO will work with the individual departments (involving HR as appropriate) to preserve relevant data.

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:

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

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

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

Discovery: 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 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:

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

If the college has previously preserved information, as described in section f. Pre-Litigation Data Retention, above, the GC and CIO will determine whether the set of preserved data is sufficient to meet the requirements of the discovery request. The CIO will also notify the GC of any extraordinary circumstances, costs of compliance, or other concerns.

If the CIO and GC determine that the preserved data is not sufficient to meet the requirements of the discovery request, the CIO will work to retrieve additional electronic data.

The CIO will perform searches on the preserved data specific to the discovery requirements.

The CIO will supply the retrieved data to the GC.

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

5. COMPLIANCE

Depending on the seriousness of the offense, violation of the above rules may result in the temporary or permanent loss of access to The Citadel's information technology resources; suspension or termination of employment and other disciplinary or legal actions.

6. NOTES

A. Dates of official enactment and amendments:

Approved by Vice Presidents on 14 January 2022.

B. Responsible Department:

Information Technology Services

C. Responsible Official:

Chief Information Officer

D. Cross References:

None

7. RESCISSION

The following policies are hereby rescinded:

Memo No. 6-302 Computer and Networking Use Policy, published July 30, 2009
Memo No. 6-305 Appropriate Use of Mass Email, published September 21, 2011
Memo No. 6-306 Electronic Information Security Policy, Published July 30, 2009

8. REVIEW

This policy will be reviewed on a biennial basis.

FOR THE PRESIDENT:
OFFICIAL:

xx Sally Selden, PhD *xx*
Provost and Dean of the College
Brigadier General, SCM