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

MEMORANDUM 30 July 2009
NUMBER 3-2

COMPUTER AND NETWORKING USE POLICY

1. PURPOSE

The purpose of this Memorandum is to announce the college policy governing the proper use and management of all computing and network resources of The Citadel. This Memorandum applies to all users of college computing resources, whether affiliated with the college or not, and whether on campus or from remote locations.

2. REFERENCE

Computer Fraud and Abuse Act, 18 USC §1030
Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860, 2905
Computer Crime Act, S.C. CODE ANN. § 16-16-10 (1976)

3. DEFINITIONS

The Citadel's computing 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 ("computing resources").

4. POLICY

A. BACKGROUND

The Citadel provides computing resources to support the college's mission; instruction, academics, scholarship, research and service; administrative functions; student and campus life activities; and the free exchange of ideas among members of the college community and between the college and the wider local, national, and world communities.

The right of academic freedom applies to the use of college computing resources. So, too, however, do the responsibilities and limitations associated with that right. The use of college computing resources is a

revocable privilege. The use of college computing resources, like the use of any other college resource or activity, is subject to the normal requirements of legal, ethical, authorized and appropriate behavior. Users must abide by all applicable restrictions, whether or not they are integrated into the computing resources and whether or not they can be circumvented by technical means.

Users, including college employees and students, should understand that their expectations of privacy and ownership in their use of college computing resources are limited and may be unfounded. The college, including the General Counsel and the Director of Information Technology Services (see “Security and Privacy” below), will engage in activities authorized by this policy with due and careful regard for the interests of college employees and students in academic freedom, privacy, and employee or student proprietary information.

B. POLICY STATEMENT

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 or federal laws. Information Technology Services (ITS), on behalf of the college, may restrict the use of its computers and network systems in response to complaints presenting evidence of violations of college policies or codes, or state or federal laws. Specifically, the college reserves the right to limit access to its networks through college-owned or other computers, and to remove or limit access to information contained in college-owned systems, in addition to imposing any of the penalties stated below.

C. POLICY VIOLATIONS

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

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

2) Impede or interfere with the activities of others;

3) Download or post to college computers, or transport across college networks, material that is illegal, proprietary, in violation of college contractual agreements, or otherwise is damaging to the institution;

4) Propagate electronic chain mail;

5) 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.

Other examples of policy violation include:

6) Deliberate circumvention of network or system access control mechanisms;

7) Use of a username and password assigned to another individual in order to gain that person's access rights or to masquerade as that individual;

8) Unauthorized exposure or careless handling of confidential, privileged or private information;

9) Unauthorized alteration or deletion of information stored on college computers;

10) Use of unlicensed or illegally obtained software.

From time to time, Information Technology Services will institute policies and procedures intended to protect the college's network and systems from inappropriate use or disruption. Violations of these policies or failure to follow these procedures also constitute a violation of the overarching Responsible Use policy and include:

11) Without prior permission from Information Technology Services (ITS), uninstalling, failing to install, or otherwise disabling software required by ITS to protect its systems from the propagation of viruses, worms, malware or spyware;

12) Connection of communications devices such as modems, hubs, routers and switches, network monitoring tools such as sniffers and port scanners, and provision of services which may only be provided by ITS such as DNS, VPN and DHCP servers.

D. ADMINISTRATION

Questions concerning policies and procedures relating directly to the use of information technology resources and requests for exceptions should be sent to the Director of Information Technology Services.

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 computing and network resources; suspension, dismissal, or expulsion from the college (for students); suspension or termination of employment (for faculty and staff); and other disciplinary or legal actions.

6. NOTES

A. Dates of official enactment and amendments:

Approved by the 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. 3-3 Computer Security
Memorandum No. 3-4 Access to Electronic Mail Services
Memorandum No. 3-5 Appropriate Use of Mass Electronic Mail
Memorandum No. 3-6 Electronic Information Privacy Policy

7. RESCISSION

Computer and Network Use Policy, published 23 October 2007, is rescinded.

FOR THE PRESIDENT:

OFFICIAL

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