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

MEMORANDUM 30 July 2009
NUMBER 3-3

COMPUTING RESOURCES SECURITY POLICY

1. PURPOSE

The computing resources at The Citadel include centrally located server systems and desktop, laptop, and handheld devices. Although most of the systems centrally managed are reasonably secure, installation and monitoring of detection and protection systems is both expensive and increasingly time consuming. Individual desktops, laptops, and handheld devices are even less secure. The purpose of this Memorandum is to announce the college policy governing the proper security procedures to be followed when using computer 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

Computer Crime Act, S.C. CODE ANN. § 16-16-10 (1976)

3. POLICY

A. Policy: The Citadel employs various measures to protect the security of its computing resources and of users' accounts. However, the college cannot and does not guarantee the security of its computing resources, or of personal information located on any college owned or personally owned device. Therefore, The Citadel expects all users to take certain basic security steps to enable their computer to run smoothly and safely on The Citadel's Network. These steps are not a guarantee that individual computers or the college's computing system will not be compromised, but serve to make individual computers and the system a less inviting target to malicious persons

B. Procedures: Users are expected to engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing their passwords regularly. Also, users should ensure the installation of anti-virus software and appropriate

updates for personally-owned computers connecting to the college's network and computers.

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 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. 3-4 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 Resources Security, published 23 October 2007, is rescinded.

FOR THE PRESIDENT:

OFFICIAL

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