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

MEMORANDUM 14 February 2022
NUMBER 3-608

Information Security Policy

1. PURPOSE

The Information Security Policy for The Citadel describes the responsibilities and expectations for the Citadel's Information Security Program.

2. REFERENCE

N/A

3. DEFINITIONS

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

B. A User is defined as any person accessing Citadel data or Citadel computing resources, including but not limited to: students, faculty, staff, contractors, clients, consultants, invited guests, and others working at or for The Citadel.

4. POLICY

The Citadel strives to provide a safe computing environment and is committed to securing its data and computing resources per state and federal laws, statutes, and regulations. In order to support risk management and compliance efforts, the Information Technology Services department (ITS) is responsible for administering a campus-wide Information Security Program.

A. ITS reports progress on the Information Security Program to the Board of Visitor's Operational Risk Management Council.

B. The Citadel prohibits interference with (or avoidance of) information security measures. Such actions may be grounds for investigation and disciplinary action.

C. ITS will:

1. Develop and maintain the Information Security Program. The program will focus on the most significant threats to Citadel data and computing resources, weighing the impact of requirements on college operations.

2. Develop, implement and maintain Security Incident Response procedures.

   ITS may omit internal details due to the sensitive nature of some incident response practices.

3. Act to protect users, data and computing resources, including interruption of access until a threat or vulnerability is resolved.

4. Operate per state and federal laws, statutes, and regulations governing data and computing resources.

5. Carry out all provisions of the Information Security Program. Provisions may include, but are not limited to, reporting current protections, implementing safeguards, documenting improvement plans, and maintaining approved exceptions to program requirements.

   Each User will:

   a. Protect Citadel data and computing resources according to ITS instructions.

   b. Stop using an information technology resource if the user suspects a compromise and report the incident. Users may report incidents to the IT Help Desk or IT Security Manager.

5. COMPLIANCE

6. NOTES

A. Dates of official enactment and amendments:

Approved by the Vice Presidents on 14 January 2022.

B. Responsible Department:

Information Technology Services

C. Responsible Official:

Chief Information Officer

D. Cross Reference

None.

7. RESCISSION

The Policy on Computing Resources Security, published July 30, 2009, is hereby rescinded.

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