COLLEGE of CHARLESTON

OFFICIAL POLICY

10.20	Acceptable Use of Information Technology	10/14/2020

Policy Statement

The Office of Information Technology has established this policy regarding access to, and acceptable use of the College's Information Technology Resources. In order to successfully carry out its mission, the College of Charleston will act to protect the confidentiality, integrity and availability of information technology assets in accordance with all applicable policies, standards, procedures and best practices.

Information Technology Resources are the College's Network Infrastructure and all other College Information Technology Resources; and other Information Technology Resources made available to the College community through a College vendor-sourced network; and other electronic device regardless of ownership when such device is actively using the College Network or is otherwise interfacing with a College Information Technology Resource.

Policy Manager and Responsible Department or Office

Information Security Office

Purpose/Reason for the Policy

All users of College of Charleston information technology resources must adhere to applicable state and federal laws, statutes, and regulations; must comply with applicable policies, standards and procedures as defined by the College of Charleston; must understand and acknowledge that information technology assets and data are for

authorized use only; and must not compromise the confidentiality, integrity and availability of these assets and data.
The College of Charleston provides information technology resources for use by faculty and staff for College of Charleston-related duties, responsibilities and business.

Departments/Offices Affected by the Policy

College of Charleston faculty and staff.

Procedures Related to the Policy

Definitions

1. The College of Charleston's voice, video, and data systems and those systems, as defined below, will be referred to generally as "College of Charleston Information Technology Resources / assets" in this document.

2. The phrase " College of Charleston Information Technology Resources / assets " is defined as the College Network and all College computers and computer components, electronic storage devices, wiring, and electronic transmission devices owned, rented, leased or operated by the College or and all College owned or licensed software.

3. The term "user(s)" refers to any person(s) accessing College of Charleston information technology assets, including but not limited to: students, faculty, staff, contractors, clients, consultants, College volunteers, retirees, Emeriti, Adjuncts and others working at or for the College of Charleston.

4. The "Information Security Office" is defined as the group assigned to implement College of Charleston-wide information security strategy and is led by the Chief Information Security Officer.

5. The term "access credentials" refers to the user identification, logon/login identification, or other system-specific means granted to a user permitting access to College of Charleston information technology assets or data.

6. The term "authentication" is defined as a means to determine whether a user attempting to gain access to College of Charleston information technology assets by means of particular access credentials is in fact the user those credentials were assigned to.

7. The term "authorization" is defined as a means to determine whether a user is permitted access to specific College of Charleston information technology assets.

8. The term “College Data” means any information, regardless of format, that is generated or collected for or by the College. College data are vital College assets that are used in the operations of the College to carry out the College’s mission and to execute the College’s business function.

Procedures

1. The College of Charleston Division of Information Technology will establish and maintain a set of requirements -- in the form of policies, standards and procedures -- that must be met by users of College of Charleston information technology resources and assets.

2. All users are responsible for complying with the Acceptable Use Policy and established IT policies, standards, procedures and guidelines. Users are responsible and accountable for all activity initiated or conducted through the use of assigned access credentials. Violation of any portion of this policy may result in immediate loss of access to College of Charleston information technology assets, initiation of legal action by the College of Charleston, and/or disciplinary action as appropriate. All users are responsible for reporting any actual or suspected violation of this policy to the College of Charleston Information Security Officer immediately.

3. Access Credentials must be protected. Passwords must not be shared with anyone. The password must contain 8-12 characters, contain a letter, contain a digit, and contain a special character (~ ^* _ + ? - .). Passwords will expire and must be renewed after 120 days.

4. All computers connected to College of Charleston Information Resources are required to have up-to-date, operational, running antivirus software.

5. Personally owned technology such as mobile devices (e.g., smart phones, tablets, portable computing devices, etc.) or home computers that interface with College of Charleston information technology assets will be subject to this policy.

Related Policies, Documents or Forms

Privacy Policy

Issue Date:7/26/2016 Date of Policy Review: 10/14/2020	Next Review Date:10/26/2025

POLICY APPROVAL
(For use by the Office of the Board of Trustees or the Office of the President)

Policy Number: 10.20

President or Chairman,
Board of Trustees

Date: 10/14/2020