1.0 Policy Statement

The Network Infrastructure Use Policy defines the College of Charleston standards for managing access to the College of Charleston network and electronic resources. The purpose of the NIUP is to ensure secure, reliable, and efficient network access for the College of Charleston community.

All confidential information including electronically stored information must be protected in a manner to commensurate with its sensitivity, value, and criticality; this includes protecting computing and communications systems containing that data accordingly. Procedures associated with this policy establish best practices for managing computing and communications systems and their network access. This policy is intended to protect the integrity of the campus network and to mitigate the risks and losses associated with security threats to the campus network and information systems.

While these policies identify many roles and responsibilities for safeguarding information resources, they cannot cover every situation or future development. Therefore, the NIUP is to be considered an evolving document which will be modified or amended to meet the growing needs of the College of Charleston. It will be reviewed on at least an annual basis for corrections and to ensure compliance with current rules and regulations.

2.0 Scope

The NIUP applies to all College of Charleston faculty (including adjunct and visiting faculty), staff, and students as well as any other user of the network infrastructure.

3.0 Policy

3.1 Ownership of Network Infrastructure

The College of Charleston network infrastructure is owned by and the property of the College of Charleston. The Network Engineering division of the IT department is primarily responsible for overseeing the operations and management of the network infrastructure. The College of Charleston network infrastructure includes, but is not limited to the following:
- College of Charleston network connections (wired and wireless).
- Network based communication services.
- Wireless technologies including, but not limited to: access points, SSIDs, and wireless switches.
- Network servers and appliances.
- Remote Access Technologies
- Network management and performance evaluation software

3.2 Installation of network equipment and Prohibited Devices

To maintain electronic systems integrity and ensure service availability, all College of Charleston network connections and network equipment installations are made only by authorized personnel under the direction of the Network Engineering Division of the IT department.
The College of Charleston Network is designed to support one Ethernet device per port. Network users are prohibited from installing network communication devices, which provide for simultaneous access by more than one Ethernet device via a College of Charleston data network port. Devices that are network intrusive (monitor, interrupt network services, or change the College of Charleston Data Network topology in any way) are prohibited. Prohibited devices include, but are not limited to, port splitters, hubs, switches, routers, wireless access points, multi-homed PC’s, and packet/data monitoring equipment/software. Network services and wiring may not be modified or extended beyond the area of their intended use. This applies to all network wiring, hardware, and jacks.

All requests for four or more College of Charleston data network connections should be directed to the Network Engineering Division of the IT department. Requests for less than four College of Charleston telecommunication outlet locations or for the relocation of a TO should be directed to the Helpdesk Division of the IT department. Any violations of standards, procedures, or guidelines pursuant to this policy may result in immediate disconnection of network services and/or removal of the intrusive device. Exceptions to NIUUP must be obtained in writing from the Network Engineering Manager.

3.3 Specialized Departmental Network Infrastructure Use

Since the College of Charleston cannot be directly responsible for all campus technology resources, users throughout the community share in the task of maintaining information technology security. In larger or more complex departments, there may be one or more employees assigned to provide departmental personal computer support. It is expected that these technical support administrators will employ College of Charleston recommended practices and procedures, cooperate with College of Charleston policies, and help in addressing security problems.

3.4 Internet Usage

College of Charleston provides access primarily to enable the conduct of academic and administrative activities in support of the College of Charleston’s Strategic Goals.

The following guidelines are for Internet usage:

Access to internet resources from on-campus College of Charleston facilities must be made through Internet access arranged or approved by the Network Engineering division of the IT Department.

Users must not download material from the internet that is subject to copyright or other intellectual property right protections unless the material is governed by fair use principles or express permission to do so is granted by the material owner.

Users are strongly encouraged to verify the authenticity and accuracy of materials sent via the Internet, and to use good judgment when deciding whether to download or open materials from people they do not know and organizations they did not contact. If in doubt contact the Helpdesk Division of the IT department.

3.5 Wireless Policy

Please see the College of Charleston Wireless Policy for information and regulations pertaining to the College of Charleston Wireless network.
3.6 Network Monitoring / Services and Expectation of Privacy and Confidentiality

The College of Charleston reserves the right to monitor and examine the type and content of electronic communications sent or received using the College of Charleston network at any time and without prior notice for the purpose of maintaining security responsibilities, responding to duly authorized law enforcement requests, and maintaining network integrity. There is no interest on the part of the College of Charleston to abridge academic freedom or personal speech rights, nor to monitor or track personal behavior for reasons unrelated to technical operations or compliance with these policies. Every effort will be made by security personnel to avoid violation of privacy of individuals or groups.

3.7 Network Scanning

Users may not conduct network scans searching for other connected devices or conduct any form of network monitoring that will intercept data not intended for the user’s computer. Users must not download, install, or run programs designed to reveal or exploit weaknesses in system security such as password discovery programs, packet sniffers, or port scanners, unless the intended use is to enhance the security of the system on which these programs reside. Any computer found doing so will be disconnected from the network with the possibility of having the computer removed by Public Safety.

3.8 Network Services

Unless specific authorization is received from the College of Charleston, Network Engineering Division of the IT department, individual users or departments must not operate DHCP, DNS, proxy, e-mail, remote access, or internet connection sharing services on the network. External DNS providers will not be allowed to advertise services at the College of Charleston network.

3.9 Remote Access to the College of Charleston

Safeguards regarding confidentiality and privacy of College of Charleston information apply equally at on-campus locations as well as at any remote location. When employees are working at an off campus location and remotely connecting to systems on the College of Charleston network, an encrypted communication channel must be used in order to protect the confidentiality of User Name, passwords, and College of Charleston records containing personal, confidential, or legally protected information. When using VPN technology with personal equipment, users must understand that their machines are acting as an extension of the College of Charleston’s network, and as such are subject to the same rules and regulations that apply to College of Charleston-owned equipment.

3.10 Simultaneous Connections to external networks

Machines connected simultaneously to the College of Charleston network and any external third party networks may not route traffic between systems on the external networks and the College of Charleston network unless authorized by the Network Engineering division of the IT department. All policies and regulations for connecting to the College of Charleston Data network from outside of the College can be found in the College of Charleston Remote Access Policy.
4.0 Guidelines for Enforcement

All policies and regulations for action taken in regards to blocking network access can be found in the Guidelines and Procedures for Network Access Policy

5.0 Future Policies, Pending Technology Development and Implementation

5.1 Maintaining Network Robustness

All computers connected to the College of Charleston network are required to undergo an automated evaluation to determine if certain software settings and applications are correctly installed and operational. As a result of this evaluation, the user may be required to install software or reconfigure existing software before unlimited network access is granted. Access to any resources to accomplish this task will be permitted. The College of Charleston will not access or modify software or information stored on personally owned equipment without permission of the owner; however, access to the College of Charleston network may be denied or limited unless these policies are complied with in full.

5.2 Device Registration

Every networked device which is to be connected to the College of Charleston Data Network must be registered. In order to register a device, a user must provide a valid College of Charleston user name and password.