SECURITY OF NETWORKS AND NETWORKED DATA

POLICY

Brunswick Community College's (hereinafter "College") computing and telecommunication networks, computing equipment, and computing resources are owned by the College and are provided to support the academic and administrative functions of the College.

The purpose of this policy is to outline the definitions of the procedures in supporting a high standard of network security as defined in the North Carolina Institutional Information Processing System Users' Group Information Security Standards (NCIIPS ITS) . Adherence to the policy will help protect the integrity of the campus network and networked data. Enforcement actions will mitigate risks and losses associated with security threats to the network and networked data.

Federal and state law, and College policies and procedures govern the use of BCC equipment and technologies. This policy applies to all faculty, staff, students, and other authorized individuals who connect network communications devices to the College data network. It is fundamental to all information security efforts at the College. The intent of this policy is not to change the ownership of computing and telecommunication networks, computing equipment, or computing resources. Additional rules and regulations may be adopted by divisions/departments to meet specific administrative or academic needs. Any adopted requirements must be in compliance with applicable federal and state laws, and this policy.

PROCEDURE

1. **Scope**
   The policy applies to all faculty, staff, students, and other authorized individuals who connect network communications devices to the College data network. It is fundamental to all information security efforts at the College.

   The intent of this policy is not to change the ownership of computing and telecommunication networks, computing equipment, or computing resources.

2. Policy
   A. Network Operation and Transport
      i. Physical Connections
         The following restrictions apply:
         a. Only a single network communications device should be attached per Ethernet jack. If additional jacks are required, a cabling request must be submitted to Information Technology Services (ITS).
         b. Physical access to infrastructure network switching equipment is not permitted without specific authorization of ITS.

c. Attached cables must be certified by ITS and shall not exceed 20 feet in length.
d. Ethernet hubs/repeaters must not be attached.
e. Ethernet switches/bridges must not be attached except as installed by ITS.
f. Hardware firewall/network address translation devices must not be attached.
g. Wireless enabled devices must not be attached.
h. Network layer 3 (logical layer) routing devices must not be attached.
i. All attached devices must have an identified owner and user.

ii. Logical Addressing

BCC has been granted Internet address spaces. ITS will exclusively provide allocation and administration of these address spaces in accordance with ITS procedures, standards, and protocols.

a. All network attached devices require registration in the ITS network registration system.
b. Name resolution to/from the Internet will only be provided for devices specifically identified as servers. Servers with administrative applications are subject to the Enterprise Systems Policy
c. ITS will manage additional domain name space (for example, student.brunswickcc.edu, idcard.brunswickcc.edu, etc.) in support of the College mission.
d. Individuals, academic colleges/departments, or administrative departments at BCC may not create and support an Internet domain name space without prior approval of ITS.

iii. Quality Of Service

ITS has the authority to implement Network Quality of Service technology to control the cost of providing Internet service, ensure equal communications access for all clients, and provide differential service for enterprise applications, which may include denial of transport.

iv. Workstation Operation

Computer workstation users are expected to adhere to the following:

a. Ensure that operating system and application software is kept up to date with manufacturer patches.
b. Take all necessary precautions to avoid workstation compromise. Employees and departments are responsible for making use of the recommended security software from the ITS division as set forth in the Standards for Computer and Related Technology (Supported Products List) and for configuring the software according to ITS standards.
c. Where possible, physically secure the workstation.
d. Do not allow others to use a workstation when logged in with your authentication credentials.
e. Do not provide personal login credentials to another employee
f. Ensure that data is retained and backed up if necessary.

g. Store all data that is classified as *Restricted* in the Data Classification Policy on ITS network storage facilities. Store all other data in personal Libraries Documents folder.
h. Employ mobile device startup password protections.
i. Follow ITS protocol for equipment disposal practices to ensure protection of data and licensed software.
j. Make reasonable precautions to avoid actions that could deteriorate the performance of the College network or networked resources (devices connected to the BCC network)

v. Server Operation
Application server administrators are expected to adhere to the following:
a. Ensure that operating system and application software is kept up to date with manufacturer patches.
b. Make all necessary precautions to avoid server compromise. Employees and respective departments are responsible for making use of the recommended security software from the ITS division as set forth in the Standards for Computer and Related Technology (Supported Products List) and for configuring the software according to ITS standards.
c. Physically secure the server.
d. Ensure that data is backed up and retained according to the Computer Systems Backup Policy.
e. Maintain system activity logs for auditing purposes.
f. Equipment disposal practices must follow ITS protocols to ensure protection of data and licensed software.
g. Adhere to the Enterprise Systems Policy.

vi. Human Safety
Network connected devices with applications directly involving human safety must be operated on a physically or logically isolated network. Examples are physical security and environmental control devices.

vii. Wireless Computing
The wireless communications spectrum is managed as part of the campus network. See Wireless Communications Policy.

B. Enterprise Passwords
Passwords are an important aspect of computer security. Passwords represent the front line of protection for all user accounts. A poorly chosen password may compromise BCC's entire network.

i. General Requirements
a. System or user-level passwords must be changed on the currently recommended standard periodic basis.
b. Passwords must be kept secure, and sharing of accounts is prohibited. Authorized users are responsible for the security of all assigned account and equipment activity and should follow security procedures determined by ITS standards.

c. User accounts that have system-level privileges through some form of group membership, or other implementation, must have a unique password from other accounts held by that user.
d. Passwords must not be inserted into e-mail messages or any other form of electronic communication.
e. All manufacturer default passwords must be changed before network connection.
f. The use of ITS enterprise authentication services is required.

ii. External Consultant Requirements
External consultants with applications containing passwords, shared secrets, or key phrases contained within should adhere to the following guidelines:
a. Support authentication through ITS enterprise authentication services.
b. Support authentication of individual users and not groups.
c. Must not store passwords in clear text or any form that is reversible.
d. Vendors of BCC requiring internal access from external sources must use the VPN services and a representative of said company must sign a confidentiality agreement.

C. Remote Access
i. The public sections of the College's Web site are available to any user through remote access.
ii. Remote access connections, whether originating from College-owned or personal equipment, should be given the same security consideration as an on-site connection.
iii. Faculty, staff, or students are the only ones permitted to remotely access College network resources and only through ITS-supported remote access technology.
iv. All remote access will be encrypted, and authenticated using ITS enterprise authentication services.
v. Approaches to network traffic that threaten security are strictly prohibited.

D. Acceptable Encryption
Encryption technology protects information content during network transport.
i. Some data must be encrypted in conformity with the Wireless Communications Policy and the Data Classification Policy.
ii. ITS-supported algorithms should be selected when using encryption technology.
iii. Cryptographic key lengths must be of sufficient length as to prevent successful intrusion in a short time period.
iv. The use of proprietary encryption algorithms is not allowed for any application housing data classified as Restricted as defined by the Data Classification Policy.
v. Export of encryption technologies is subject to federal law.

E. Non-Affiliate Access
Visitors or non-College community members may require temporary access to computer or network resources. Non-affiliate network access is subject to the following restrictions:
i. Non-affiliate network access is subject to all College policies including the Acceptable Use of Computing and Electronic Resources Policy.

ii. Only Deans and Department Heads can sponsor non-affiliate network access.
iii. Faculty, staff, and students must not use non-affiliate access procedures to gain any form of temporary computer or network access.
iv. Faculty and staff must not share their account information with non-affiliates.

F. Perimeter Security
The perimeter of BCC's network infrastructure is defined as the electronic border between the BCC campus network, and the first Internet Service Provider (ISP) networking device supplying wide area network (WAN) connectivity.
i. ITS maintains perimeter security for the purposes of general infrastructure protection.
ii. Only authorized ITS employees may modify perimeter security measures.
iii. All application servers must be specifically identified to ITS.

G. Compliance With Laws And Regulations Relating To Networked Data
BCC complies with federal and state laws and regulations relating to the security of networked data.

3. Enforcement
ITS will enforce the *Security of Networks and Networked Data Policy* and establish standards, procedures, and protocols in support of the policy. Alleged violations of this policy are subject to the due process provided in existing College policies. ITS has the authority to disconnect network service or modify/enhance network security without notification in the event of law violation, systems compromise involving restricted data, or negative network communications impact affecting service for other users.

4. Review
The Director of Information Technology Services has submitted the *Security of Networks and Networked Data Policy* to the Board of Trustees and will periodically review the policy as appropriate.

Links to Related College Policies
Computer Systems Backup Policy
Data Classification Policy
Enterprise Systems Policy
Wireless Communications Policy
Acceptable Use of Computing and Electronic Resources Policy

Approved by Brunswick Community College Board of Trustees
June 9, 2010; February 19, 2018