POLICY 8200

NETWORK SECURITY

Policy Category: Information Technology
Area of Administrative Responsibility: Information Technology Services
Board of Trustees Approval Date: April 17, 2018
Effective Date: April 18, 2018
Amendment History: N/A

Contents:

PURPOSE

This policy is intended to protect the integrity of the campus network, to mitigate the risks and losses associated with security threats to computing resources and to ensure secure and reliable network access for the Nassau Community College (NCC) community. This policy is necessary to provide a reliable Campus network to conduct the College's business and prevent unauthorized access to institutional, research or personal data. In addition, the College has a legal responsibility to secure its computers and networks from misuse.

Passwords are a vital aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password can compromise NCC's data systems and services. As such, all users (including contractors and vendors with access to NCC systems) are responsible for taking the appropriate steps, outlined below, to select and secure their passwords. The purpose of this policy is to establish standards for the creation of strong passwords, the protection of those passwords, and the frequency of change of passwords.

The policies and procedures outlined in this document will be enforced by the Chief Information Officer (CIO) or designee. The CIO or designee reserves the right to deviate from the policies and procedures described in this document, as new technology is introduced and business practices evolve.

SCOPE

This policy applies to all Nassau Community College (NCC) faculty, staff, students, vendors/contractors, guest account holders, and any other person who may connect to the College's network computing resources. This policy also applies to all devices, which are used by those individuals for network access, whether personally owned, College issued or otherwise obtained. These devices include but are not limited to workstations, laptops, tablets, smartphones, servers, consoles, controllers, and any other computing device, which is capable of communicating through the College networks.

POLICY

A. Addressing and Domain Service:

1. Information Technology Services (ITS) is solely responsible for managing any and all Internet domain names related to the College (e.g. ncc.edu). Individuals, academic departments or administrative departments may not create nor support additional Internet domains without prior approval from ITS.

2. To ensure the stability of network communications, ITS will solely provision and manage both the public and private IP address spaces in use by the College.

B. Network Connections and Usage:

1. Nassau Community College faculty, staff or students may not connect, nor contract with an outside vendor to connect, any device or system to the College's networks without the prior review and approval of ITS. Departments that wish to provide Internet or other network access to individuals or networks not directly affiliated with the College must do so for only legitimate educational or administrative purposes and must obtain prior approval from ITS.

2. In order to maintain reliable network connectivity, only ITS shall deploy wireless routers, switches, bridges, and/or Dynamic Host Configuration Protocol (DHCP) services on Campus. Any exceptions to this must be reviewed and approved by ITS.

3. Users are permitted to attach devices to the network provided that they:

   a. are approved by evidencing their acknowledgment of the terms of Policy 8100 Use of College Computer Resource

   b. are for use with normal College business, educational purposes or student operations

   c. do not interfere with other devices on the network

   d. conform to the usage that is in compliance with all other NCC policies

   e. are not used for personal gains

4. Network usage which is determined to be appropriate by ITS is permitted. Some activities deemed inappropriate include, but are not limited to:

   a. Attaching unauthorized network devices, including but not limited to wireless routers, gateways DHCP or DNS servers; or a computer set up to act like such a device.

   b. Engaging in network packet sniffing or snooping.

   c. Setting up a system to appear like another authorized system on the network (Trojan).

   d. Other use which is unauthorized or prohibited under this or any other College policy.

5. Network access will be revoked at the time of termination of employment with the College.

C. Wireless:

1. ITS is solely responsible for managing the unlicensed radio frequencies (wireless networking) on Campus, which includes the 2.4 GHz and 5 GHz spectrum and may include future wireless spectrum standards.

2. ITS is responsible for maintaining a secure network and will deploy appropriate security procedures to support wireless networking on Campus.

3. The College will maintain a campus wireless network based only on industry standards. ITS will collaborate with academic departments where devices used for specific approved educational or research applications may require specific support or solutions.

4. ITS will provide a general method for network authentication to College systems. Additional security protocols may be applied as needed.

D. External Traffic, Services and Requests:

1. ITS will take action to prevent spoofing (impersonation) of internal network addresses from the Internet. ITS will also take action to protect external Internet sites from source address forgery from devices on the College's network.

2. The College's external Internet firewall default practice is to deny all unsolicited external Internet traffic to the College's network unless explicitly permitted. To facilitate this, academic departments and other administrative departments that have legitimate purposes must register systems with ITS which require access from the Internet. Users that would like to request access through the College firewall must open a help desk ticket.

3. Access and service restrictions may be enforced by device, IP address, port number or application behavior.

E. Monitoring and Auditing:

1. ITS will maintain and monitor traffic logs for all network devices and systems for security auditing purposes.
2. ITS reserves the right to monitor, access, retrieve, read and/or disclose data communications when there is reasonable cause to suspect a College policy violation, criminal activity, monitoring required by law enforcement or by appropriate management request. Reasonable cause to take disciplinary action may be provided by a specific complaint of a policy violation or possible criminal activity, or may arise from prohibited or unlawful usage, which is noticed incidentally by ITS staff while carrying out their normal duties.
3. ITS may perform penetration testing of any College owned devices or systems on its networks in order to determine the risks associated with protecting College information assets. ITS may further perform non-intrusive security audits of any system or device attached to the College's networks in order to determine what risks that system or device may pose to College's overall information security.

F. Rights and Responsibilities:

1. Any device found to be in violation of this policy, or found to be causing problems that may impair or disable the network or systems connected to it, is subject to immediate disconnection from the College's network. ITS may subsequently require specific security improvements where potential security problems are identified before the device may be reconnected.
2. Attempting to circumvent security or administrative access controls for information resources is a violation of this policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of this policy.
3. The College reserves the right to test and monitor security, and to copy or examine files and information resident on College systems related to any alleged security incident or policy violation.
4. ITS may investigate any unauthorized access of computer networks, systems or devices. To accomplish this, ITS will may collaborate with academic or administrative departments and law enforcement authorities when appropriate.
5. All devices connecting to the network must be authenticated prior to gaining system access.
6. If a security breach is observed, it is the responsibility of all Nassau Community College users to report the breach to their supervisor or directly to ITS for investigation.

G. Exceptions:

If compliance with this policy is not feasible or is technically impossible, or if deviation from this policy is necessary to support a legitimate business function, an exception to the policy can be requested, which exception must be approved by the ITS CIO or designee.

PASSWORDS

A. General:

1. User must change passwords periodically.
2. The frequency of password change is generally based on the privilege or access level of the account. Accounts with greater privilege or access should have their passwords changed more frequently.
3. For all employees the required interval for password changes is once every 180 days.
4. If a password has been compromised or suspected to be compromised, the password should be changed immediately. Change your password by visiting https://myncc.ncc.edu or contact the helpdesk at Helpdesk@NCC.edu for assistance.
5. Passwords must not be inserted into email messages or other forms of electronic communication.

All user-level and system-level passwords must conform to the guidelines described in the General Password Guidelines in the Procedures to this policy.

B. Password Requirements:

Nassau Community College users shall select passwords according to the following minimum requirements:

1. Password must be no fewer than eight (8) characters
2. Password must have at least one upper case letter
3. Password must have at least one lower case letter
4. Password must have at least one number
5. The last three (3) passwords can’t be used
6. Three (3) or more consecutive characters of the users first or last name can’t be used.

Any user whose password does not meet the minimum requirements above will receive a rejection while attempting to change their password.

Advance warnings of upcoming password expiration will prompt the user five (5) days prior to expiration. These repeated reminders will appear with a countdown, until the expiration date upon which users will not be permitted to login until they have changed their password.

Attempts to login using an expired password will not succeed.

In the event you incorrectly enter your password five (5) times, your account will be immediately locked out. Your account will be unlocked after 5 minutes of wait time.

ENFORCEMENT

Violation of this policy will result in disciplinary action as follows:

A. Students will be subject to disciplinary charges brought under the Student Code of Conduct.

B. Employees who are part of a bargaining unit will be subject to disciplinary action brought under their respective collective bargaining agreement.

C. Employees who are not members of a bargaining unit will be subject to discipline by their supervisor.

D. Third parties who fail to abide by this policy will be dealt with as appropriate under the circumstances.