08-17-00 Computer Security Awareness and Training

PURPOSE

The purpose of this policy is to establish executive administration authorization to conduct Security and Privacy Awareness training for employees and to establish a comprehensive framework for cybersecurity awareness and training across the college community. It is designed to ensure that all employees understand their roles and responsibilities in protecting information technology resources. By promoting a strong culture of security awareness, this policy supports the protection of confidentiality, integrity, and availability of organizational information and systems, in accordance with applicable industry standards and best practices.

DEFINITIONS

Security and Privacy Awareness training consists of a curriculum of modules that cover best practices for password construction and handling, computer use, training in the techniques of hackers including phishing, vishing, spear phishing, malware, spyware, ransomware, and ways to recognize and avoid computer-based threats.

POLICY/GUIDELINE

I. **Purpose and Framework**

A. Nashville State Community College adopts the principles of the NIST 800 Series and requires its Technology Services Division to implement a comprehensive Security Awareness and Training Program. The program is designed to educate users on their responsibilities for protecting Nashville State systems and data.

II. **Employee Security Awareness Training**

A. Initial Training

1. All Nashville State employees must complete the 4-core required security awareness training within 30 days of hire.

B. Ongoing Training

1. Monthly security awareness training is required following completion of initial training.

C. Phishing Simulations

1. Employees will participate in periodic phishing simulations conducted by the TSD department.

2. A phishing failure includes:
    a. Clicking a malicious or simulated link
    b. Downloading a simulated attachment
    c. Responding to a simulated phishing message

D. Remedial Training

1. Employees who fail a phishing simulation must complete mandatory refresher training within 30 days of the failure.

III. **Training Concepts.** Security awareness training will, at a minimum, include instruction on the following topics:

A. Policies and procedures for protecting Nashville State systems and data, especially sensitive information

B. Separation of duties

C. Preventing, identifying, and reporting security incidents, including malicious code

D. Proper disposal of storage media

E. Correct use of encryption

F. Access controls and password management

G. Remote access policies

H. Individual data security responsibilities

I. Phishing, social engineering, and least privilege principles

J. Verify before trusting (zero-trust mindset)

IV. **Recourse for Noncompliance**

A. Authority and Compliance Requirements

1. Nashville State Technology Services Division has the authority to intervene when individuals fail to comply with this guideline. To remain compliant, employees must meet the following requirements:
    a. *Initial Training:* Complete required security awareness training within 30 days of initial system access.
    b. *Ongoing Training:* Complete assigned monthly training activities within 60 days of assignment.

c. *Refresher Training:* Complete required refresher training within 30 days of notification.

B. Noncompliance Actions

1. Employees who fail to complete required security awareness training within the specified timeframes will be considered non-compliant and subject to progressive enforcement actions as outlined below:

a. *Supervisor Escalation.* (Two Weeks Past Compliance Deadline)
If the individual does not complete the required training following the grace period, a notification will be sent to the employee and their supervisor or department head.

b. *Limited System Access.* (Two Weeks Past Supervisor Escalation)
Continued noncompliance will result in restricted system access, limiting exposure to sensitive systems and data until training requirements are fulfilled.

c. *Formal Action.* (Two Weeks Past Limited System Access)
If noncompliance persists, the individual's system account will be deactivated until completion of the required training.
At that point, the employee's supervisor must submit a service request to schedule an in-person training session at the Nashville State White Bridge Road campus to restore access.

C. Exceptions

1. Nashville State's TSD will accept exceptions for the following areas:

a. Temporary exemptions for short-term contractors or vendors with limited access to sensitive systems.

b. Medical or personal leave that prevents participation during the training window, with the requirement to complete it upon return.

c. Employees whose access is so limited or isolated that the standard training might not apply.

d. Employees and/or vendors who have already completed equivalent training through another recognized program within a recent timeframe

RELATED POLICIES

- TBR B-092 Security Awareness and Training
- NSCC 08-03-00 Acceptable Use Policy
- NSCC 08-04-00 Privacy Policy

- NSCC 08-05-00 Authorization for Use
- NSCC 08-06-00 Password Policy
- NSCC 08-07-00 Remote Network Access
- NSCC 08-08-00 Wireless Policy

CHANGE LOG

Date	Change	By
3/17/2021	Policy created	PAK
9/19/2023	Changed "at least annually" to "in monthly segments"	BR
04/28/2026	Policy rewritten to adhere to TBR B-092	BR

Approved by President's Cabinet 6/14/21; updated 12/11/23; updated 5/18/26