Information Technology Department

Security Awareness and Training Policy

Version:	1.3
Effective Date:	08/01/2022
Last Reviewed:	05/10/2022
Last Approver:	Javornda Ashton
Replaces:	N/A - New

PURPOSE

The purpose of this policy is to establish and maintain a security awareness program for Northumberland County Public Schools (NCPS) to educate users on how to interact with enterprise assets and data in a secure manner.

SCOPE

The scope of this policy includes all NCPS users who have an electronic account or handle physical data for NCPS.

RESPONSIBILITY

The Director of Educational Technology is responsible for the review, approval, and enforcement of this policy. This policy must be reviewed and updated annually, or when significant changes occur that could impact any safeguard in this policy.

COMPLIANCE

Compliance is expected with all NCPS policies and standards. Policies and standards may be amended at any time. If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a NCPS function, entities shall request an exception through a technology request in the IncidentIQ system at https://ncps.incidentiq.com. Any associate found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Security Awareness and Training Policy

IT should provide training and awareness communications for associates to ensure users are aware that fraudulent social engineering and other attacks occur, what users can do to recognize cyber security related attacks, and how users should report the attacks.

1. Training Requirements
    1.1. All users of NCPS systems should be trained:
        1.1.1. To recognize social engineering, ransomware, spam, and other attack vectors.
        1.1.2. On authentication and password best practices.
        1.1.3. How to identify and properly store, transfer, and destroy sensitive data.
        1.1.4. On causes for unintentional data exposure.
        1.1.5. To recognize and report potential, suspected, or actual Security Events.

1.1.6. To recognize and report out of date software patches and failures of NCPS automated tools and processes.
1.1.7. On the dangers of connecting to and transmitting data over insecure networks for NCPS activities.

2. Training Frequency
   2.1. New users receiving a NCPS account for the first time must receive security training within two days of initially receiving their user id.
   2.2. Existing users with a NCPS account should take security training at minimum annually.
3. Training Updates - Security awareness and training activities should be reviewed and/or updated at least annually and kept up to date to include current attack tactics.
4. Other Security Awareness Measures
   4.1. All users with a NCPS email address should receive anti-phishing tests at least twice a year.
   4.2. IT may occasionally also perform other cybersecurity tests and user awareness campaigns including educational emails, surveys, USB drop tests, or other.
   4.3. IT must track performance and enforce compliance with security awareness and training.

Policy References to IT Standards

K-12 Model Security Plan V1.0 – Security Awareness Training

1. Establish an annual program that includes quick training sessions for users with network, services, or data access.
2. Track user performance and enforce compliance.
3. Consider performing a training campaign during the school year. Too often, tasks are assigned to teachers and staff in the busy summer months when time is limited.
4. Allow a campaign ample time to be successful. Think months, not weeks.
5. Campaigns should include topics such as social engineering, ransomware, hygiene, data sharing, spam recognition, and generic security concepts.
6. Consider requiring training for new hires before network access is granted or within a window of time directly after hire. You may be able to add to your division's onboarding process.
7. There are many free resources for awareness training. You can also develop your own. However, cloud-based vendors make the management and tracking very easy to accomplish. There are also vendors that can work with SCORM compliant Learning Management Systems.