<center>**Delaware Area Career Center**</center>

<center>**TECHNICAL INFRASTRUCTURE DATA PRIVACY, SAFETY, AND SECURITY PLAN**</center>

Purpose

This document has been designed to provide clarity for the privacy, safety, and security of data throughout the Delaware Area Career Center's technical infrastructure for Council on Occupational Education (COE).

Support and Environmental Overview

The Delaware Area Career Center Information Technology team aims to provide value added services to students and staff of our organization. Currently we provide support across 14 locations which include two main campus buildings and 12 satellite programs.

- 2 Main Campus Buildings:
  - South Campus
  - North Campus

- 12 Satellite Programs:
  - Buckeye Valley Middle school
  - Buckeye Valley High School
  - Project Search - Grady Hospital
  - ABLE - (Vineyard Church)
  - Dempsey Middle school
  - Delaware Hayes High school
  - Delaware City Middle School
  - Big Walnut Middle school
  - Big Walnut High school
  - Equine Science
  - Zoo
  - Wildlife (Camp Lazarus)

Our technology team practices the principle of least privilege (PLOP) which is the practice of limiting access to the minimal level that will allow individuals to effectively perform their job duties with the lowest level of user rights possible. The department employs full time IT staff to maintain our technical infrastructure which includes our network, servers, backups, and end point technologies.

We maintain a Cisco based network and secure Windows based server environment which resides primarily in a virtualized environment. All networking equipment, servers, and end points are regularly patched per protocol at least once every 30 days, if not more. Our network configurations are backed up weekly and data and server configurations are backed up nightly with Veritas System Recovery to a network attached storage (NAS) devices. We have two NAS devices, one at North Campus and one at South Campus. Backups are stored onsite then replicated across sites to ensure redundancy.

Symantec endpoint protection is pushed to all computers to help ensure CIPA compliance on the network, as well as providing protection from malware, viruses, and other various content. We also push out patches to third party software packages when updates are available or when vulnerabilities are present through group policy and or with PDQ.

Our primary internet service provider (ISP) is currently metasolutions. Along with internet connectivity, metasolutions also provides us with web filtering on all devices connected through our network and also provide us with firewalls to further enhance our IT security.

Our servers and primary networking equipment have uninterruptible power supplies (UPS) connected to them to help ensure they have power in the event of a power fluctuation or failure. This helps to ensure systems do not crash with power fluctuation and allows IT staff to appropriately power down systems in the event of a prolonged power failure.

Passwords are required to be changed every 90 days and must meet the following criteria:
- May not use the previous 6 passwords
- May not contain the user's account name or parts of their full name
- Must be at least 8 characters in length
- Must contain characters from 3 of the 4 categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (A through Z)
  - Base 10 digits (0 through 9)
  - Non-alphanumeric characters (for example: !, *, %, #)

In addition to Information Technology procedures, every staff member and student at the Delaware Area Career Center are required to review and sign an Internet User Agreement during their onboarding (if staff) or at the beginning of every academic school year (if student).

In conclusion, through both policy and procedure, the Information Technology Department comprehensively provides top notch privacy, safety, and security of data throughout the Delaware Area Career Center.