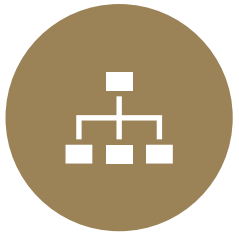
Technology Committee

MONDAY, NOVEMBER 6, 2023

INFRASTRUCTURE

CYBER SECURITY



DEPARTMENT

NO UPDATES

WEBSITE

CIS CONTROLS

Infrastructure

Previous meeting

- SAN is deployed and operational.
- Phone servers are deployed. Gateways are on hold as we await our Session Initiation Protocol (SIP) trunk to be installed on October 19. Currently we have Primary Rate Interface (PRI) is SIP allows Private Branch Exchange (PBX) to communicate over our network.

Update

Session Initiation Protocol (SIP) trunk has been installed; we are scheduling the gateway installations.

Cyber Security Updates

Previous meeting

- Core switches are in and provisioned to be installed in October.
- DMZ are up and operational. All Chromebooks, iPads and guest users are in a DMZ separate from our network.
- ACL will be configured with core switch installation.

Update

- Cores switches have not been installed yet, waiting on schedule.
- ACL will be configured with core switch installation.
- Antoinette King, founder of Credo Cyber will be speaking at the November 22 Superintendent Conference Day.

****Cyber Security work is an ongoing process imbedded in our daily activities.**

ANTOINETTE KING, FOUNDER OF CREDO CYBER, GUEST SPEAKER AT SUPERINTENDENTS CONFERENCE DAY.

Antoinette King, PSP has 21 years of experience in the security industry, holding roles including Engineered Systems Specialist, Operations Manager, Regional Sales Manager, and Key Account Manager.

Website

Reminder:

Website will need to be migrated to the new platform by January 2025.

CIS Control 5 – Users – Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Control 5.1 - Establish and Maintain an Inventory of Accounts (NIST PR.AC-1)

- Establish and maintain an inventory of all accounts managed in the enterprise.
- • The inventory must include both user and administrator accounts.
- • The inventory, at a minimum, should contain: the person's name, Username, start/stop dates, department
- • Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.

Control 5.1

We have checks and balances in place for user account creation and deletion. Only School Program secretary creates/removes accounts as requested by administration.

Usernames are matched with Email addresses and email addresses are recorded in our Employee database which allows that database to server as a user account inventory.

School Program Secretary will be auditing accounts Quarterly as previously we reviewed annually.

CIS Controls®
Version 8

Control 5.2 – Use Unique Passwords

- Use unique passwords for all enterprise assets.
- Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA

District passwords are required to be unique with a minimum of 8 characters. Faculty accounts are MFA protected.

CIS Controls®
Version 8

Control 5.3 – Disable Dormant Accounts (NIST PR.AC-1)

- Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported

We do not host dormant accounts. Vendor accounts are enabled and disabled as needed.

CIS Controls®
Version 8

Control 5.4 – Restrict Administrator Privileges to Dedicated Administrator Accounts (NIST PR.AC-4)

- Restrict administrator privileges to dedicated administrator accounts on enterprise assets.
- Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account

All departmental technician maintain a privileged account and a general account.