Account Management Guideline

Purpose

The quality and integrity of Cornwall-Lebanon School District's information system accounts are the only legitimate method by which Cornwall-Lebanon School District information systems may be accessed. Without active account management, the potential exists that legitimate users can use these accounts for illegitimate purposes. Additionally, the potential exists that these accounts can be usurped and used illegitimately to access Cornwall-Lebanon School District's information systems.

Scope

The Account Management Policy applies to all employees of Cornwall-Lebanon School District, including all temporary or contract workers. Specifically, it includes:

- Servers and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, content filters, and other devices that provide dedicated security capabilities.

Policy Statements

1. All information system accounts will be actively managed by appropriate administrative staff. Active management includes the acts of establishing, activating, modifying, disabling, and removing accounts from information systems.
2. Information system accounts are to be constructed such that they enforce the most restrictive set of rights/privileges or accesses required for the performance of tasks associated with that account. Further, accounts shall be created such that no one account can authorize, perform, review, and audit a single transaction to eliminate conflicts of interest.
3. Information system accounts are to be reviewed to identify accounts with inappropriate privileges (either too high or too low) on a semi-annual basis. Should information system accounts be discovered with inappropriate privileges, those privileges will be manually reset to the established level.
4. Information system accounts are to be reviewed to identify inactive accounts. Should information system accounts that are associated with an employee or third party be discovered that have been inactive for 30 days, the owners of the account will be notified of pending disablement. Should the account continue to remain inactive for 30 days it will be manually disabled.
5. Login attempts to information systems will be restricted such that after three failed attempts, they will be locked out. Lockout will be automatically lifted after 15 minutes or may be manually lifted by technology services.