Password Policy

Purpose

Passwords are the primary form of user authentication used to grant access to Cornwall-Lebanon School District's information systems. To ensure that passwords provide as much security as possible, they must be carefully created and used. Without strict usage guidelines, the potential exists that passwords will be created that are easy to break, thus allowing easier illicit access to Cornwall-Lebanon School District's information systems, and thereby compromising the security of those systems.

Scope

The Password Policy applies to all information systems, information components, and employees of Cornwall-Lebanon School District, including all temporary or contract workers. To ensure that passwords provide as much security as possible, they must be carefully created and used. Without strict usage guidelines, the potential exists that passwords will be created that are easy to break, thus allowing easier illicit access to Cornwall-Lebanon School District's information systems, and thereby compromising the security of those systems.

- Servers, and other devices that provide centralized computing capabilities.
- SAN, NAS, and other devices that provide centralized storage capabilities.
- Desktops, laptops, smart phones, tablets, 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.
- Cloud services, including but not limited to, infrastructure as a service, platform as a service, and/or software as a service.

Policy Statements

1. Passwords must be constructed according to set length and complexity requirements. As such, passwords must be 8 characters in length and must include upper and lower case letters, numbers and special characters.
2. Passwords will have both a maximum lifespan. As such, passwords must be replaced at a maximum of 45 days.
3. Passwords may not be reused any more frequently than every five password refreshes. Reuse includes the use of the exact same password or the use of the same root password with appended or pre-pended sequential characters.
4. Passwords are to be used and stored in a secure manner. As such, passwords are not to be written down or stored electronically. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
5. Passwords are to be individually owned and kept confidential and are not to be shared under any circumstances.