Password Management EHAAB

Every Crook County School District #1 employee and student is required and agrees to follow this policy as it applies, in its entirety, to all systems, network, and applications that process, store, or transmit sensitive information.

Crook County School District #1 requires that:

- All passwords must be changed at least once every 90 days. Systems not currently enabled to prompt for password changes will be reviewed and a project plan developed to bring system into compliance.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Unique, identifiable user accounts must be used; generic user accounts are not authorized unless approved by the technology coordinator.
- User-ids and passwords must not be inserted into a single email message or other forms of electronic communication but must be broken out into two separate emails.
- Passwords should not be transmitted utilizing any application source that uses only clear text; transmission must be encrypted.

Users must select strong passwords. Strong passwords have the following characteristics:

- Not contain the users account name or parts of the users full name
- Be at least eight characters in length
- Contain characters from three of the following four categories:
    - English uppercase letters (A through Z)
    - English lowercase letters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example,!,$,#,%)
- Be different from the previous 3 passwords
- Students in grades K-3 will have less stringent password requirements, approved by the technology coordinator, and supervised by a staff member

Note that poor, weak passwords have the following characteristics:

- The password contains less than six characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, and so on.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, and so on.
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (for example, secret1, 1secret)

Further, systems that authenticate must require passwords of users and must block access to accounts if more than five unsuccessful attempts are made.

Members of the workforce must follow these guidelines for passwords:

- Don't reveal a password over the phone to ANYONE
- Use different passwords for each of your accounts
- Always log off or "lock" your system if you leave it for an extended period of time, i.e. 5 minutes
- Avoid entering passwords when using unsecured Wi-Fi connections

- Avoid entering passwords on devices that you do not control, i.e. Internet Café', airports, coffee shops, hotels, public libraries, etc.
- Do not use the "Remember Password" feature of applications (web browsers, etc)
- Do not write passwords down and store them anywhere in your office. Further, passwords must not be stored on ANY computer system (including smartphones or similar mobile devices) without encryption.
- If someone demands a password, refer them to this document or have them call the technology department.

Password cracking or guessing may be authorized to be performed on a periodic or random basis by the superintendent or technology coordinator. If a password is guessed or cracked during one of these scans, the user will be required to change it.
Members of the workforce must not share their passwords with anyone, including administrative assistants. All passwords are to be treated as sensitive, confidential information.

The superintendent and technology coordinator are responsible for ensuring the implementation of the Password Management Policy. Failure to comply with this or any other security policy will result in disciplinary actions. Legal actions also may be taken for violations of applicable regulations and standards such as state and federal rules to include the Family Educational Rights and Privacy Act (FERPA).

References: The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

Adopted: August 16, 2016