Girl Scouts of Western Ohio

Password Guidelines

General Password Guidelines
Passwords are used for various purposes at Girl Scouts of Western Ohio. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and voicemail passwords. As a rule passwords are the responsibility of the end-user and must be managed by the end-user. When an employee leaves all computer and network passwords must be changed on the effective leave day.

Poor or weak passwords have the following characteristics:

- The password contains fewer 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, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Organization, place or event names like "Drexel", "Philly", "Super Bowl" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Passwords for Banner and Web Financials must begin with a letter and cannot contain these characters: $! & " or '
- Are at least seven alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Passwords must not be inserted into email messages or other forms of electronic communication. End Users should try to create passwords that can be easily remembered. For example, an End User can create a password based on a song title, affirmation, or other phrase, e.g. the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use any of these examples as passwords!

Password Protection Standards
End Users should not use the same password for Girl Scout accounts as for other non-Girl Scout access (e.g., personal ISP account, benefits, etc.). Also, End Users should select separate passwords for a Windows domain account, a network account, an OCN account, and an ISP account.

End Users must not share passwords with anyone; all passwords are to be treated as sensitive, confidential Girl Scout information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Don’t reuse passwords in the course of one year
- When changing a password, don’t derive it from a previous password (eg. TmB1w2R!-1 becomes 1TmB1w2R!-2)

If someone demands a password, the End User should refer her/him to this Policy.

End Users should not use the "Remember Password" feature of applications (e.g., Internet Explorer, Outlook, etc).

End Users should not write down passwords or store them anywhere in their offices. End Users should not store, without encryption, passwords in a file on ANY Computer System, including PDAs.

End Users must change their passwords at least once every 6 months (except system-level passwords which must be changed every 3 months).

When an End Users suspects that her/his account or password has been compromised, she must report the incident to the VP of Technology and change all of her/his passwords.

The VP of Technology may, on a periodic or routine basis, test the security of End User passwords. If VP of Technology determines that password is weak, the End User will be required to change it.