Starke County Government
Password Policy

Best Practice Passwords

Starke County Government depends on the strength and complexity or your passwords. It is an easy way to prevent bad actors from stealing information and/or installing malware on Government devices.

As part of Starke County's best practices, we recommend a mass password change in your department for all users.

Changing your password by following the guidelines listed below, will prevent 85% of hacker attempts on our systems.

In addition, Adding another layer of authentication such as multifactor (MFA) for these logins helps insure you are taking every measure possible to prevent future credential and account compromises.

How to Create a Secure Password

The following are requirements for creating a secure password.

1. Create a complex, minimum 12-character **passphrase** rather than a password.
   - Choose a phrase that you can remember but is not well known.
   - This phrase can include random words that are not often used together and should have nothing to do with you, your role in the company or your personal life.
     - For example: Manycatsswimtall^ or *Sandscallfastfar&
2. Do not reuse any portion of a previous password
3. Do not use your first, last or username in your new password
4. Must include 3 of the 4 following complexities:
   - Upper Case letters
   - Lower Case letters
   - Numbers
   - Symbols
5. Never share your password with anyone
6. This password should **ONLY** be used for logging into Government systems – not for any purpose outside of work.
7. If you believe your credentials have been compromised, change your password according to these guidelines and contact Starke County IT for assistance.

Password Change

- When changing or updating passwords, users will need to provide a second layer of verification.
- User will need to enroll and provide one of the following, personal security question, email generated code, application generated code.

Password Don'ts

- Do not share your password.
- If you can, do not write your password down.
- Do not use a word that can be found in a dictionary (even foreign).
- Do not make your password obvious. It should not contain any form of your name or User ID, and don't use obvious words such as "password," "guest," "user" or "admin."
- Do not use personal information, such as family members or pets names, your date of birth, social security number or other similar information. Since such information may be public, you should not use it in a password, even in combination with other characters.
- Do not use common words or acronyms; spelled forwards or backwards.
- Avoid using password-saving features, such as Microsoft's Auto Complete feature.

Password Dos

- Change your password immediately if you believe there is any chance your password has been compromised.
- Log off your computer before leaving work at the end of the day.
- Lock your keyboard if you leave your computer, even if only for a few minutes.
- Change your password early in the week. Changing it on a Friday or before a vacation will make it harder to remember upon your return.
- Change your password if someone on your team or in your area is suddenly put on disciplinary leave or fired.