POLICY:

It is the intent of the Board of County Commissioners to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

PROCEDURE:

1. Passwords are an important aspect of computer security. All employees (including contractors, vendors, and volunteers with access to county systems) are responsible for selecting and securing their passwords as outlined below.

2. This policy applies to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any County facility, or has access to the County's network.

3. User-level directory service passwords must be changed at least once per year. Passwords will be at least eight (8) characters long but may be longer. Each person is only authorized to login as themselves and not login for anyone else. Passwords must be treated as confidential information.

4. **All passwords should conform to the following guidelines**:

   a) Users should consider creating strong passwords.

   b) Passwords should be at least eight alphanumeric characters long, not a single word in any language, slang, dialect, jargon, etc., and should not be based on personal information, names of family, pets, etc.

   c) Where possible, Systems Management may implement password complexity enforcement via software.

5. **Password Protection Standards**:

   a) Do not use the same password for county accounts as for other non-work related access.

   b) Do not share County passwords with anyone, including administrative assistants, or secretaries, or supervisors, or reveal a password to co-workers for while you are vacation or to conduct business as there are other methods of sharing information based on email rules or network file rights. All passwords are to be treated as sensitive confidential information. Violation of this standard may result in disciplinary action.

   c) Password confidentiality is crucial to system security. Never give a password out to someone over the phone or in an email message even if they claim to be from the Office of Systems Management.

d) If someone demands a password, refer them to someone in Systems Management. This includes supervisors, elected officials, law enforcement personnel and attorneys.

e) Never use the "Remember Password" feature of applications.

f) Do not write passwords down and store them anywhere in your office or work area. If you store passwords in a file on ANY computer system (including mobile devices) use encryption on the file.

g) If an account or password is suspected to have been compromised, report the incident to the Systems Management immediately and change all passwords.

6. Use of Passwords and Pass-phrases for Remote Access Users

Access to the county networks via remote access is to be controlled by using either an encrypted password authentication or a public/private key system with a strong pass-phrase.

7. Any employee found to have violated this procedure may be subject to loss of network access. Additional disciplinary action may be taken, up to and including termination of employment.

8. For departmental or division-only software that has internal security not managed by a directory service, the ranking supervisor or manager has the responsibility to maintain the users, passwords, and internal security of that application. In such case, the Division shall enforce password rules and policies similar to those described herein. The Division Directors shall perform a quarterly audit of their system(s) and purge any expired accounts and shall review the access granted to the current users. Written affirmation of the quarterly security audit must be submitted to Systems Management.

9. Where possible and practical Systems Management will perform quarterly audits on those software systems for which they are responsible for password and login security and forward said reports to Division Managers for review and updates. Audits may occur at any time without prior notification.

FOOTNOTES & REFERENCES TO RELATED AR's: Supersedes AR 16.11 dated January 27, 2009; AR 16.06 dated June 22, 2010.