POLICY 305 PASSWORD SECURITY

1. Purpose. To provide a mechanism to maximize the security of information stored on Eau Claire County technology through the appropriate use of passwords. Passwords are assigned to each individual as a method to control and monitor their unique access to systems and information, and should never be shared with others.

2. Policy.

2.1 Eau Claire County's policy is to minimize the risk of breaches of security through theft of information technology accounts by providing password security guidelines.

3. Scope.

3.1 This policy applies to any and all personnel, including but not limited to contractors, students, volunteers, and Board members, who have any form of computer account requiring a password on the County network including, but not limited to a domain account and e-mail account.

4. Password Creation Guidelines.

4.1 Where possible, the Information Systems Department will implement automatic password expiration processes to ensure passwords are changed in a regular and timely manner.

4.2 Computer logon account passwords **MUST** meet the following requirements.

4.2.1 Must be at least eight characters long;

4.2.2 Must contain characters from three of the following four categories.

- English uppercase characters (A through Z);
- English lowercase characters (a through z);
- Base 10 digits (0 through 9); and
- Non-alphabetic characters (for example, !, $, #, %).

4.2.3 Must not contain the user's account name or parts of the user's full name that exceed three consecutive characters.

4.2.4 New passwords must be different from the previous six passwords. In addition, users should use the following guidelines when creating or changing a password.

4.2.5 Make each password unique – do not use the same password for multiple accounts or systems and do not use the same password for both personal and business accounts.

4.2.6 Do not use any words that would be listed in any language dictionary, slang, dialect, jargon, etc.

4.2.7 Do not use reverse spelling of words.

4.2.8 Do not use simple transformations of words, such as Tiny8 or 7Eleven.

4.2.9 Do not use alphabetic or numeric sequences such as “lmnop” or “12345” as part of a password.

4.2.10 Do not use common acronyms as part of a password.

4.2.11 Do not use names of people or places as part of a password.

4.2.12 Do not use part of your login name in your password.

4.2.13 Do not use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.

5. Password Protection.

5.1 Treat all passwords as sensitive, **CONFIDENTIAL** Eau Claire County information. Users should adhere to the following guidelines to protect their passwords.

5.1.1 Never write passwords down.

5.1.2 Never send a password through email.

5.1.3 Never include a password in a non-encrypted stored document.

5.1.4 Keep passwords hidden from colleagues, friends, or family (especially children) that could pass them on to less trustworthy individuals.

5.1.5 Never reveal passwords over the telephone.

5.1.6 Never hint at the format of a password.

5.1.7 Never reveal or hint at a password on a form on the Internet. Never use the "Remember Password" feature of application programs such as Internet Explorer, an email program, or any other program.

5.1.8 If using a personal County computer logon password on an account over the Internet, only use secure logins where the web browser address begins with https.//. Never use County computer logon passwords where the web browser address begins with http.// since this is not a secure login.

5.1.9 Report any suspicion of a password being broken to the Information Systems Department.

5.1.10 Be careful about letting someone see you type your password.

5.1.11 Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer." The user must re-enter his or her password in order to "Unlock" their computer.

6. When to Change Passwords.

6.1 Change your password if.

- You do not meet the above-listed guidelines.
- You have used the same password for more than three to six months.
- You shared your password with anyone.
- You have written your password down anywhere.

7. Other Considerations.

7.1 Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.