



PASSWORD POLICY

- 1.0 Purpose.** To develop a password policy for the organization that meets or exceeds the relevant guidelines in section 2.0 below.
- 2.0 Requirements.** Governing regulations and guidelines include: Sarbanes-Oxley Act, Gramm-Leach-Bliley Act as well as the Privacy Act. While the interpretation of the above acts is still in debate the fact that we have Social Security Information, personal address information and work history in some form we need to be able to protect this data from unauthorized access. While limiting file shares has been enough in the past, we now have to limit the IT staff's and Supervisor's access to this information. Most users log on to their local computer and to remote computers by using a combination of their user name and a password typed at the keyboard. Although alternative technologies for authentication, such as biometrics, smartcards, and one-time passwords, are available for all popular operating systems, most organizations still rely on traditional passwords and will continue to do so for years to come. Therefore it is very important that organizations define and enforce password policies for their computers that include mandating the use of strong passwords. Strong passwords meet a number of requirements for complexity – including length and character categories – that make passwords more difficult for attackers to determine. Establishing strong password policies for our organization can help prevent attackers from impersonating users and can thereby help prevent the loss, exposure, or corruption of sensitive information such as social security numbers, financial information, etc.
- 3.0 Scope.** All users of the system will be required to change their passwords at least annually. Passwords must meet the following structure. The password must contain six characters from the following four categories:
- English uppercase characters (A-Z)
 - English lowercase characters (a-z)
 - Base 10 digits (0-9)
 - Non-alphanumeric (for example: !, \$, #, or %)

The system will remember 1 password.

- 4.0 Responsibility.**
- 4.1 It is the responsibility of the IT staff to ensure that all password documentation sheets currently in hand are destroyed.
 - 4.2 It is the responsibility of the CEO to ensure that the IT staff does not have any user passwords.
 - 4.3 It is the responsibility of the CEO and IT staff to review this policy annually for adherence.



POLICY – 305
Rev. Level: B
February 13, 2009

5.0 History.

Name	Date	Rev. Level	Description of change	Effective Date
Mark Canfield		A	New Policy	
Deb O’Neil	2/13/2009	B	Update logo, CIO, CFO, EO Officer	7/01/2009

Auxiliary aids and services are available upon request to individuals with disabilities.

Equal Opportunity Employer Program
Paul Newlin – Equal Opportunity Officer
Phone: (814) 333-1286
TTY/TDD (814) 337-7205