Section:	Corporate Security	**Number:**	????
Title:	Password Policy	**Audience:**	Users
Issue Date:	May 31, 2011	**Supersedes:**	July 8, 2010

Policy Objective:

The purpose and goal of the Password policy is to establish standard guidelines for the creation of strong and secure passwords, the protection of those passwords, and the frequency of change.

Policy:

It is the policy of Generic Company that all users with approved authorization to the organization's network or system applications must be responsible for selecting and protecting their passwords. Users are defined as employees, guests, contractors, partners, and vendors.

It is also the policy of Generic Company that network passwords expire every 30 30 days which the user must select a new password. It is recommended that if any system application that does not automatically expire, the user should change their password to the system application frequently. All passwords must conform to the guidelines listed below.

Enforcement:

The IT Manager, or Executive Team, or both will enforce this policy. Violations of this policy may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

If any illegal activities are suspected, such as password cracking or theft of company property (physical or intellectual), the company may report such activities to the proper authorities.

Guidelines:

A strong and secure password is important to the organization’s security. Creating and remembering strong passwords doesn’t have to be difficult. All authorized users must adhere to the guidelines for constructing strong and secure passwords.

1. Secure passwords must be comprised of the following:
   - At least 8 characters in length; and
   - A mix of upper and lower case letters, numbers, and special characters (e.g. @#$%^&*()_+|~-=\` {}[]:”;’<>/)

   For example, the number 3 can be used for the letter E or a dollar sign ($) can be used for the letter S.

   Another method to creating a strong yet easy to remember password is to think of a sentence and then use the first letter of each word. For example, *The quick brown fox jumps over the lazy dog!* is easily turned into *Tqbfjotld!* as the password.

2. Secure passwords must **NOT** be comprised of any of the following:
   - Words that can be found in the dictionary;
   - Obvious keyboard sequence (e.g. asdfqwer); or
   - Easy to guess words such as birthdays, locations, phone numbers, or personal information about yourself, your spouse, pet, or children.

3. Passwords must be considered confidential data and treated with the same discretion as any of the organization's proprietary information in which users must **NOT**:
   - Share or disclose their passwords with others (co-workers, supervisors, family, and etc.) by inserting passwords into e-mail messages or other forms of electronic communication and over the phone;
   - Write down passwords and leave them unsecured;
   - Check the **Save Password** check box when logging into system applications; or
   - Reuse passwords or use the same password for different system applications, or accounts, or both.

4. Compromise of one password can have a catastrophic impact on the security of the network. Therefore, it is the responsibility of the user to report any suspicious activity involving their password(s) to the IT Manager and to change their password(s) immediately.

Procedure:	N/A	
Definitions:	***Authentication / Authenticating***	A method used to verify the identity of an authorized user and grant access to a system application or network.
References:	N/A	