**1.0 Overview**

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of CareerBuilder’s entire corporate and site network. As such, all Careerbuilder employees (including contractors and vendors with access to Careerbuilder systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

**2.0 Purpose**

The purpose of this policy is to establish a standard for creation of passwords (and to encourage strong passwords but not mandatory), the protection of those passwords, and the frequency of change.

**3.0 Scope**

The scope of this policy includes 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 Careerbuilder facility, has access to the Careerbuilder network, or stores any non-public Careerbuilder information.

**4.0 Policy**

**4.1 General**

* All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed every three months (90 Days).
* All production system-level passwords must be part of the Careerbuilder administered global password management database (Active Directory).
* All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed every three months (90 Days).
* Passwords must not be inserted into email messages or other forms of electronic communication.
* Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
* All user-level and system-level passwords must conform to the guidelines described below.
* Account lockout duration This security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. This feature has been added to the 2006 audit requirements and is now set to 0 (after five attempts, user must contact siteops to unlock).
* Enforce Password History: 5 previously remembered passwords cannot be used.
* Minimum length of Password will be 8 characters.

**4.2 Guidelines**

**A. General Password Construction Guidelines**

Passwords are used for various purposes at Careerbuilder. Some of the more common uses include: user level accounts, web accounts, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select passwords. Currently strong passwords are not required but may in the future, below are suggestions for recommended passwords.

Poor, weak passwords have the following characteristics:

* The password contains less than eight characters
* The password is a word found in a dictionary (English or foreign)
* The password is a common usage word such as:
  + Names of family, pets, friends, co-workers, fantasy characters, etc.
  + Computer terms and names, commands, sites, companies, hardware, software.
  + The words "Careerbuilder", "Atlanta1", "Peachtree1" or any derivation.
  + Birthdays and other personal information such as addresses and phone numbers.
  + Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  + Any of the above spelled backwards.
  + Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
* Strong passwords have the following characteristics:
  + Contain both upper and lower case characters (e.g., a-z, A-Z)
  + Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&\*()\_+|~- =\‘{}[]:";’<>?,./)
  + Are at least eight alphanumeric characters long.
  + Are not a word in any language, slang, dialect, jargon, etc.
  + Are not based on personal information, names of family, etc.
  + Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

**B. Password Protection Standards**

Do not use the same password for Careerbuilder accounts as for other non- Careerbuilder access (e.g., personal ISP account, option trading, etc.). Where possible, don’t use the same password for various Careerbuilder access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share Careerbuilder passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Careerbuilder information.

Here is a list of "dont’s":

* Don’t reveal a password over the phone to ANYONE
* Don’t reveal a password in an email message
* Don’t reveal a password to the boss
* Don’t talk about a password in front of others
* Don’t hint at the format of a password (e.g., "my family name")
* Don’t reveal a password on questionnaires or security forms
* Don’t share a password with family members
* Don’t reveal a password to co-workers while on vacation.
* If someone demands a password, refer them to this document or have them call someone in the IT Infrastructure Department.
* Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook Express, Netscape Messenger).
* Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
* If an account or password is suspected to have been compromised, report the incident to the IT Infrastructure Department and change all passwords.
* Password cracking or guessing may be performed on a periodic or random basis by the IT Infrastructure Department or its delegates.
* If a password is guessed or cracked during one of these scans, the user will be required to change it.

**C. Application Development Standards**

Application developers must ensure their programs contain the following security precautions.

Applications:

* should support authentication of individual users, not groups.
* should not store passwords in clear text or in any easily reversible form.
* should provide for some sort of role management, such that one user can take over the functions of another without having to know the other’s password.
* should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever

possible.

**D. Use of Passwords and Passphrases for Remote Access Users**

Access to the Careerbuilder Site Network via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

**E. Passphrases**

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The\*?#>\*@TrafficOnThe101Was\*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

**5.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**6.0 Definitions Terms Definitions**

Application Administration Account Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

**7.0 Revision History**

1.0 06/29/09 Robert Wicks

1.1 10/06/2009 Robert Wicks

1.2 07/21/2011 Ali Shahzad

1.3 02/21/2012 Brooke Covert

1.4 11/28/2012 Brooke Covert

**8.0 References**

The SANS Institute, “Sample Policies”

http://www.sans.org/resources/policies/Password\_Policy.pdf

Microsoft.com, “Selecting secure passwords”

http://www.microsoft.com/canada/smallbiz/french/sgc/articles/select\_sec\_passwords.mspx

**9.0 SiteOps Password Policy Settings (quick view)**

1.0 Active Directory Group Policy Settings

1. Enforce Password History

Determines the number of unique new passwords a user must use before an old

password can be reused.

CB Setting: 5 times

1. Maximum Password Age

Determines how many days a password can be used before the user is required to

change it.

CB setting: 90 days

1. Minimum Password Age

Determines how many days a user must keep their new password before they can change it.

CB setting: 1 days

1. Minimum Password Length

Determines how short passwords can be.

CB setting: 8 characters

1. Passwords Must Meet Complexity Requirements

Determines whether or not password complexity is enforced.

CB setting: enabled

1. Store passwords using reversible encryption

Determines whether or not password is encrypted.

CB setting: disabled