Proposed Password Policy

1.0 Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in

unauthorized access and/or exploitation the company's resources. All users, including contractors

and vendors with access to company 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 strong passwords, 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 <Company Name> facility,

has access to the <Company Name> network, or stores any non-public <Company Name> information.

4.0 Policy

4.1 General

• All system-level passwords (e.g., root, enable, Windows Administrator, application administration

accounts, etc.) must be changed on at least a quarterly basis.

• All production system-level passwords must be part of the InfoSec administered global password

management database.

• All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every

six months.

• User accounts that have system-level privileges granted through group memberships or programs

such as "sudo" must have a unique password from all other accounts held by that user.

• 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.

4.2 Guidelines

A. General Password Construction Guidelines

All users at the company should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

• Contain at least three of the five following character classes:

o Lower case characters

o Upper case characters

o Numbers

o Punctuation

o “Special” characters (e.g. @#$%^&\*()\_+|~-=\`{}[]:";'<>/ etc)

• Contain at least 8 alphanumeric characters.

This policy meets and/or exceeds those stated in the NIST SP800-53 standard.

Template Source:

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