

<b>System Document</b>		<b>Kinyo Virginia, Inc.</b>		
<b>Password Construction Policy</b>				<b>Issue: ITP017</b>
<b>Date: 05/26/2022</b>	<b>Approved: F. Koshiji</b>	<b>Issued By: I.T. Department</b>	<b>Revision: 001</b>	<b>Page: 1 of 2</b>

## 1. Overview

- 1.1 Passwords are critical components of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or network. This policy provides best practices for creating secure passwords.

## 2. Purpose

- 2.1 The purpose of this guidelines is to provide best practices for the created of strong passwords.

## 3. Scope

- 3.1 This guideline applies to employees, contractors, consultants, temporary and other workers, including all personnel affiliated with third parties. This guideline applies to all passwords including but not limit to user-level accounts, system-level accounts, web accounts, e-mail accounts, screen saver protection, voicemail, and local router logins.

## 4. Policy

- 4.1 To maintain the security of Kinyo internal databases, access by software programs must be granted only after authentication with credentials.

### Access to Database Usernames and Passwords

- Database passwords used by programs are system-level passwords as defined by the password policy.
- I.T. department must have a process in place to ensure that database passwords are controlled and changed in accordance with the password policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

## 5. Statement of Guidelines

- 5.1 Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of fourteen characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include "it's time for vacation" or "block-curious-sunny-leaves." Passphrases are both easy to remember and type yet meet the strength requirements. Poor, weak, passwords have the following characteristics:
  - Contain eight characters or less.
  - Contain personal information such as birthdays, addresses, phone numbers, or names family members, pets, friends, and fantasy characters.
  - Contain number patterns such as aaabbb, qwerty, zyxwvut, or 1234234.
  - Some versions of "Welcome123" "Password123" "Changeme123".

<b>System Document</b>		<b>Kinyo Virginia, Inc.</b>		
<b>Password Construction Policy</b>				<b>Issue: ITP017</b>
<b>Date: 05/26/2022</b>	<b>Approved: F. Koshiji</b>	<b>Issued By: I.T. Department</b>	<b>Revision: 001</b>	<b>Page: 2 of 2</b>

## 6. Policy Compliance

### 6.1 Compliance Measurement

The I.T. department team will verify compliance to this policy through various methods, including but not limit to, periodic business tool reports, internal and external audits, and feedback to the policy owner.

### 6.2 Exceptions

Any exceptions to the policy must be approved by the I.T. department in advance.