Password Construction Guidelines

1. Overview

Passwords are a critical component of information security. Passwords serve to protect user accounts; however, a poorly constructed password may result in the compromise of individual systems, data, or Be Data's networks. This guideline provides best practices for creating secure passwords.

2. Purpose

The purpose of thes guidelines is to provide best practices for the construction of strong passwords.

3. Scope

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

4. Statement of Guidelines

All passwords should meet or exceed the following guidelines:

- where possible, be randomly generated;
- contain at least 12 alphanumeric characters;
- contain both upper- and lower-case letters;
- contain at least one number (for example, 0-9);
- contain at least one special character (for example,!$%^&*()_+|~-=\`{}[]:";'<>?,/).

Passwords must not:

- contain words found in dictionaries, slang, dialects or jargon, either in English or other languages;
- contain words spelled backwards;
- contain words with numbers appended, i.e. 1pass, password3;
- contain words with simple obfuscation, i.e. p@ssw0rd, l33th4x0r, g0ldf1sh;
- contain doubled words, i.e. *passpass*, etc.;
- contain common sequences from a keyboard row, i.e. qwerty or other patterns, i.e. aaabbb, zyxwvuts, or 123321;
- contain numeric sequences based on well-known numbers such as 999, 0800, etc.;
- contain identifiers, i.e. jsmith123, 1/1/1970, 555–1234, one's username;
- contain any information related to an individual: license plate number, social security number, current or past telephone numbers, current or previous addresses, date of birth, sports team, relative's or pet's names/nicknames/birthdays/initials, etc.;
- contain work-related information such as building names, system commands, sites, companies, hardware, or software.

Passphrases

Passphrases generally are used for public/private key authentication. A passphrase is similar to a password in use; however, it is relatively long and constructed of multiple words, which provides greater security against dictionary attacks. Strong passphrases should follow the general password construction guidelines to include upper and lowercase letters, numbers, and special characters (for example, TheTrafficOnThe101Was*&!$ThisMorning!).

5. Policy Compliance

5.1 Compliance Measurement

The Head of Technology/DevOps team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Head of Technology/DevOps team in advance.

5.3 Non-Compliance

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

6. Related Standards, Policies and Processes

None.