Password Protection Policy

1. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Be Data's resources. All users, including contractors and vendors with access to Be Data's systems, are responsible for taking the appropriate steps, asoutlined below, to select and secure their passwords.

2. 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. 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 Be Data facility, has access to the network, or stores any nonpublic Be Data information.

4. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to guidelines on the Password Construction Guidelines page.

4.1.2 The same password must not be used for more than one account, i.e. every account must have a unique password.

4.2 Password Change

4.2.1 All system-level passwords (for example, root, enable, application administration accounts, and so on) must be changed on at least a quarterly basis.

4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every three months.

4.2.3 Password cracking or guessing may be performed on a periodic or random basis by the Technology Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection (General)

The following security precautions apply to the use of passwords generally:

4.3.1 Passwords must not be shared with anyone (including administrative assistants, secretaries, managers, co-workers while on vacation, or family members). All passwords are to be treated as sensitive, Confidential Information.

4.3.2 Passwords must never be inserted into email messages or other forms of electronic communication such as instant messages or SMS messages.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not hint at the format of a password (for example, "my family name").

4.3.6 Do not write passwords down and store them in an accessible location.

4.3.7 Do not store passwords electronically without encryption.

4.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.9 Any user suspecting that his/her password may have been compromised must report the incident to line management and the Compliance Officer and change passwords accordingly.

4.4 Password Protection (Development)

The following security precautions apply to developers and the use of passwords in development:

4.4.1 Internal to Be Data, where there is no option other than to share credentials, sharing of passwords must be authorised by the Head of Technology where passwords are shared internally, they must be shared using LastPass.

4.4.2 Where passwords have to be shared with parties outside Be Data, sharing must be authorised by the Head of Technology; passwords shouldbe encrypted using public key/asymmetric cryptography. If the party with whom a password is to be shared is unable to provide a public key, a cipher must be used to transmit the password, with the messages containing the encrypted password and instruction on how to decode each transmitted over a separate channel, i.e. password sent via SMS andinstruction on how to decode explained via instant message.

4.4.3 Applications/Systems must support authentication of individual users, not groups.

4.4.4 Applications/Systems must not store passwords in clear text or in any easily reversible form.

4.4.5 Applications/Systems must not transmit passwords in clear text over the network.

4.4.6 Applications/Systems must 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.

4.5 Use of Passwords and 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. Policy Compliance

5.1 Compliance Measurement

The Technology Team will verify compliance to this policy through various methods, including but not limited to, 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 Technology 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

Refer to Password Construction Guidelines.