PASSWORD POLICY

1 Overview

The BRITISH GOLD BANK Password Policy establishes the position that poor password management or construction imposes risks to the security of Company information systems and resources. Standards for construction and management of passwords greatly reduce these risks.

2 Objective & Purpose

This document describes the acceptable standards for password construction and management.

3 Scope

The requirements in this standard apply to passwords for any computing account on any Company computer resource, to the users of any such accounts, and to system administrators who manage or design systems that require passwords for authentication.

4 Standards

Password Construction:

Passwords shall have a minimum of 8 characters with a mix of alphanumeric and special characters; if a particular system will not support 8 character passwords, then the maximum number of characters allowed by that system shall be used.

Password Composition:

Passwords shall not consist of well-known or publicly posted identification information. Names, usernames such as the My Account, and personal ID numbers including date of birth other number are all examples of well know identification information that SHOULD NOT be used as a password. Additional password construction guidelines can be found in Appendix A – Password Construction Guidelines.

Password Management:

Passwords shall be memorized and never written down or recorded along with corresponding account information or usernames. Passwords must not be remembered by unencrypted computer applications such as email. Use of an encrypted password storage application is acceptable, although extreme care must be taken to protect access to said application.

Password Aging:

Users must change their passwords AT LEAST every month with the new password incorporating changed characters. Users will be prohibited from re-using the last 5 previously used passwords. Passwords can only be changed once in every 24 hours.

Password Reuse:

Care shall be taken to prevent the compromise of one username/password from compromising the security of multiple systems or resources. The username and password(s) used for your BGB accounts should never be used for any other non-BGB accounts and services.

Password Sharing and Transfer:

Passwords SHALL NOT be transferred or shared with others unless the user obtains appropriate authorization to do so. When it is necessary to disseminate passwords in writing, reasonable measures shall be taken to protect the password from unauthorized access. For example, after memorizing the password, one must destroy the written record.

Electronic Transmission:

Passwords SHALL NOT be transferred electronically over the Internet or any other electronic device, such as USB flash memory sticks and etc.

Requirements for System Administrators:

- Require Passwords for Login – Systems shall not be configured to allow user login without a password.
- Protect Against Password Hacking – System administrators shall harden their systems to deter password cracking by using reasonable methods to mitigate "brute force" password attacks. For example, it is better to lock an account for a few minutes after several failed login attempts, or detect where the attack is coming from and block further attempts from that location, or at minimum alert an alert in real-time that an attack is underway so that manual action can be taken.
- Logging – Practicable measures shall be put in place to log successful and failed login attempts.
- Changing Password after Compromise or Disclosure – System administrators shall, in a timely manner, reset passwords for user accounts or require users to reset their own passwords in situations where continued use of a password creates risk of unauthorized access to the computing account or resource. Examples of these situations include but are not limited to:
    - disclosure of a password to an unauthorized person; discovery of a password by unauthorized person;
    - system compromise (unauthorized access to a system or account); insecure transmission of a password; replacing the user of an account with another individual requiring access to the same account;
    - password is provided to IT support staff in order to resolve a technical issue;
    - account password is communicated to a user by the system administrator.
- Default Passwords – System administrators shall not use default passwords for administrative accounts.

Enforcement and Implementation:

Roles and Responsibilities BGB IT department is responsible for implementing, reviewing and monitoring internal policies, practices, etc. to assure compliance with this standard. CIO of BGB is responsible for enforcing this standard.

Consequences and Sanctions:

Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other BGB policies. Any device that does not meet the minimum-security requirements outlined in this standard may be removed from the BGB network, disabled, etc. as appropriate until the device can comply with this standard.

Exceptions:

Exceptions may be granted in cases where security risks are mitigated by alternative methods, or in cases where security risks are at a low, acceptable level and compliance with minimum security requirements would interfere with legitimate business needs. To request a security exception, contact the IT department at Appendix A:

Password Construction Guidelines:

Acceptable Methods to Create a Strong Password

- Use a minimum of 8 characters. Generally, the more characters you can use, the harder a password is to be cracked or guessed.
- Choose a password that is easy for you to remember but would be hard for another to guess. One useful approach is to use a sentence or saying to create a "passphrase" by using the first letters, capitalization, and special characters as substitutes. For example, "One ring to rule them all, one ring to bind them" may be used to create a passphrase like "1R2rtAor2Bt" that can be used as a very strong password.
- Passwords must include at least three of the four following types of characters.
- English uppercase letters (A through Z).
- English lower-case letters (a through z).
- Numbers (0 through 9).
- Special characters and punctuation symbols (Example: _, -. +, =,!, @, %, *, &, ", :, ., or /).
- Do not use the following characters \, ~ or <.
- Do not use a space or tab. Reuse of any of your last 5 passwords is prohibited. Tips for Creating a Strong Password.
- Avoid words, numbers, or known or public information associated with you. (e.g. Social security numbers; Names, family names, pet names; birthdays, phone numbers, addresses; etc.).
- Avoid using your login name or any variation of your login name as your password. If your login is 'Fredrick', do not use substitution or letter reordering. Examples would be 'fr3dr1ck', where the 3=e and the 1 (one)= i. Alternatively, do not use kcirderf (backwards) or add a digit to the beginning or end of the word (1fredrick or fredrick1).
- Avoid using the same character for the entire password (e.g., '11111111') or using fewer than five unique characters.
- Avoid common letter or number patterns in your password (e.g., '12345678' or 'abcdefgh'). They are the first things hackers will test.

- Substitution should not be used on common words or with common substitutions (e.g., 3=E, 4=A, 1=I, 0=O, etc).