Password Policy

Purpose

Passwords are an important component of information and network security. The use of a user id and password combination serves to identify and authenticate a user to system resources and information assets. It is only through authenticated access that the enterprise can be assured that systems and data are being used appropriately. As such, passwords must be constructed, used and protected appropriately to ensure that the level of security they imply is actually met.

The purpose of this policy is to provide the guidelines necessary for all of the employees of Banks DIH Limited to create appropriate passwords and to use them and protect them in an appropriate manner.

Scope

This policy applies to all employees of Banks DIH Limited who have any form of computer or application account that requires password access. Examples of accounts include:

- Workstation (desktop/laptop)
- iSeries Client Access terminal session
- Network
- E-mail system
- Internet
- Accounting application
- Customer information database

Please note: This list is not intended to be all-inclusive; it is simply provided for reference purposes.

Policy

General

1. Password construction, lifecycle and re-use parameters will be variable according to the classification of the system or data that they are intended to protect.

2. Passwords should not be based on well-known or easily accessible information, including personal information, nor should they be words commonly found within a standard dictionary.

3. Users will be notified one week in advance of password expiration. At that point, and at every subsequent login until a change is made, users will be prompted to select a new password.

4. Banks DIH Limited will use technical measures to ensure that users conform to the policy.

5. All passwords must conform to the guidelines outlined below.

Password Construction Guidelines

1. Passwords used to access data classified as “Secret” or the systems that host this data must be a minimum of ten (10) characters in length. Further, these passwords must use at least one character of the four character types, those being lower case letters, upper case letters, numbers and special characters.

2. Passwords used to access data classified as “Confidential” or the systems that host this data must be a minimum of ten (10) characters in length. Further, these passwords must use at least one character of three of the four character types, those being lower case letters, upper case letters, numbers and special characters.

3. Passwords used to access data classified as “Private” or the systems that host this data must be a minimum of nine (9) characters in length. Further, these passwords must use at least one character of two of the four character types, those being lower case letters, upper case letters, numbers and special characters.

4. Passwords are not needed to access data classified as “Public” or the systems that host this data, as long as these systems do not host data of a higher classification level and so no construction guidelines need to be set.

Password Lifecycle Guidelines

1. Passwords used to access data classified as “Secret” or the systems that host this data will have a maximum age of one (1) month and a minimum age of one (1) month. As such, passwords must be changed every month and cannot be changed more frequently. Where the application or system can only be specified to change on the basis of a variable number of days, maximum and minimum age will be set at thirty (30) days.

2. Passwords used to access data classified as “Confidential” or the systems that host this data will have a maximum age of three (3) months and a minimum age of two (2) weeks. As such, passwords must be changed every three (3) months and cannot be changed more frequently than every two (2) weeks. Where the application or system can only be specified to change on the basis of a variable number of days, maximum age will be set at ninety (90) days and minimum age at fourteen (14) days.

3. Passwords used to access data classified as “Private” or the systems that host this data will have a **maximum age of sixty (60) days and a minimum age of one (1) week**. As such, passwords must be changed every sixty (60) days and cannot be changed more frequently than every one (1) week. Where the application or system can only be specified to change on the basis of a variable number of days, maximum age will be set at one hundred and eighty (180) days and minimum age at seven (7) days.

4. Passwords are not needed to access data classified as “Public” or the systems that host this data, as long as these systems do not host data of a higher classification level and so no lifecycle guidelines need to be set.

Password Reuse Guidelines

1. Passwords used to access data classified as “Secret” or the systems that host this data may never be reused once they have expired. As such a completely new password is required at each expiry. “Completely new” is defined as having at least fifty percent (50%) of the characters different from the previous password.

2. Passwords used to access data classified as “Confidential” or the systems that host this data may be reused every **twelfth** password. As such a completely new password is required for the first five expiries; thereafter the first password can be reused. “Completely new” is defined as having at least fifty percent (50%) of the characters different from the previous password.

3. Passwords used to access data classified as “Private” or the systems that host this data may be reused every third password. As such a completely new password is required for the first two expiries; thereafter the first password can be reused. “Completely new” is defined as having at least fifty percent (50%) of the characters different from the previous password.

4. Passwords are not needed to access data classified as “Public” or the systems that host this data, as long as these systems do not host data of a higher classification level and so no reuse guidelines need to be set.

Password Protection Guidelines

1. Passwords are to be treated as confidential information. Under no circumstances is an employee to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, and family members.

2. Under no circumstances will any member of the organization request a password without the request coming from both a representative of the IT department and the user’s direct manager. Should a request be made that does not conform to this standard, immediately inform both the IT department and your direct manager.

3. Passwords are not to be transmitted electronically over the unprotected Internet, such as via e-mail. However, passwords may be used to gain remote access to company resources via the company’s Virtual Private Network or SSL-protected Web site.

4. No employee is to keep an unsecured written record of his or her passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access safe if in hardcopy form or in an encrypted file if in electronic form.

5. Do not use the “Remember Password” feature of applications.

6. Passwords used to gain access to company systems are not to be used as passwords to access non-company accounts or information. Similarly, passwords used to access personal, non-work related accounts are not to be used to access company accounts.

7. Each application, system and data point should be protected by a different password where possible. The use of the same password to protect all access is strongly discouraged.

8. If an employee either knows or suspects that his/her password has been compromised, it must be reported to the IT Department and the password changed immediately. If the minimum aging requirement has not been met for the password, the IT department will reset the minimum aging for the account allowing the user to create a new password.

9. The IT Department may attempt to crack or guess users’ passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

Enforcement

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