Disclosure &
Barring Service

TATA

TATA CONSULTANCY SERVICES

TCS/DBS Password Policy

Document Reference No:	TCS.04.368
Document Author:	Hatim Lokat *TCS Information Security Consultant*
Document Owner:	George Kuncheria *TCS Client Director* Paul Whiting *DBS Senior Information Risk Owner*
Version:	2.0

1.0 Introduction

1.1 Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire TCS/DBS Production network. As such, all TCS/DBS employees, contractors and third party suppliers (Hereafter referred to as 'Staff') providing service to the DBS and with access to TCS/DBS systems, network devices, applications and databases (Hereafter referred to as 'Systems') are responsible for taking all appropriate steps, as outlined in this policy, to select and secure their passwords

1.2 The purpose of this policy is to establish a standard for the creation of strong passwords, the protection/management of those passwords, and the frequency of change. The policy also outlines different types of accounts being used within the TCS/DBS Systems and standards for their creation and management.

2.0 Scope

The scope of this policy includes all TCS/DBS Staff who have or are responsible for an account, including privilege accounts (or any form of access that supports or requires a password) on any TCS/DBS Systems, that, has access to the TCS/DBS network, or stores any TCS/DBS information not in the public domain. It encompasses all systems owned or managed by the TCS/DBS Staff.

3.0 Standard Requirements

3.1 General Password standards

3.1.1 All TCS/DBS account passwords must conform to the following minimum standards where the operating system or platform supports them. Where systems do not support this standard, it must be documented and a risk assessment undertaken to identify additional compensatory controls and mitigating actions for those systems.

3.1.2 TCS/DBS system owners must, at the earliest opportunity, change default passwords installed by vendors at initial delivery of equipment and software.

3.1.3 The possession and / or use of password sniffing or other hacking tools are forbidden on the TCS/DBS network and infrastructure. .

3.1.4 Passwords shall be singular and unique to a user wherever possible.

3.1.5 Any password compromises must be logged as a security incident as defined in the TCS.04.385 TCS/DBS User Security Incident Handling Procedures

3.1.6 When a user leaves the employment of TCS/DBS or changes role, any privileged account passwords that they may have known must be changed wherever practical. On termination of employment, access including privileged access to all TCS/DBS Systems shall be disabled. (Refer: TCS.04.369 TCS Logical Access Control Policy for Information Systems and TCS.04.372 TCS Starter Movers and Leavers Process)

3.1.7 Computer screen savers must be password protected and activate after no more than 5 minutes of user inactivity. (Refer: TCS.04.371 TCS Secure Logon Procedures)

3.1.8 All TCS/DBS Staff with access to the TCS/DBS Systems t must treat passwords and / or other access credentials as sensitive information (that is, use similar controls as those you would use for your bank account / Debit card PIN number).

3.1.9 All Passwords must

a) Comply with the guidelines contained in CESG IS7.
b) Be changed at initial (first) login.
c) Be stored in irreversibly encrypted form.
d) Be changed immediately whenever accounts have been compromised.
e) Be significantly different from previous passwords.
f) Include all of the following elements below (complex password):
    a. *Lower case characters*
    b. *Upper case characters*
    c. *Numeric characters*
    d. *Any of these special characters ¬ ! $ % ^ & * ()_+ - = [] {} ; ' # @ ~*
g) Temporary passwords must be set to expire on first use and shall expire after 24hrs if not used

3.1.10 All Passwords must not

a) Be the same as or a derivation of:
    a. *Username*
    b. *First name*
    c. *Last name*
    d. *Password*
    e. *TCS*
b) Be viewable when entered
c) Contain two consecutive identical characters
d) Be allowed to change more than once within 24 hrs
e) Be written down
f) Be shared with anyone
g) Be transmitted in clear text over network
h) Be the same as the user ID/ account name
i) Be easy to guess, such as TATA, DBS or password
j) Be a spouse's name, partner's or friend's name
k) Be the owner's pet's name or child's name
l) Be the name of the operating system or hostname being used
m) Be a string of numbers or letters, like 1234, abcde
n) Contain information easily obtained about the user (for example, address or phone number)
o) Contain simple patterns of letters on the keyboard, like 'asdfg'
p) Be centred around favourite football team or sportsperson

3.1.11 Guidelines for choosing strong passwords.

a) choose a long phrase, a line from a poem, a lyric from a song or your own made up phrase
b) substitute some of the words for letters, as you might when texting (are = r, for = 4, you = u, to = 2 nothing = 0, be = b)
c) use symbols in place of words, such as '& for and' ; '@ for at or a'
d) pick the first letter of each word from the phrase

e) combine all of the above to make your password

3.1.12 Examples of strong passwords

a) We have nothing to fear but fear itself becomes ‘ Wh@2FbFi ‘
b) Momma always said, Life was like a box of chocolates becomes ‘ MasLw1@boc’
c) Tragedy, when the feeling’s gone and you can’t go on becomes ‘T!Wtfg&ucg0’

3.2 Account Standards

All accounts shall comply with guidelines contained in CESG IS7

3.2.1 Standard User account (non-privileged, normal windows, unix login accounts) must:

a) Be unique to each staff member / individual
b) Have a minimum password length of 9 characters (complex password)
c) Be changed at least every 30 days
d) Remember 6 history of passwords
e) Get locked out after 3 unsuccessful login attempts
f) Account lockout after unsuccessful attempts should be at least 30 minutes or until it is reset via Service Desk team
g) Have auditing enabled for account logon success and failure attempts

3.2.2 Privileged User Account (Standard user account with privileges to perform administrative function)

a) Be unique to each staff member / individual
b) Have a minimum password length of 9 characters (complex password)
c) Be changed at least every 30 days
d) Remember 6 history of passwords
e) Get locked out after 3 unsuccessful login attempts
f) Account lockout after unsuccessful attempts should only allow reset via Service Desk team
g) Have auditing enabled for account logon success and failure attempts

3.2.3 System / Application Administrator account (default system / application accounts created for e.g. administrator, root, oracle etc.) must:

a) Have a defined owner to the account
b) Have a minimum password length of 14 characters (complex password)
c) Be changed at least every 90 days
d) Remember 12 history of passwords
e) Get locked out after 3 unsuccessful login attempts
f) Account lockout after unsuccessful attempts should only allow reset via Service Desk team

g) Have auditing enabled for account logon success and failure attempts

h) Management Guidelines for Systems Administrators accounts:
   - Shall be used for admin related activities only
   - Shall be disabled if not required,
   - If the account is required, wherever possible it shall be renamed and password changed immediately upon installation and configuration of the systems or application
   - If these accounts act as ‘User to last resort’ (fail-safe support account that is used only if all the accounts are locked), then it shall be written down and stored securely.

3.2.4 Application Service accounts (application service accounts created during the installation of application and / or created for cross application connection / access) must:

a) Have a defined owner of the account. The owner can be the application owner as well.

b) Have a minimum password length of 14 characters (complex password)

c) Be changed at least every 180 days

d) Remember 12 history of passwords

e) Not permit direct login into the application through the account

f) Have a defined process for changing the password.

g) Have auditing enabled for account logon success and failures attempts

h) Management Guidelines for Systems Administrators accounts:
   - Shall be disabled if not required.
   - If the account has been created as default during the application installation, but cannot be disabled, then it has to be renamed and password changed immediately upon installation and configuration of the system or application

3.2.5 Shared accounts (accounts created to be used on systems/application by more than one employee) must:

a) Have a defined business case of account creation / usage and shall be approved by TCS Operations Security Manager

b) Have a defined owner of the account

c) May only be a normal user account

d) Have a minimum password length of 9 case-sensitive alphanumeric characters (complex password)

e) Be changed at least every 30 days

f) Remember 6 history of passwords

g) Get locked out after 3 unsuccessful login attempts

h) Account lockout after unsuccessful attempts should only allow reset via Service Desk team

i) Have auditing enabled for account logon success and failure attempts

3.3 Two Factor Authentication

3.3.1 Any user request for two factor authentication (software token and hardware token) shall be through IT service desk and approved by the user line manager and service delivery manager and be commensurate with users job responsibilities.

3.3.2 Infrastructure team shall issue all hardware tokens with a face to face identity check of recipient through ID badge and completion of service desk request with all the approvals.

3.3.3 All software token shall be sent through CJSM e-mail to the user in encrypted form and an activation / unlock code must be sent by CJSM e-mail to the user's line manager.

3.3.4 If a soft or hard token cannot be used (e.g. token damaged, forgotten token etc.) the user, upon approval from TCS/DBS Security team and line manager, will be issued with either a temporary replacement token or with a 10 digit fixed passcode set with an expiry of 24 hrs.

3.3.5 If the user forgets the PIN then, it has to be cleared through IT helpdesk. After help desk clearing of token PIN the user must set a new PIN at their next login.

3.3.6 The two factor authentication system shall send email notification to users for any change of setting to the user profile.

3.3.7 Appropriate logging and auditing shall be enabled for all accounts which must be monitored through the protective monitoring system.

3.3.8 The PIN required to support the one-time pass code shall follow the standards:

a) Shall be minimum of 4 numeric digits
b) Be changed at initial (first) login.
c) Be stored in irreversibly encrypted form.
d) Be changed at least on an annual basis
e) Be changed immediately whenever account have been compromised.
f) Must lock the account after 3 unsuccessful attempts until helpdesk reset
g) Must not be shared with anyone
h) Must not be transferred in clear text over the network

3.4 Password reset/forgotten process

In an event of forgotten password following process shall be followed:

a) Users must raise the Service Desk ticket for password reset.
b) The ticket will be actioned by Service desk team / TCS Security team (in case of privilege accounts) and verify the identity of the user (with the valid physical ID badge) before resetting the account with one time password.
c) The one time password will have to the changed on first logon and will expiry if not used within 24hrs.
d) The new one time password will be communicated to the user in person.
e) The service desk team will then close the ticket appropriately.
f) When the user cannot be physically present for identity verification, the local Tech Services team at user's location will verify the identity of the user (with

physical ID badge) and then sent an email to IT service desk with the Service desk ticket number and confirmation on user identity verification. The Service desk team would then reset the password and communicate to the user via an appropriate channel

4.0 Breach of Policy

TCS/DBS Security team will ensure that all users of TCS/DBS Systems are provided with the necessary security guidance, awareness and, where appropriate, training to discharge their security responsibilities. Non-compliance with this policy may result in disciplinary and / or criminal proceedings against the user.

5.0 Exceptions

It is understood that there would be scenarios where due to systems/application limitations and other parameters, all the standards in the policy will not be possible to be achieved. Any deviation and / or need for exception to this policy shall be documented and shall have a formal approval from TCS/DBS Security team.