STATE BANK OF INDIA

Sri Lanka

Password Creation and Maintenance

- Sharing passwords is a security risk.
- Do not divulge your password to anyone.
- Enter your user-id password only in the space provided for- that you are normally used to.
- Any changes from normal make sure there is no attempt to steal your personal information before providing it.
- Do not provide user id passwords on any page popping up by clicking on a hyperlink received through email. Better practice would be to log into the service by typing in the URL in the address bar after making sure the page opening up is from the genuine service provider.
- Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
- Change passwords at regular intervals.
- **Unique Characters**: An acceptable password must have at least five (5) different characters. Repeated characters can make for palindromes and make it easier to crack.
- **Character Types**: An acceptable password should be minimum 8 characters to maximum 20 characters and should include a combination of alphabets having upper case, lowercase, special character and numerals.
- **Long Alpha Sequences**: A strong password should preferably not have an alphabetic sequence any longer than three (3) characters.
- **Long Digit Sequences**: An strong password should preferably not have a digit sequence any longer than two (2) characters.
- **Forbidden Characters**: There are a few characters that will cause problems if used in a password - the "delete" character is one of the obvious ones.
- **Writing down your password**: One should never write down a password. Someone may discover the password. Make the password difficult for others to guess or crack but easy for you to memorise and remember.
- Passwords should not be any of the following:
    - Dictionary words (including foreign and technical dictionaries)
    - Name of a person or a thing, a place, a proper noun, a phone number or a vehicle number
    - Simple pattern of letters on keyboards
    - Any of the above reversed or concatenated
- One possible method for picking a good password is to make up your own acronym.
- Do not let your computer remember your password. Do not accept auto complete option provided by your computer/ browser.

- As far as possible do not use un-trusted system to access sensitive service. If you must, change the password on the first occasion immediately thereafter from a trusted system