***** **VERY IMPORTANT INTERNET BANKING SECURITY RELATED INFORMATION** *****

Many of our customers are receiving the unsolicited email from some fraudsters. Customers are being asked to enter their User-ID and Passwords and registered mobile numbers in the attached link. The fraudsters are using the ID and passwords entered by the customer and using the details to withdraw money fraudulently through Internet Banking. PLEASE IGNORE AND DELETE ANY SUCH EMAIL IF YOU HAPPEN TO RECEIVE IT.

Please note the following online Safety Tips to protect yourself:

- ✓ Your Internet banking ID and password are your keys for accessing our online services. Only the right combination of these allows you access.
- ✓ Don't use links to access our site. Always type the website address www.syndicatebank.in. Do not use a link in google/yahoo/bing etc. as this may take you to a phoney website that may look exactly like ours designed to trick you and collect your personal information. This is called **Phishing**. Sometimes links to such websites are contained in email messages purporting to come from financial institutions/RBI/Income-Tax Dept. etc.
- ✓ Also please ignore any POPUP in any website asking for your ATM card details like pin, DOB, expiry date, CVV etc.
- ✓ Review your bank statements / transactional SMS for any unusual transactions or withdrawals and notify the bank immediately if you suspect any discrepancies.
- ✓ Logging in: Ensure you enter your correct password(s) without the details being inadvertently disclosed to someone who may be looking over your shoulder.
- ✓ Logging off: Always remember to log off from the Internet Banking session and close your browser when you have finished your online banking. This will clear all traces of your visit from the PC's memory.
- ✓ Make sure you have the latest OS security updates and patches.
- ✓ Install and regularly update anti-virus software.
- ✓ Use personal firewalls and anti-spyware programs.
- ✓ Configure your browser settings to ensure that you are warned each time you access secured or unsecured web pages.
- ✓ Do not cache secure web pages if your computer is accessed by other people.
- ✓ Take care where you go online from. If you can, try to avoid using Internet Banking at Internet Cafés, Libraries, and other public sites to avoid the risk of information being copied and abused after you leave.

- ✓ Change your passwords - Always change passwords that may have been compromised.
- ✓ Contact the bank if you think someone else knows your Internet banking password
- ✓ Password-protect your computer: Use a password on your computer to prevent unauthorised individuals from accessing your information.
- ✓ Disable the 'AutoComplete' function within your browser: This will help prevent others from seeing personal information. On Internet Explorer, for example, the ‘AutoComplete' function remembers data you have input, sometimes including passwords. Typically, the browser's own Help function will tell you how to disable the 'AutoComplete' function. If you are unsure how to do this, you may need to ask someone.
- ✓ Buy from well-known companies if you are doing e-commerce transactions and only provide bank information during secure sessions.
- ✓ Never leave your computer unattended while logged on to Internet Banking.
- ✓ If you visit any questionable website before Internet Banking, we recommend you close your browser and restart it before proceeding to Internet Banking.
- ✓ Keep your password to yourself - Don't be tempted to share your User IDs, passwords or any unique personal identifiers/details with someone else. Nor should you supply personal information to anyone over the phone or to a web site unless you have satisfactorily verified the identity of the recipient of such information.
- ✓ Memorise your passwords; do not keep any records of them in your wallet / purse or store as a file in your computer. If you really need to record your password then use a code system, e.g. transpose some of the letters.
- ✓ Be unique - Try and create passwords that are unique and not easy to guess.
- ✓ Use letters, numbers and special characters in your password
- ✓ Be different- Avoid using the same password for different services.
- ✓ Don't be personal - Do not be tempted to use passwords that can easily be guessed e.g. your name / spouse/children’s/pet's name, your date of birth, telephone numbers.
- ✓ Change your passwords- Always change passwords that may have been compromised. Even otherwise, Change your password regularly.
- ✓ Be wary of opening any unexpected email messages with attachments
- ✓ Keep your email secure
- ✓ Never send sensitive information by email

Internet Banking Cell

Syndicate Bank