For Your Security,

1- Ensure that you change your password regularly.

2- Please do not share your user name and password with any other person.

3- Passwords and codes should be kept secret – they shouldn’t be written down or given to other people to use, nor should they be given out over the phone or in email. Make sure no-one can see you when you enter passwords or PINs. Passwords should be well-chosen so as not to be easily guessable, avoiding standard personal info like birthdays.

4- Don’t let other people use your cards – keep them in a safe and regularly check that your cards are OK.

5- Never provide confidential or personal data by electronic mail or by any other means, even if the request is made by an apparently legitimate source. BKT will never require your personal data without your presence.

6- Don't provide identity or other confidential information without confirming that the site is secure. Check that the address begins with https:// followed by the respective name of the required site and that the page shows a padlock in the lower or upper toolbar.

7- Do not allow any other person to use your device as you are logged into Internet/ Mobile Banking

8- Install antivirus software and keep it up to date at all times. Failure to update antivirus software is the same as not having it.

9- Use a firewall to filter Internet traffic entering and leaving your computer.

10- Keep on the watch for security updates provided by reliable software manufacturers and apply them in accordance with the instructions supplied.

11- Don't access, through links, any sites that require you to provide personal or confidential/ sensitive information or allow you to carry out banking transactions. Always type in the full address of the site that you want to access in the respective bar.

12- Don't open electronic mail messages without checking the identity of the sender and the subject. If you have any doubts as to the origin of the message delete it immediately and don't open any file or attachment it may contain.

13- Please do not do any banking transaction on computers open to public access. Some different type of hacking programs enables hackers to access your account details and personal information through computers which are open to public access.

14- Please show utmost sensitivity not to use web pages which are opened through mails or other platforms. Do not enter your Internet Banking over any other page.

15- After having entered Internet/ Mobile Banking you will be informed about your last login date and time in the main page. In the light of this information you can check whether your account has been used by any other person after your last usage.

16- Keep an eye on your account – check your account at least every two-four weeks. If you're on old-fashioned paper statements, you need to read them within two weeks of their arrival.

17- Keep the devices you use to access online banking well secured – ensure that any devices (tablet, smartphone, PC, laptop etc.) used to access online banks are kept updated with the latest security patches. This includes security software such as anti-malware and firewalls. Don't run any pirated software. Lock your devices with a passcode, and make sure you log off when you're done with an online banking session.

18- Report any incidents or anything suspect to the bank – tell BKT promptly if you think anything is amiss, and then follow their instructions.

19- In you are a user of Mobile Banking Application

a. a. Activate your mobile device's code lock
b. b. Don't save your access data such as PIN and Transaction Authentication Number (TAN) Personal Access Number (PAN) etc. on your mobile device, and always cover the device so no-one can see them when you enter them
c. c. Only use the most up-to-date system version of your mobile device
d. d. If possible, use up-to-date virus protection software and a personal firewall

20- After having completed your transaction please click the secure exit button and close your Internet Browser/ Mobile Banking Application.

21- For a secure usage of the apps in your mobile device, we recommend not to use rooted/jail broken devices.