

## **Privacy and security measures**

### **How we protect you**

At BCP Bank (Mauritius), we believe that the confidentiality and security of your information is of utmost importance. Our systems and security procedures are designed to keep your personal and financial data confidential at all times.

However, You also have a significant role to play and should adopt the following practices in order to keep your personal and financial information protected from unauthorised use.

### Security regarding your Logon Information

Your Internet banking logon information is your access to your accounts online and should be kept confidential.

### Client ID

Your client ID is computer generated and provided by the bank.

### Personal code

Your personal code should contain only numbers. To improve authentication security, BCP Bank (Mauritius) is using a digital grid (virtual keypad). The digits are displayed randomly on the grid.

### Personal code

Your Personal code is the key to your online account information and you are recommended to:

- Protect and change your Personal code on a regular basis - every 30-60 days is a suggestion.
- Change your password immediately if you believe that your password has been exposed.
- Create a personal code which is unique to you and which cannot easily be guessed by someone else.
- Avoid associating the personal code with anything personal such as birth dates, telephone numbers, or other familiar numbers.
- Memorize the personal Code and never to write it down or reveal it to anyone.



Client using OTP (One Time Password) is requested to take all precautionary measures concerning the access to their phone data, to inform the Bank immediately in the event they loses their mobile phone or change their mobile phone number.

Your attention is drawn to the fact that no one at BCP Bank (Mauritius) will ever ask you for your login ID or personal Code.

You are strongly advised not to give out any personal information to anyone on the telephone or from a website. Reputable companies will not ask you for your password or Personal Identification Number(s) (PIN) through email or over the telephone.



You are recommended to contact the bank if you receive unusual telephone inquiries regarding your accounts or unusual online requests for account information.

### Your Online Protection

You are advised:

- To install firewall software on your Personal Computer ('PC') to help prevent unauthorised individuals or information from entering your computer system. This is important for computers that use a broadband connection to access the Internet
- Anti-virus scans should be run regularly on computer systems using an up-to-date antivirus software, in order to detect malwares. Anti-virus software can scan the incoming and outgoing email and attachments for computer infections like worms, viruses, Trojan Horses and other malicious code that can affect the computer files and operation;
- Ensure that your computer has the latest version of an antivirus software where updates are done regularly;
- To keep the software of your PC updated and apply all security patches for the computer operating system to keep the security information updated;
- To consider acquiring anti-spam software to filter unwanted email or spam from incoming email list until it is deleted;
- Not to input personal information on a website form or application that does not display the "https://" before a website address or does not display a padlock symbol in the lower right hand corner of the webpage. This commonly ensures that the online session is in a secured environment and that the personal information entered is protected;



- To password protect your PC to prevent unauthorised individuals from accessing your information and change it every 30 - 60 days;
- To disable the 'AutoComplete' function to prevent others from seeing your logon information each time the Internet Banking is used;
- To always log off and close your browser after every online banking session and shut down your PC when not in use; Not use Internet Banking at Internet cafés, libraries, and other public sites to avoid your information from being copied, traced or re-entered after you have left
- Use internet banking only on secure WiFi Networks. Avoid using free-wifi in public places where security measures are not enforced.
- To read the privacy policy of the websites visited to learn about information privacy and how it is used in email offers, advertisements or sweepstakes. Learn how to remove your name from their promotional database to eliminate future unwanted email or spam;
- To verify the source of your emails before opening them and always run anti-virus software before opening email;
- Not to send any sensitive, personal or financial information unless it is encrypted on a secure website from a trusted source;
- To be aware that there are emails and websites designed to trick consumers and collect personal information. If you receive an email or a page link requesting confirmation of personal details, do not input information - even if the page appears legitimate;
- Not to respond to a chain letter email in the event that an attachment contains a computer virus. The best response is to delete it;



- Not to open an email or email attachments from unknown sources.  
Scan emailsthrough your anti-virus software first;
- Not to double-click on an email attachment that contains an executable file or files with the extensions 'exe ' 'com ' or 'vbs ' unless you can trust the source.
- Do not share personal or confidential information on the net or social media.

### Your offline protection

You are strongly recommended:

- Not to give out your Internet Banking client ID or Personal Code or any personal information to anyone on the telephone, from a website or otherwise. No one at the Bank's level will request such kind of information;
- Not to share access to your PC with strangers;
- To disable the 'File and Printer Sharing' capabilities on your computer to prevent anyone on the Internet from browsing or deleting your computer files;
- To review your bank and credit card statements for unauthorised transactions or withdrawals and notify the bank immediately if any discrepancies are suspected on the statement. The transactions and purchases may also be verified through Personal Internet Banking or Business Internet Banking;
- To be up to date dated on email news and the steps you may take to help keep your online experience secure.

Should you be the victim of an illegal activity on your account:

**BCP BANK  
(MAURITIUS)**



You are recommended to notify the bank immediately on **2071000** if you suspect that you may be a victim of fraud or if you suspect that there may be illegal activity on your accounts.

Moreover, you are also advised to file a police report and obtain copies of the report so that you may share and reference it with your creditors.

NB: The use of our Online Banking Services is subject to the terms and conditions set out in your agreement with the Bank including (but not limited to) those set out in the document 'Convention de Compte - Particuliers' or 'Convention de Compte - PME / PMI et Corporates' as may be applicable.