CLIENT INFORMATION SECURITY GUIDELINES

Banque BEMO SAL is committed to minimizing the risks of using online services, and has invested in adequate systems and processes to protect you when using our network. **Online security is a shared responsibility.** As your options for banking online grow, so does your need to safeguard your privacy and security while using the internet on your personal computer, tablet or mobile device. **This brochure is to help you understand what you should do to minimize these risks including general guidelines on protecting your information and assets.**

PROTECTING YOURSELF AND YOUR IDENTITY

The Bank will never ask you to provide the below by e-mail or SMS:

- Passwords
- Account Numbers
- Card Numbers
- User Names
- Any other confidential or private customer information

Fraudulent e-mails may be designed to appear as though they were originated from Banque BEMO SAL, therefore:

-**Don't respond to e-mails that claim to be from your bank (or any other company) requesting your account details**. No bank is ever likely to approach you this way

-**Be careful about what (and where) you click online**. Keep in mind that links you receive in emails or in messages on social networking sites can be harmful or fraudulent, even if they appear to come from friends. Requests for personal information or a call for immediate action are almost always a scam. If you suspect the link might give you a virus or steal personal data, don't click on it. Talk to the sender directly and make sure it came from them.

-**Be mindful of how much personal information you share on social networking sites.** The more you post about yourself, the easier it might be for someone to use the information you post to access your accounts, steal your identity and more. Maximizing your privacy settings on social networking sites can also help protect your personal information.

KEEP YOUR COMPUTER PROTECTED

1) Install a robust anti-virus, anti-spyware and firewall software on your computer and other devices and configure it **to update regularly**.

2) Perform regular scans of your systems for malware and other risks.

3) Operating system providers such as Microsoft, periodically releases updates and patches that improve the security of your operating system. You should periodically check for these updates and keep your system current or configure it to do so automatically.

4) Use strong passwords for all your accounts. A strong password (one that is not easily guessed by a human or computer) will have 10 or more characters, including letters, numbers and symbols. Make sure to use different user IDs and passwords for your financial accounts and for any other sites you use online. Change passwords regularly at least every 60 days with no repetition. Passwords should not be written down or recorded in any form. Never share your passwords with anybody **Change your password IMMEDIATELY if you suspect it has been revealed or compromised**.

5) Disable the auto complete function in your browser, which can store or retain user IDs and passwords that can be used by others.

6) Do not open email attachments or click on links from strangers. Delete junk or chain emails. Watch out for file extensions and delete any files that have double extensions as they are likely to be a virus. Do not install software or programs of unknown origin in your PC. Before you run any software or program, ensure that it comes from a trusted source.

7) Always log off from your online session when you leave your computer unattended, even for a while, and clear your browser cache after logging off.

Please report directly to Banque BEMO SAL any suspicious calls, e-mails, messages or if your online-banking user name or password were stolen.

Banque BEMO SAL staff and management have pledged to apply all the necessary measures to insulate your confidential information and to give you the directions needed on how you can protect yourself from the diversified risks and threats; however your awareness and application of the aforementioned steps and guidelines remain ESSENTIAL in helping us secure your information.