Important Notes for Security in relation to Cyberbanking and BEA Mobile Banking

These important notes apply to both personal and corporate Cyberbanking services and BEA Mobile Banking. Please read and adopt the following security precautions before using Cyberbanking or BEA Mobile Banking:

(1) Keep your Cyberbanking account number, ATM card number, user identity ("ID")/name and Personal Identification Number ("PIN") for all Cyberbanking, ATM, BEA Mobile Banking and BEA App channels and i-Token Service confidential at all times. Ensure that you (and, where relevant, any Authorised Person) do not disclose or share this information with anyone - including any joint account holder or any financial management software or programs - under any circumstances, and do not transmit this information via email or any instant messaging software/programs. Never assign the same PIN for any other service (such as your internet connection, or login for another website).

In addition, choose login credentials, user ID/name and/or PIN which are significantly distinct from those used for your other personal accounts, especially from social media accounts.

(2) Notify The Bank of East Asia, Limited ("BEA") immediately of any actual or possible unauthorised use of your Cyberbanking account number, user ID/name and/or PIN, and send confirmation in writing to BEA without delay. If your device with i-Token Service/Biometric Authentication activated is lost or stolen, you should also contact our Customer Services Hotline - Internet on (852) 2211 1321.

(3) It is not necessary for anyone affiliated with BEA to know your PIN. Do not disclose or share such information with anyone, including BEA staff or police officers, under any circumstances.

(4) Contact BEA for confirmation immediately whenever a website or app claiming to originate from BEA looks suspicious to you.

(5) Do not install or use apps, applications, programs, or software from untrustworthy sources on your computers, mobile phones or tablet devices (collectively referred to as your "device") to access Cyberbanking, BEA Mobile Banking or BEA App. Understand the permissions of applications carefully before you install them.

(6) Use the version of operating system and browser recommended by BEA to access Cyberbanking, BEA Mobile Banking or BEA App. Keep the operating system and apps installed on your device up to date with the latest security patches.

(7) Only download BEA's official mobile application(s) from official stores (App Store or Play Store). Do not use the app on any "jailbroken" or "rooted" devices.

(8) Only login to Cyberbanking through www.hkbea.com. Do not open any email attachments or click on URLs or hyperlinks embedded in any email, SMS, instant message, QR code, search engine, or any untrusted source to access Cyberbanking.

You should access the BEA website by typing www.hkbea.com into the web browser or through bookmarking the BEA website.

(9) When accessing Cyberbanking, BEA Mobile Banking or BEA App on your device, check what other applications are running in the background and stop unnecessary application from running.

(10) Disable your browser's "AutoComplete" function. On some browsers, this function remembers the data you have input previously. Refer to your browser's "Help" function if necessary.

(11) Make sure that all other browsers are closed before logging in to Cyberbanking or BEA Mobile Banking or BEA App.

(12) Every time you log in to Cyberbanking or BEA Mobile Banking, please verify your previous login date and time on the first page.

(13) Avoid sharing your device with others, and do not allow any third party's biometric credentials to be stored on your device. Do not use other people's devices to log in Cyberbanking, BEA Mobile Banking or BEA App.

(14) If any suspicious screens pop up, or any unusual login screen request appears asking you to provide additional personal information, or if your device's network/traffic is unusually slow, you should log out Cyberbanking or BEA Mobile Banking immediately and scan your device, with the most up-to-date version of your virus protection software.

(15) After you finish a session, make sure to log out of Cyberbanking or BEA Mobile Banking, and clear your browser cache.

(16) Check your transaction history and e-statement regularly. Notify BEA immediately if you discover any problems (such as a lost ATM card) or any suspicious transactions and/or unauthorised transactions.

(17) Never leave your device unattended while using Cyberbanking or BEA Mobile Banking or let any other person use your Cyberbanking or BEA Mobile Banking. To prevent unauthroised access by others, set up auto-lock or a passcode, and enable remote wiping for your device in case of any loss/theft.

(18) Do not use a public computer or public Wi-Fi network to access the Cyberbanking or BEA Mobile Banking. Choose encrypted networks when using Wi-Fi and remove the settings of any unnecessary Wi-Fi connections. Disable any wireless network functions such as Wi-Fi, Bluetooth, near-field communication (NFC) when not in use.

(19) Take precautions against hackers, viruses, spyware, and any other malicious software when sending and receiving emails, opening email attachments, visiting

and disclosing personal/financial information to unknown websites, and downloading files or programmes from websites. Do not browse suspicious websites or open suspicious emails or click on the hyperlinks and attachments (including but not limited to encrypted files, compressed files (zip)) or scan QR code in suspicious emails or messages received through WhatsApp, Line, WeChat, and other e-communities.

(20) Use proper firewalls, anti-virus and anti-spyware software, keep them updated, and scan your device regularly.

(21) Upgrade your browser and applications to support Transport Layer Security (TLS) encryption or a higher encryption standard, and make sure that the browser option for storing or retaining user ID/names and PINs is unselected.

(22) Remove shared files and printers from your computer, especially when accessing the internet via broadband connection, wireless network, or similar setup.

(23) Change your PIN immediately the first time you use the service, and destroy any documents containing your PIN. Memorise your PIN. Do not write them down.

(24) Use a combination of numbers (0 to 9) and letters (A to Z) for your Cyberbanking PIN. Do not use your identity card number, telephone number, date of birth, driving license number, or any commonplace number sequence (such as 987654 or 123456) when choosing your PIN or ATM card password.

(25) Keep your ATM Card, statements, cheque books, other important documents, and any security device for accessing Cyberbanking or BEA Mobile Banking in a safe place. Keep your PIN separate from your Cyberbanking account number and user ID/name, and do not keep your ATM card and password together. If you want to discard any documents that contain your personal information, destroy them first.

(26) Change your PIN and ATM card password regularly.

(27) Be alert to your surroundings before conducting any transactions. Make sure no one sees your user ID/name or PIN. Cover the keypad when you enter your PIN. Check that the protective keypad cover is intact before using any ATM in Hong Kong. Contact BEA immediately if in doubt.

(28) Check the authenticity of the BEA website by checking the URL. A security icon that looks like a lock or key will appear when authentication and encryption is expected.

(29) Change your PIN immediately if you suspect that you have been deceived by a fraudulent website or email, or through a public Wi-Fi, public computer, third party's device, or any other means (for example, if you fail to log in to a service website after inputting your correct PIN, whether or not any alert messages appear).

(30) When you receive an SMS with an One-time Password ("OTP"), or a security code, verify the accuracy of the login or transaction details prior to entering the OTP or the security code. When you receive our SMS message or inbox message or push notification, verify the accuracy of the transaction details in a timely manner and inform BEA immediately of any suspicious situations. No SMS containing an OTP will be forwarded to any other mobile phone number, even if you have subscribed to an SMS-forwarding service provided by your telecommunications provider in Hong Kong.

(31) If your device is capable of biometric authentication (e.g. fingerprint or facial recognition), do not disable any features that can strengthen the security of biometric authentication.

(32) Check the website's privacy policy statement and statement on security safeguards before providing personal data to the website.

(33) Should you notice any suspicious devices at an ATM (such as micro-skimmers, pin-hole cameras, or fake key pads) or any suspicious activities around you when performing an ATM transaction, cancel your transaction and inform BEA immediately.

(34) Count the banknotes immediately after withdrawing cash at an ATM. Keep all transaction receipts and check them against your account records. Do not take away any banknotes left behind by someone else at the cash dispenser or ATM card left in the card insertion slot. Let the ATM retract the banknotes and/or ATM card automatically.

(35) Retrieve the banknotes (if withdrawing cash), transaction receipt (if applicable), and ATM card as instructed after your ATM transaction is completed. Never try to push your ATM card back into the ATM.

(36) Set your effective date and expiry date for overseas ATM cash withdrawal before travelling. Invalidate the function when you have returned from travelling.

(37) Check the storage, battery, and mobile data usage of apps in your device from time to time to see if there are any suspicious apps. Uninstall any suspicious app when necessary.

(38) Please visit any of our branches to update your personal information if your mobile phone number, email address and/or correspondence address recorded in the Bank has been changed or become invalid. Please register your mobile phone number and email address before using i-Token service.

(39) To avoid being deceived by a message, verify the sender's identity through alternative channels before taking any action.

(40) Review and follow the security tips issued by BEA on a regular basis.

Issued by The Bank of East Asia, Limited 東亞銀行有限公司刊發