

## **OPERATING GUIDELINES**

These «Operating Instructions» are issued from time to time with the purpose of providing information to customers with regard to the way the Bank of Cyprus electronic channels and services (1bank) are operating.

### **1. EQUIPMENT/SOFTWARE**

- 1.1. For accessing the electronic channels of 1bank, the use of a personal computer (pc) is essential (for accessing internet banking) or a smart phone with access to the internet (for both accessing internet banking and mobile banking)
- 1.2. For your security, we recommend that you lock your mobile phone in order to avoid access to it by unauthorised persons. If your mobile phone number has changed, you should notify the Bank either by visiting any branch or calling the 1bank Call Center at the number indicated in the Contact Information section below.
- 1.3. In case of a wifi/wireless connection to the internet, we urge you to install properly your wireless equipment. We also urge you to read carefully the relevant installation instructions and always follow the manufacturer's security instructions.
- 2.1. The usage of the 1bank electronic channels is not affected by the operating system or browser that you use. However, we recommend that you use the most common browsers. For more information on the browsers, click here.
- 2.2. We recommend (where applicable) the following settings in your browser:
  - Delete Cookies and files
  - Accepting Cookies should be enabled
  - Java Script should be allowed
  - Active Scripting should be allowed
  - TLS 1.0, TLS 1.1 and TLS 1.2 security protocols should be used
  - Encrypted pages should not be saved on disc
- 1.1. If you wish to use the dedicated mobile applications (Apps), you will additionally need an App Store account (for the iOS application) or a Google Play Store account (for the Android application).
- 1.2. Refer to the 1bank Terms and Conditions for the obligations and responsibilities of the different parties.

### **2. INTERNET AND EMAIL SECURITY**

- 2.1. Always access the Bank of Cyprus electronic banking service (1bank), via the official website at [www.bankofcyprus.com.cy](http://www.bankofcyprus.com.cy), [www.1bank.com](http://www.1bank.com) or through the Bank of Cyprus App on your mobile device.
- 2.2. Never trust website pages which you did not access directly from the above addresses or disclose to such pages your 1bank login credentials (User ID and Passcode).
- 2.3. Never leave your pc unattended while using the 1bank electronic services.
- 2.4. Avoid using public pcs for accessing the 1bank electronic services.
- 2.5. Save your personal financial information only on your pc.
- 2.6. In case you stop using a pc, we urge you to delete any personal information that you may have saved on it using appropriate software.
- 2.7. From time to time, Bank of Cyprus will send promotional electronic messages (via email, SMS, etc). The Bank will never ask you to disclose any personal information or your 1bank login credentials through emails, pop up windows and banners. Never reveal through the internet or email or through any other electronic media your personal details such as User IDs, Passcodes, Digipass codes, card numbers, bank account numbers etc.
- 2.8. If you receive any email that asks you to «confirm your account», «to confirm your 1bank login credentials» or with any other similar content, this is probably a fraud or «phishing email».
- 2.9. If you receive spam emails or emails containing suspicious attachments, we urge you to delete them immediately and not respond.

- 2.10. Never respond to or download files on your pc from unknown publishers or websites.
- 2.11. If you doubt the authenticity of a website page, remember to check its certificate. A website page is authentic if the bar on the top of your screen (with the website url) is green (this applies only for EV certificates). Additionally, by clicking on the lock on the same bar, you will see the official owner of the certificate (for the Bank the official owner is: BANK OF CYPRUS PUBLIC COMPANY LTD).
- 2.12. Never open unexpected attachments received from known or unknown sources.
- 2.13. Refer to the 1bank Terms and Conditions for the obligations and responsibilities of the different parties.

### **3. PERSONAL COMPUTER PROTECTION (FROM MALWARE, VIRUS, SPYWARE) / FIREWALL**

- 3.1. Install on your pc anti-virus programs for protecting it from viruses, spyware and malware. Use these programs regularly for detecting and removing these threats.
- 3.2. Make sure that the anti-virus and anti-spyware programs are updated with the latest updates.
- 3.3. Make sure that the operating systems and software on your pc are updated with the latest security updates.
- 3.4. Use a firewall (or personal firewall) to prevent external users from accessing your pc, especially if you use a high-speed connection to the internet or a continuous connection to the internet such as DSL or a cable modem.
- 3.5. Refer to the 1bank Terms and Conditions for the obligations and responsibilities of the different parties.

### **4. PROTECTION OF LOGIN CREDENTIALS**

- 4.1. Never disclose your 1bank Passcode to anyone
- 4.2. Never write your 1bank Passcode in places where it can be found by third parties.
- 4.3. The members of the staff of Bank of Cyprus will never ask you to disclose your 1bank Passcode, either over the phone or in an email.
- 4.4. Never let third parties watch you while entering your 1bank User ID and Passcode to access the 1bank electronic services.
- 4.5. Avoid using your pc's auto connection feature that saves your Passcode on your pc.
- 4.6. Always logout from the 1bank electronic services when you complete your online banking. Do not just close your browser or your mobile's App.
- 4.7. Activate your pc's time out feature, to lock it when you are not using it.
- 4.8. Never set predictable Passcodes such as your birth date, your identification number, your passport number, etc.
- 4.9. For additional security, we urge you to change your Passcode regularly.
- 4.10. Refer to the 1bank Terms and Conditions for the obligations and responsibilities of the different parties.

### **5. PROTECTION OF SECURITY DEVICES (DIGIPASS)**

- 5.1. Always carry the security device (digipass), with you.
- 5.2. Never disclose your digipass PIN to a third party.
- 5.3. Never disclose to a third party the One Time PINs (OPTs) generated from your digipass device.
- 5.4. Regarding the usage of hardware digipass refer to the 1bank Terms and Conditions Terms and Conditions of 1bank for the obligations and responsibilities of the contracting parties up to their complete withdrawal upon the Bank's decision.
- 5.5. Refer to the Terms and Conditions for Owing and Operating Digipass APP for the obligations and responsibilities of the contracting parties.
- 5.6. Refer to the Terms and Conditions for Owing and Operating SMS Digipass for the obligations and responsibilities of the contracting parties.

## 6. COMPROMISED 1BANK PASSCODE/ENTERING OF 1BANK PASSCODE OR OTP IN A WEBSITE PAGE THAT DOES NOT BELONG TO THE BANK

- 6.1. If you suspect that your Passcode has been compromised (revealed or stolen), change it immediately through either the internet banking service or the mobile banking service.
- 6.2. If you have received a «phishing email» with a link that directs you to a fake Bank of Cyprus page, do not respond to it. Send it immediately to the email address [abuse@bankofcyprus.com](mailto:abuse@bankofcyprus.com). The Bank will take all the appropriate actions to shut down this page as soon as possible.
- 6.3. If you have responded to a «phishing email» and you have entered/submitted any personal or other information, contact us as soon as possible for the following actions:
  - 1bank Passcode - We will cancel the code and send you a new one.
  - Card - We will cancel your card and issue a new one.
- 6.4. In case the incident took place during a bank holiday or during non working hours, we recommend that:
  - 1bank Passcode - Change it immediately, if possible. If you cannot login to any of the 1bank electronic services (if a third person has already changed your Passcode), attempt to login using your User ID and any Passcode at least 6 times in order to lock the User ID. Contact us the next working day.
  - Card - Contact JCC on +357 22868100 to cancel your card. Contact us the next work day.
- 6.5. Refer to the 1bank Terms and Conditions for the obligations and responsibilities of the different parties.

## 7. INSTRUCTIONS FOR MONEY TRANSACTIONS

- 7.1. All money transactions to a third party bank account require the usage of a security device (digipass).
- 7.2. You can specify that all money transactions from your accounts require the approval of one or more persons (subscribers).
- 7.3. The cancellation of a money transaction is possible provided that this has a future execution date or if it has not yet been approved for execution by the authorized signatory.
- 7.4. With the submission of a transaction to the Bank, the transaction will be automatically executed and the account debited (with the amount and charges, if any), provided that the instruction complies fully with the criteria set by the Bank. Transactions that do not comply with criteria set by the Bank for automatic execution are received by the Bank Units and are executed. The communication with the Account Holder or Subscriber is not mandatory for the execution of these transactions.
- 7.5. Set up Alerts to receive account balances or information for transactions in your accounts. The messages are sent to your email or mobile number (sms). The service is offered free of charge
- 7.6. The 1bank QuickPay service is available to all individual Users and can be activated via the Bank of Cyprus App. QuickPay allows Users to assign a bank account to their mobile phone number to make and receive payments. QuickPay allows 1bank Users to pay other activated QuickPay users by entering their mobile phone number and also allows payments to any other Bank of Cyprus account holder by entering their account number. Refer to the QuickPay Terms and Conditions and FAQs for more information
- 7.7. Refer to the 1bank Terms and Conditions for the obligations and responsibilities of the different parties.

## 8. BANK, SUBSCRIBER AND ACCOUNT HOLDER RESPONSIBILITY

- 8.1. All money transactions to a third party bank account require the usage of Instruments Producing Single Use Codes (SMS Digipass & Digipass APP).
- 8.2. Check regularly the Standing Orders and Direct Debits opened on accounts connected to your subscription (whether these accounts belong to you or to a third party – private individual or legal entity), for

orders not opened by you or the Account Holder(s). If you suspect that an order might not be authentic, we urge you to contact us.

- 8.3. Check «Pending» transactions from the Transaction Status screen, for instructions that have not been submitted by you. Cancel them or contact us.
  - 8.4. Refer to the 1bank Terms and Conditions for the obligations and responsibilities of the different parties.
- ## 9. OTHER USEFUL SECURITY INFORMATION/TIPS
- 9.1. 1bank electronic services have preset (default) transaction limits, as these are displayed on the relevant application forms. You can, however, set lower limits for money transactions via 1bank.
  - 9.2. You can use multiple signatures for your electronic banking. This option allows you to set different rules for creating and approving money transactions. If you do so, money transactions created by one subscriber will need the approval of another before being sent to the Bank for execution.
  - 9.3. If your accounts are connected to a third party and this party (subscriber) is no longer associated with you:
  - 9.4. Notify us in order to terminate his/her access to your accounts
  - 9.5. Do not hand over the logon credentials of this subscriber, to a different person without submitting the proper application forms to us.
  - 9.6. If you have authorized a third party to have access to your accounts and you wish to terminate it, contact us.
  - 9.7. Refer to the 1bank Terms and Conditions for the obligations and responsibilities of the different parties (website link).

## 10. CUTOFF TIMES FOR OUTWARD PAYMENT ORDERS

The Bank process outward payment orders with same value date as the execution date, during work days and before the following cutoff times:

Currency	Cutoff time
EUR	Up to 13:30
USD	Up to 13:30
GBP	Up to 13:00
CAD, RUB	Up to 13:00
CHF, RON	Up to 13:00
NOK, PLN, SEK, CZK, DKK, HUF	Up to 12:00

## 11. CONTACT INFORMATION

- 1bank Call Centre, 800 00 800 or +357 22128000 if calling from abroad, Monday to Friday, 07:45 – 20:00.
- Contact us form
- email: [info@bankofcyprus.com](mailto:info@bankofcyprus.com)