CIMB Bank Berhad (13491-P)

IMPORTANT NOTICE DATED 1 JUNE 2024
NOTICE OF AMENDMENTS TO THE CIMB ONLINE BANKING TERMS AND CONDITIONS

Dear Valued Customers,

Effective 22 June 2024, the CIMB Online Bank Terms and Conditions shall be amended to reflect the following:

(i) Transaction limit cooling-off period upon any increase of the daily transaction limit.
(ii) Primary device will be the mobile device on which you activated CIMB Clicks App and/or CIMB OCTO app.
(iii) Mobile Banking Application Security enhancement.
(iv) Enable DuitNow Request service.
(v) Enable DuitNow Online Banking/Wallets service.

The full revised CIMB Online Banking Terms and Conditions can be viewed here from 22 June 2024 onwards.

Should you require any further clarification, please refer to FAQ.

For ease of reference, a tabulation of the amended and additional clauses are set out in the table in *italics* below:

Existing Clause	Revised Clause
2A. Procedure for first time setup and subsequent log on to the CIMB Mobile Banking Application: i) ... viii)	*Insertion of sub-clause ix):* 2A. Procedure for first time setup and subsequent log on to the CIMB Mobile Banking Application: *ix) By using the CIMB Mobile Banking Application, you agree to grant us permission to access selected functions and data on your Primary Device to support the operation of the CIMB Mobile Banking Application as well as for monitoring and prevention of fraudulent activities. These functions may include location services and device information such as OS version, device model and device unique identifiers.*
5.2 You must, at all times: 5.2.1 observe all security measures as may be prescribed by CIMB Bank or CIMB Islamic Bank in relation to your CRN, CIMB Card Pin, Online Banking Password, SecureTACTM, TAC on SMS, Passcode, User ID and Biometric Data. You are required to adhere to the Dos and Don'ts in relation to the protection and safeguarding of your: (i) personal information, (ii) CIMB Online Banking details, (iii) CIMB Card Pin, and to protect your computer/ mobile devices and your online information by taking the recommended measures as set out at https://www.cimb.com.my/en/personal/help-support/security-and-fraud/security-and-fraud-awareness.html;	*Insertion of "Primary Device" in Clause 5.2.1.* 5.2 You must, at all times: 5.2.1 observe all security measures as may be prescribed by CIMB Bank or CIMB Islamic Bank in relation to your CRN, CIMB Card Pin, Online Banking Password, SecureTACTM, TAC on SMS, Passcode, User ID, *Primary Device* and Biometric Data. You are required to adhere to the Dos and Don'ts in relation to the protection and safeguarding of your: (i) personal information, (ii) CIMB Online Banking details, (iii) CIMB Card Pin, and to protect your computer/ mobile devices and your online information by taking the recommended measures as set out at https://www.cimb.com.my/en/personal/help-support/security-and-fraud/security-and-fraud-awareness.html;
6.6 CIMB Bank or CIMB Islamic Bank reserves the right to refuse to carry out any Instructions given by you for any reason. This includes but is not limited to, where such Instructions are: 6.6.1 – 6.6.3 …	*Insertion of sub-clause 6.6.4* 6.6 CIMB Bank or CIMB Islamic Bank reserves the right to refuse to carry out any Instructions given by you for any reason. This includes but is not limited to, where such Instructions are: 6.6.1 – 6.6.3 …*; or* *6.6.4 detection of a security threat or compromised access to*

	your CIMB Online Banking.
12.1 You agree, give your consent to and authorise CIMB Bank and/or CIMB Islamic Bank to divulge, reveal and/or otherwise disclose any and all particulars and information relating to yourself, your Account or any transactions or dealings between you and CIMB Bank and/or CIMB Islamic Bank to: -	*Insertion of "Primary Device" in Clause 12.1.* 12.1 You agree, give your consent to and authorise CIMB Bank and/or CIMB Islamic Bank to divulge, reveal and/or otherwise disclose any and all particulars and information relating to yourself, your Account, *your Primary Device* or any transactions or dealings between you and CIMB Bank and/or CIMB Islamic Bank to: -
13.9 You must not install or use the CIMB Mobile Banking Application on a jail-broken or rooted mobile device, hardware or software. Unauthorised modifications to any mobile device's operating systems ("jail-breaking or rooting") bypasses security features and can cause numerous issues to any such hacked device. CIMB Bank and CIMB Islamic Bank strongly caution against installing the CIMB Mobile Banking Application in any hacked mobile device as such mobile device will be vulnerable to fraudulent attacks and may expose your Account to being used by unauthorised persons and or lead to unauthorised access and/or use of the CIMB Mobile Banking Application and the Banking Services by any person, whether remotely performed or otherwise. You must indemnify and hold CIMB Bank harmless against any Loss arising from your use of the CIMB Mobile Banking Application or the Banking Services on any jail-broken or rooted mobile device, hardware or software, including instances where such Loss is caused by any damage or corruption to or failure of the CIMB Mobile Banking Application or the Banking Services due to your use of the same on such jail-broken or rooted mobile device, hardware or software.	*Amendments to Clause 13.9 to reflect security measures against compromised device* 13.9 You must not install or use the CIMB Mobile Banking Application on a *compromised,* jail-broken or rooted mobile device, hardware or software. Unauthorised modifications to any mobile device's operating systems *either intentionally or unintentionally through jail-breaking, rooting or malicious mobile application downloads* bypasses security features and can cause numerous issues to your device. CIMB Bank and CIMB Islamic Bank strongly caution against installing *and/or* using the CIMB Mobile Banking Application in any hacked *or compromised* mobile device as such mobile device will be vulnerable to fraudulent attacks and may expose your *CIMB Mobile Banking access* and Account(s) to unauthorised persons and/or lead to unauthorised access and/or use of the CIMB Mobile Banking Application and the Banking Services by any person, whether remotely performed or otherwise. You must indemnify and hold CIMB Bank harmless against any Loss arising from your use of the CIMB Mobile Banking Application or the Banking Services on any *compromised,* jail-broken or rooted mobile device, hardware or software, including instances where such Loss is caused by any damage, *takeovers* or corruption to or failure of the CIMB Mobile Banking Application or the Banking Services due to your use of the same on such *compromised,* jail-broken or rooted mobile device, hardware or software.
15. Unauthorised Fraudulent Transactions 15.1.1 You must take the necessary steps to protect yourself from unauthorized and/or fraudulent transaction and apply necessary safeguards to protect your device by ensuring adequacy of security protocol as set out in Clause 5.2.1 and Clause 13.1. 15.1.2 You are required to keep abreast of online scams either through the awareness published through CIMB Bank and CIMB Islamic Bank assets, through the Amaran Scam Facebook Page (https://www.facebook.com/amaran penipuan/), a dedicated site set up by Bank Negara Malaysia that shares information and host webinar/live sessions on financial fraud or from other reliable public sources.	*Amendments to Clause 15.1.1 to reflect the security measure against compromised device and renumbering of the Clauses 15.1.* 15. Unauthorised *And/Or* Fraudulent Transactions 15.1.1 You must take the necessary steps to protect yourself from unauthorized and/or fraudulent transactions and apply necessary safeguards to protect your *computers and/or* device(s) by ensuring the adequacy of security protocol as set out in Clauses 5.2.1, 13.1 *and 13.9 including authorising CIMB Bank to take fraud countermeasures to protect yourself CIMB Online Banking access and Account(s) from unauthorised usage.* 15.1.2 You are required to keep abreast of online scams either through the awareness published through CIMB Bank and CIMB Islamic Bank ~~*assets,*~~ *or* through the Amaran Scam Facebook Page (https://www.facebook.com/amaran penipuan/), a dedicated site set up by Bank Negara Malaysia that shares information and host webinar/live sessions on financial fraud, or from other reliable public sources.
	Insertion of sub-clause 21.2.12

21.2 However, CIMB Bank or CIMB Islamic Bank may terminate, suspend or restrict your access to CIMB Online Banking or any part of CIMB Online Banking immediately without notice to you, if: - 21.2.1 – 21.2.11.	21.2 However, CIMB Bank or CIMB Islamic Bank may terminate, suspend or restrict your access to CIMB Online Banking or any part of CIMB Online Banking immediately without notice to you, if: - 21.2.1 – 21.2.11 …*; or* *21.2.12 your CIMB Online Banking access is on a compromised Primary Device resulting from social engineering scams, rogue application downloads, malware and/or inadequate security protocol such as jail-broken or rooted mobile device.*
"Primary Device" means the last mobile device on which you activated the CIMB Mobile Banking Application or the mobile device selected by you to be Primary Device in the 'Manage Device' tab in CIMB OCTO App.	***"Primary Device"*** *means the mobile device on which you activated CIMB Clicks App and/or CIMB OCTO App.*
	Clause Newly added: *9.10 You agree and acknowledge that there will be a time lapse of approximately 12-hour cooling-off period upon any increase of the daily transaction limit made by you via your CIMB Clicks, CIMB Clicks App or CIMB OCTO App. You can transact with the new limit only after the cooling-off period.*
	Clause Newly added: ***"DuitNow Online Banking/Wallets"*** *means a real-time online payment service that allows you to make secure online transfers via PayNet.*
	Clause Newly added: ***"DuitNow Request"*** *means a service which allows you as recipient to directly request and receive fund transfers from payers, and as payer to transfer funds directly to a recipient's account as a result of a request made by the recipient.*
"PayNet Related Services" means the services which facilitates industry -wide ubiquitous payments or credit transfer i.e. DuitNow to Account, DuitNow to Mobile /ID, DuitNow QR, DuitNow Online Banking/Wallets, JomPAY, Inter Bank Giro (IBG), Financial Process Exchange (FPX) which complies with the requirements of PayNet.	***"PayNet Related Services"*** *means the services which facilitates industry -wide ubiquitous payments or credit transfer i.e. DuitNow to Account, DuitNow to Mobile /ID, DuitNow QR, DuitNow Online Banking/Wallets, DuitNow Request, JomPAY, Inter Bank Giro (IBG), Financial Process Exchange (FPX) which complies with the requirements of PayNet.*

The Management
CIMB Bank Berhad