

BOC Life Mobile Application Terms and Conditions

Please read the terms and conditions below carefully. By using this mobile application ("this service" or "this Mobile App") and the materials from time to time available through this service ("these materials"), you agree to be bound by these terms and conditions. As these terms and conditions may be amended from time to time at the discretion of BOC Group Life Assurance Company Limited (the "Company", "we", "us", or "our") and be posted on this service, you should read them again carefully whenever using this service. You are assumed to have agreed to the revised terms and conditions if you continue to use this service following any changes to these terms and conditions.

These terms and conditions are in addition to the license agreement agreed between you and the relevant software providers (including Google Play™ store and App Store) for use of the Service (the "License Agreement"). In case of any inconsistency or conflict between the License Agreement and these terms and conditions, the latter shall prevail.

Availability

Products and services mentioned in these materials are not available to all persons in all geographic locations. Only persons who are permitted by applicable law may browse the information and/or subscribe the services and products offered. Persons browsing these materials are required to ensure that they are aware of and observe all relevant restrictions that apply to them and are responsible for satisfying themselves that they may do so under the laws or the jurisdiction to which they are bound or located. Eligibility of any person for particular product or service is subject to the final determination of the Company.

Remarks: Google Play logo is a trademark of Google Inc., and the App Store is a service mark of Apple Inc.

Disclaimer

The information contained in these materials is for general information only and is provided on an "as is" basis without warranty of any kind (including without limitation, merchantability, title, fitness for particular purpose, freedom from computer virus, non-infringement, compatibility, security, accuracy and completeness) and may be withdrawn and/or changed at any time without prior notice.

This service and/or these materials may not be available at all times and there may be

delays, failures, errors or omissions or loss of transmitted information.

No information contained in these materials should be regarded as an offer or solicitation to sell, to subscribe to, or provide any recommendation to any person. The information is not intended to be relied upon as the basis for any decision which may affect you or your business. All persons should consult their own professional adviser before making any investment, financial decision or purchasing any product or subscribing any service.

The viewer should be aware that any information regarding rates, indexes, exchange rates and unit prices available through this service is on a delayed basis. The Company will endeavour to ensure the accuracy and reliability of the information provided but do not guarantee its accuracy or reliability and accept no liability (whether in tort or contract or otherwise) for any loss or damage arising from any inaccuracies or omissions.

To the extent permitted by applicable law, the Company disclaims liability for any error, omissions or inaccuracies in the information contained in these materials and for any loss or damages, resulting from its use or reliance, or inability to use, by any party or in connection with any error, interruption, delay in operation or incomplete transmission, line or system failure or computer virus. The Company is not responsible in any manner for direct, indirect, special, incidental or consequential damages arising out of the use of this service and/or these materials.

Your use of this service and these materials is entirely at your own risk. The Company does not represent or warrant that no viruses or other destructive properties will be transmitted or that no damage will occur to your equipment or mobile phone. You are solely responsible for adequate protection and back up of data and/or equipment and for undertaking reasonable and appropriate precautions to scan for computer viruses or other destructive properties and to prevent, safeguard and ensure that no computer virus enters your equipment or mobile phone. The Company makes no representations or warranties concerning the accuracy, functionality or performance of any third party software that may be used in connection with this service.

Continued use of GPS running in the background can dramatically decrease battery life.

Security Information

This Mobile App provides you with one-stop policy information and management

services. You can search "BOC Life" for free download of this Mobile App in the online App stores (Google Play and App Store). Do not install mobile Apps from mistrusted sources. If there is any suspicious App, you should not download or login and should stop operation immediately.

Avoid using Mobile Apps via wireless networks (i.e. Wi-Fi) which is public or without password setting. We advise using encrypted and reliable mobile internet connections especially for financial transactions.

Disable any wireless network functions (e.g. Wi-Fi, Bluetooth, NFC) or Payment Apps when not in use. Choose encrypted networks when using Wi-Fi and disable Wi-Fi auto connection setting.

Please do not connect your mobile device to any suspicious computer infected by virus; at the same time, it is recommended to install anti-virus software and setup the firewall in your mobile. Don't use Mobile Apps via any jailbroken iPhone or rooted Android mobile to avoid any potential security loophole. Also, you can download the appropriate mobile security Apps from the online App stores. You can visit HKCERT website for reference: <https://www.hkcert.org/mobilesecurity-tools>, to select the appropriate Apps.

To protect your online transactions, we will check whether your mobile device is jailbroken or rooted and with recommended operating systems for minimum security requirements upon using this Mobile App. Customer may not be allowed to access this service via such device. Please pay attention to the reminder.

Activate the auto-lock function of your mobile device. Do not use easy-to-guess personal information, numbers or words as your password and avoid using the same password that you have used for accessing other web services.

Upon the successful registration of the "Biometric Authentication" on your mobile phone, any biometric credential that is stored on your mobile phone can be used for the purpose of the "Biometric Authentication". You must ensure that only your biometric credential is stored on your mobile phone to access the device, and ensure the security of the security codes as well as the password or code that you can use to store your biometric credential and register the "Biometric Authentication" on your mobile phone. For security reasons, do not register biometric credential of other person(s) on your mobile phone or use jailbroken or rooted mobile phone.

You can enable / disable the "Biometric Authentication" through "Menu > Settings > Enable Biometric Authentication Login" in this Mobile App after login. Please note that after you have cancelled the "Biometric Authentication", your biometric credential will be continuously stored on your designated mobile device. You may consider cancelling the data at your own decision.

If your biometric credential of the designated mobile device has been changed or the "Biometric Authentication" has not been used for a specified period of time (which shall be defined by the Company from time to time), your "Biometric Authentication" will be suspended.

You must not use your biometric credential(s) for Biometric Authentication if you have reasonable belief that other people may share identical or very similar biometric credential(s) of you or your biometric credential(s) can be easily compromised. For instance, you must not use facial recognition for authentication purpose if you have identical twin or triplet sibling(s).

You must not use your biometric credential(s) for Biometric Authentication if the relevant biometric credential(s) of you are or will be undergoing rapid development or change. For instance, you must not use facial recognition for authentication purpose if you are an adolescence with facial features undergoing rapid development.

You will use all reasonable care to keep your mobile phone secure. You will notify us as soon as reasonably practicable if you find or believe that your mobile phone has been lost or stolen or that any unauthorised transactions have occurred.

Please download and install updates and patches for this Mobile App and the other Mobile Apps regularly in the online App stores (Google Play and App Store) or through our website.

Hyperlinks

Use of hyperlinks to other internet sites or resources are at the browser's own risks. The Company expressly disclaims any responsibility for the accuracy or availability of the information provided by those sites or for the safety of information which the browser may provide to any third party.

We may provide hyperlinks to websites of the Company and its subsidiaries. The products and services offered on such websites may be limited to persons located or residing in that particular jurisdiction and the contents of such websites may not be

intended for persons located or residing in other jurisdictions where the distribution of such contents is restricted. In addition, there may be difference in the terms governing the use of the websites of the Company and its subsidiaries and you are reminded to read the applicable terms carefully before using the websites.

For your convenience, this Mobile App may provide hyperlinks to other websites on the internet. These hyperlinks lead to websites of third parties who are in no way affiliated with or related to the Company. We are not responsible for verifying the contents of such third party websites. You use such hyperlinks and third party websites at your own risk and we are not responsible for any consequences arising out of or in connection with your doing so. Unless otherwise expressly stated by the Company, the provision of hyperlinks to third party websites does not represent any form of endorsement, recommendation, approval, guarantee or introduction by the Company of any third parties or their products or services, or any form of co-operation between the Company and any third parties. Further, the Company is not a party to any contractual arrangement entered into between you and the provider of a third party website or any third party unless otherwise expressly specified or agreed to by the Company.

We may also provide hyperlinks to third party websites which contain downloadable software for your convenience. We are in no way responsible for any difficulties you may encounter in downloading or installing such software or for any consequences arising out of or in connection with your doing so. Please note that the use of any software downloaded from the Internet is governed by a licence agreement specific to that software. Without any obligation or responsibility on our part, you are reminded to observe the terms of such software licence agreement. Your failure to do so may result in an infringement of the intellectual property rights of the relevant software provider.

Please note that when you leave this Mobile App, you will be subject to the terms and privacy policies of the websites you are visiting.

Copyright

This service and all contents in these materials (unless otherwise specified) are protected by copyright. No part of these materials may be modified, reproduced, transmitted and distributed in any format or by any means for commercial or public use without the Company's prior written consent.

Collection of Information

The Company focuses on its duty of confidentiality to its customers. The protection of personal information of our customers is important to us. As a provider of insurance products and services, the collection and use of the personal information of our customers is fundamental to our daily business operations. Please refer to the "Personal Information Collection Statement" for the Company's general policies on collection, use, disclosure and transfer of customer data. For the Company's policies and practices in protecting personal data privacy, please refer to the "Privacy Policy Statement". "Personal Information Collection Statement" and "Privacy Policy Statement" are available at www.boclif.com.hk.

The Company will record the information of users using this Mobile App through the mobile application server access log (including the clicking date and time, IP address, pages clicked, device, operating system, Advertising Identifier (if applicable) and third-party advertising platforms from which users are directed to this Mobile App ("Advertising Source") (if applicable)). The Company might use the users' record of using this Mobile App for the purposes of improving the operation of this Mobile App, conducting statistical analysis and marketing. The Company will keep the relevant information for an appropriate period of time based on the actual needs. The server access log of this Mobile App will record the users' information automatically by default. Save where express consent or permission is required, by continuing to use this Mobile App, users are deemed to have given their consent for the Company to store and use the relevant information in the above manner. If the users do not consent to the above, the users should not continue to use this Mobile App and should not provide the user's relevant information.

(If applicable) When using this Mobile App, the user's mobile device will share the Advertising Identifier, a unique identifier for a mobile device, with the Company and third-party agencies (such as website or mobile application analytics companies). The Advertising Identifier is an anonymous users' identifier and contains no name, address information nor any information that will enable anyone to contact the users via any means. No user's personal data will be collected or stored by the Company.

The Company may use third-party applications (such as Google Analytics) to assist the Company to record the Advertising Source, Advertising Identifier and browsing history of the users. Such third-party applications will organise, aggregate and analyse the collected data (which does not involve any personally identifiable information) on behalf of the Company. Such analysed (non-personal) information may be used

together with the personal data collected by the Company for the purposes of statistical analysis and improving marketing efficiency.

The Company may entrust third-party agencies (such as website or mobile application analytics companies) to analyse information of users' other online activities (including preferences and usage patterns) through the use of users' Advertising Identifier. Such information may be analysed together with the personal data collected by the Company to enable the Company to understand more about users' preferences for the purposes of statistical analysis and improving marketing efficiency. The Company will not provide any personal data (which could identify the identity of users) with these third-party agencies or collect any personally identifiable information from these third-party agencies for the foregoing purposes.

If the users do not wish the Company and third parties (including agencies) to record and use their information (namely, Advertising Identifier and Advertising Source) for the aforementioned purposes, they may change the relevant setting on the mobile device (generally navigate to "Privacy" > "Tracking" or "Ads" in the mobile device's settings).

Governing Law

These terms and conditions are governed by the laws of the Hong Kong Special Administrative Region. The parties submit to the non-exclusive jurisdiction of the Hong Kong courts.

Language

The Chinese version of these terms and conditions is for reference only. If there is any conflict or inconsistency between the Chinese and the English version, the latter shall prevail.

Risk Disclosure Statements

Investment involves risks. Terms apply. For details and relevant investment risk factors, please contact your financial consultant or the Company's customer service hotline.

Conditions for Services

By using this Mobile App, you have confirmed your acceptance of our Terms and Conditions for eService (as amended by us from time to time). Please visit the following website for full details: <https://www.boclif.com.hk>.

Terms and Conditions for use of biometric authentication for Mobile Application of BOC Group Life Assurance Company Limited

1. These terms and conditions ("these Biometric Authentication Terms") apply to and regulate your use of biometric authentication for the mobile application of BOC Group Life Assurance Company Limited ("the Company", "we", "us" or "our"). By registering or using biometric authentication for the Company's mobile application, you are deemed to accept and agree to these Biometric Authentication Terms. If you do not accept these Biometric Authentication Terms, please stop registering or using biometric authentication for the Company's mobile application.

2. You may use your biometric credential(s) (including without limitation fingerprint(s), facial map(s) or any other biometric data as approved by the Company from time to time) stored on your designated mobile device to login the Company's mobile application, to authorize instruction in respect of transactions as specified by the Company from time to time through the Company's mobile application or to do such other things or transactions as notified by the Company from time to time. Designated mobile device means iPhone® 5s or higher, specified models of Samsung or LG and such other electronic equipment that we may enable for use with biometric authentication from time to time and includes the operating system or software that the device operates on. Please contact us for the updated list of such electronic equipment.

3. You agree that the Company may treat and consider as valid and binding on you any instruction given, or agreement made with the Company, which is authenticated through biometric authentication without the Company making any further inquiry as to the authority or identity of the person making or purporting to give such instructions or to make such agreement or their authenticity notwithstanding any error, misunderstanding, fraud, forgery or lack of clarity in the authorization. You acknowledge that the Company may still require you to authenticate a transaction by your password and/or another form of authentication even though you have authenticated the same by your biometric credential(s).

4. These Biometric Authentication Terms are in addition to and shall be read in conjunction with the Company's Terms and Conditions for eService and any other documents forming part of our insurance agreement (and any reference to the terms and conditions of the Terms and Conditions for eService shall include reference to these Biometric Authentication Terms). In the event of any conflict or inconsistency, these Biometric Authentication Terms shall prevail over the Terms and Conditions for eService and to the extent of such conflict or inconsistency.

5. You acknowledge and agree that in order to use biometric authentication for the

Company's mobile application:

- i.) You must be a valid user of our mobile application;
 - ii.) You must install our mobile application using a designated mobile device through an official source;
 - iii.) You will need to activate the relevant biometric authentication function on your designated mobile device and register at least one of your biometric credentials to control access to the designated mobile device;
 - iv.) You must register the biometric authentication through the Company's mobile application by using your Username, password and SMS, or One-time password and choosing to use the relevant biometric credential(s) that you stored on your designated mobile device for the purpose of biometric authentication;
 - v.) You understand that upon the successful registration of the biometric authentication on your designated mobile device, any biometric credential(s) that is/are stored on your designated mobile device can be used for the purpose of the biometric authentication. You must ensure that only your biometric credential(s) is/are stored on your designated mobile device to access the device;**
 - vi.) You must not use the biometric authentication if you have reasonable belief that other people may share identical or very similar biometric credential(s) of you or your biometric credential(s) can be easily compromised. For instance, you must not use facial recognition for authentication purpose if you have identical twin or triplet sibling(s);**
 - vii.) You must not use the biometric authentication if the relevant biometric credential(s) of you are or will be undergoing rapid development or change. For instance, you must not use facial recognition for authentication purpose if you are an adolescence with facial features undergoing rapid development;**
 - viii.) You should ensure the security of the security codes as well as the password or code that you can use to store your biometric credential(s) and register the biometric authentication on your designated mobile device; and
 - ix.) You will use all reasonable care to keep your designated mobile device secure. You will notify us as soon as reasonably practicable if you find or believe that your designated mobile device has been lost or stolen or that any unauthorised transactions have occurred.**
6. You may still choose to login mobile application to view policy information and manage your policy(ies) with Username and Password.
7. You acknowledge that the authentication is performed by the Company's mobile application by interfacing with the biometric authentication module on the designated mobile device and you agree to the authentication process. The Company will not collect/store your biometric credential(s) in any manner at any stage of your

registration or use of the biometric authentication for the mobile application.

8. You can cancel the biometric authentication for the Company's Mobile Application by yourself at any time on the Company's Mobile Application once you are signed in or contacting the Company's customer service hotline or accessing our Customer Service Center. Please note that cancellation of the biometric authentication for the Company's Mobile Application will not automatically delete your biometric credential(s) on your designated mobile device. Your biometric credential(s) will be continuously stored on your designated mobile device unless they are deleted by you through the relevant biometric authentication function on your designated mobile device. Biometric credential(s) stored on your designated mobile device may be used by other applications on your designated mobile device. You may consider to cancel the data at your own decision.

9. If your biometric credential(s) or other security code of the designated mobile device has been compromised, you are required to change the security code, re-register your biometric credential(s) or cease the use of the biometric authentication for mobile application.

10. If your biometric credential record of the designated mobile device has been changed or you have not used the biometric authentication for Mobile Application for a specified period of time (which shall be defined by the Company from time to time), your biometric authentication for Mobile Application will be suspended. You are required to re-register or re-activate the biometric authentication for Mobile Application.

11. You and the corporate policy owner that you are acting for and on behalf of ("the Corporate Customer") will be liable for all losses if you and/or the Corporate Customer have acted fraudulently or with gross negligence, or allowed any third party to use your designated mobile device, password and/or authentication tool, or failed to comply with your obligations under these Biometric Authentication Terms, the Terms and Conditions of this Mobile App, the Terms and Conditions for eService, the Security Information and other relevant documents as provided by the Company from time to time.

12. The laws of the Hong Kong Special Administrative Region of the People's Republic of China shall govern these Biometric Authentication Terms. You hereby irrevocably submit to the non-exclusive jurisdiction of the Hong Kong courts.

13. In addition to and without subtracting the disclaimers and exclusions of liability in the Terms and Conditions for eService:

i.) You understand that the biometric authentication module of the designated mobile device is not provided by the Company, and we make no representation or warranty as to the security of the biometric authentication function of any designated mobile

device and whether it works in the way that the manufacturer of the device represents.

ii.) We do not represent or warrant that the biometric authentication for the Company's mobile application will function at all times or with any electronic equipment, software, infrastructure or other services provided through website that we may offer from time to time.

iii.) **You and the Corporate Customer that you are acting for and on behalf of shall indemnify us and keep us indemnified against any consequences, claims, proceedings, losses or damages whatsoever and howsoever caused (save and except any direct loss or damages caused by negligence or misconduct on the part of us) that may arise to be incurred by us and against any costs and expenses (including all legal costs on an indemnity basis) of reasonable amount reasonably incurred by us in making biometric authentication available to you and/or the Corporate Customer arising in connection with any improper use of the biometric authentication.**

iv.) The Company reserves the right to amend, add or delete at any time these Biometric Authentication Terms by giving reasonable prior notice in writing to you and such notice may be made in such manner and by such means of communication as the Company shall deem fit, including, without limitation, use of direct mailing material or advertisement, website display or electronic communications such as electronic mail. You acknowledge and agree that you shall observe and comply with any such amendment, addition and/or deletion when using the biometric authentication. Your continued use of the biometric authentication shall constitute your acceptance of any such changes or modifications.

v.) These Biometric Authentication Terms are also applicable for instructions and/or enquiries relating to the Corporate Customer and its accounts given by you as a user and these Biometric Authentication Terms, as the context may require, shall extend to and be binding on the Corporate Customer and account.

vi.) These Biometric Authentication Terms are available in both English and Chinese versions. The English version shall prevail in the event of any discrepancy between the two versions.

Note: iPhone is a trademark of Apple Inc.

Mar 2026