

Terms and Conditions for Passwordless/Biometric Single-Sign-On (SSO) Authentication

Passwordless/Biometric Single-Sign-On (SSO) Authentication (“**Passwordless/Biometric SSO Authentication**”) of Hong Kong Baptist University offers a secure and convenient way to access your data and accounts of various information technology (“IT”) services by using the biometric data or biometric credentials **stored and/or registered in your own devices** to verify your identity.

By performing the [Activation and Device Registration for Passwordless/Biometric SSO Authentication](#), you shall be taken to have confirmed that you have read, understand and agree to be bound by the following Terms and Conditions (“**these Terms and Conditions**”) for using the Passwordless/Biometric SSO Authentication for identity authentication, through which you may have access to your data, accounts and IT services provided by Hong Kong Baptist University (the “**University**”). IF YOU DO NOT ACCEPT OR AGREE TO ANY OF THESE TERMS AND CONDITIONS, PLEASE DO NOT ACTIVATE (OR REGISTER DEVICE FOR) THE PASSWORDLESS/BIOMETRIC SSO AUTHENTICATION.

1. Passwordless/Biometric Single-Sign-On (SSO) Authentication (“**Passwordless/ Biometric SSO Authentication**”) is an identity authentication function using biometric credentials (including but not limited to fingerprint, facial map and/or any other biometric data).
2. Passwordless/Biometric SSO Authentication implements “Cisco Duo Passwordless” technology that uses passkeys and platform authenticators, security keys from access devices, or Duo Push to verify your identity for secure data and application access without passwords. The list of supported authentication methods, web browsers, operating systems and devices can be found [here](#).
3. Passwordless/Biometric SSO Authentication provides an alternative means of verifying your identity by using your **biometric data or biometric credentials stored and/or registered in your device(s)** that has/have been registered for the Passwordless/Biometric SSO Authentication. For using the Passwordless/Biometric SSO Authentication in your device (with biometric identity sensor supported), you must register one of the supported authentication methods, e.g. by way of fingerprint, facial recognition, Windows Hello, Face ID and Touch ID in that device by completing the steps set out in [here](#). Upon successful registration, you may use your biometric credentials to confirm your identity for accessing your data, accounts and IT services provided by the University.
4. **The University’s provision and your use of the Passwordless/Biometric SSO Authentication are subject to these Terms and Conditions. Once you have used, activated and/or registered**

device for the Passwordless/Biometric SSO Authentication, you shall be regarded as having confirmed that you have read, understand and agree to be bound by these Terms and Conditions. If you do not accept or agree to any of these Terms and Conditions, please do not use, activate or register device for the Passwordless/Biometric SSO Authentication.

5. By activating the Passwordless/Biometric SSO Authentication, you confirm and agree that you authorise the University to verify your identity by the biometric credentials and biometric data stored and/or registered in your device(s) that has/have been registered for the Passwordless/Biometric SSO Authentication, instead of your username (“SSOid”) and password. In particular, you consent to the authentication process (which involves interfacing with the biometric identity sensor module in the registered device(s)). You agree that the Passwordless/Biometric SSO Authentication function or system shall use and access the biometric credentials (including but not limited to fingerprint, facial map and/or any other biometric data) recorded and stored in the device(s) that has/have been registered for the Passwordless/Biometric SSO Authentication, and you hereby consent to the University’s access to and use of such information (and the information obtained through the biometric identity sensor) for identity authentication.
6. You fully understand and agree that upon successful registration for the Passwordless/Biometric SSO Authentication, **ALL** biometric credentials and biometric data stored and/or registered in the registered device(s) (i.e. device(s) that has/have been registered for the Passwordless/Biometric SSO Authentication) at the time of or after registration may be used to verify your identity for your access to your personal data, accounts and/or IT services provided by the University. Therefore, you must ensure that **only** your own biometric credentials and biometric data are stored and/or registered in such registered device(s). If you store or register any other person’s biometric credentials or biometric data and/or allow any other person’s biometric credentials or biometric data to be stored or registered in the registered device(s), you shall be responsible for any use (and/or any unauthorised use or processing) of such other person’s biometric credentials or biometric data to access your personal data, accounts and IT services and/or for the purpose of the Passwordless/Biometric SSO Authentication. All the use or processing of such other person’s biometric credentials or biometric data shall be deemed to have been authorised by you and will be binding on you and you shall be solely liable therefor.
7. By using the Passwordless/Biometric SSO Authentication, you agree to be liable for and to indemnify, defend, hold harmless and keep indemnified the University from and against any and all loss, costs, liabilities, expenses, claims, demands and damage directly or indirectly arising out

of or in connection with your activation or use of the Passwordless/Biometric SSO Authentication or your violation of these Terms and Conditions.

8. All instructions received by the University with your identity verified through the Passwordless/Biometric SSO Authentication shall be binding on you. You shall be liable for all such instructions and the resulting transactions and consequences.
9. You may deactivate the Passwordless/Biometric SSO Authentication at any time by contacting the University's Office of Information Technology ("ITO") Service Call Centre (Tel: 3411-7899, Email: hotline@hkbu.edu.hk). Once the Passwordless/Biometric SSO Authentication has been deactivated, you may continue to access your data, accounts and IT services by using the username ("SSOid"), password and Duo Mobile 2FA.
10. The University reserves the right to specify or vary from time to time the scope and features of the Passwordless/Biometric SSO Authentication without giving prior notice. The University reserves the right to modify, suspend, discontinue or terminate the provision of the Passwordless/Biometric SSO Authentication or its use by you at any time without giving prior notice or reason, including without limitation in the event of any actual or suspected breach hereof and/or any data security incident, and the University accepts no liability for any loss, costs, expenses, claims or demands howsoever arising therefrom.
11. You shall take all reasonable security measures and precautions to prevent loss of the device(s) which has/have been registered for the Passwordless/Biometric SSO Authentication, or unauthorised or fraudulent use of the Passwordless/Biometric SSO Authentication.
12. The University reserves the right to amend these Terms and Conditions and/or introduce additional terms and conditions regarding the provision or use of the Passwordless/Biometric SSO Authentication from time to time. You are obliged to read and observe any amended terms and conditions governing the provision or use of the Passwordless/Biometric SSO Authentication as published on the University's or ITO's website(s), and the security recommendations provided by the University from time to time. Activating or using the Passwordless/Biometric SSO Authentication after any such amendments shall constitute agreement and acceptance of such amendments.
13. You must not register or use the Passwordless/Biometric SSO Authentication in any or any modified device or operating system which does not align with the vendor-supported or warranted configurations, including without limitation devices that have been "jail-broken" or "rooted". Using the Passwordless/Biometric SSO Authentication in a "jail-broken" or "rooted" device or system may compromise security level and lead to fraudulent transactions or identity

verification, which shall be entirely at your own risk and the University shall not be liable for any losses, damages, claims, liability or any other consequences arising therefrom.

14. You shall not take any action to disable any security function provided by, or agree to any settings of, the device registered for the Passwordless/Biometric SSO Authentication, which may result in compromising the security level regarding the use of your biometric credentials or biometric data (such as disabling the “attention-aware” function for facial recognition), or conduct any behaviour which will disrupt the operation, functionality or security of the Passwordless/Biometric SSO Authentication.
15. In the event of your breach of these Terms and Conditions, the University may terminate your access to and use of the Passwordless/Biometric SSO Authentication without giving notice, and the obligations and liabilities you incurred prior to such termination shall survive the termination for all purposes.
16. The Passwordless/Biometric SSO Authentication system or function is provided on an “as is” basis. The University does not give any warranty, guarantee or representation, whether express or implied, of any kind for or in relation to the Passwordless/Biometric SSO Authentication system or function, including without limitation warranty of quality, accuracy, availability, functionality or performance.
17. The University and its employees and agents accept no liability, responsibility or obligation to you or any third party, including without limitation for any direct, indirect, special or consequential loss, costs, liabilities, expenses, claims, demands or damage howsoever caused by, arising from or in connection with any access to, activation and use of and/or registration for the Passwordless/Biometric SSO Authentication. Activation and use of and/or registration for the Passwordless/Biometric SSO Authentication are entirely at your own risk.
18. Any personal data collected by the University shall be governed by the University’s “Privacy Policy Statement and Personal Information Collection Statement” (<https://bupdpd.hkbu.edu.hk/policies-and-procedures/pps-pics/>).
19. Nothing in these Terms and Conditions confers or purports to confer on any third party any benefit or any right to enforce any of these Terms and Conditions whether pursuant to the Contracts (Rights of Third Parties) Ordinance (Chapter 623 of the Laws of Hong Kong) or otherwise.
20. If any provision of these Terms and Conditions is held by any court of competent jurisdiction to be illegal, invalid or unenforceable, such provision shall be deemed to be severed from these Terms and Conditions and shall not affect the lawfulness, validity or enforceability of the

remaining provisions of these Terms and Conditions, which shall remain in full force and effect.

21. Any waiver of any provisions of these Terms and Conditions must be made by the University in writing. Any failure or delay of the University to enforce any provisions of these Terms and Conditions or exercise any right, power or remedy hereunder shall not operate as a waiver of that provision, right, power or remedy, nor shall any single or partial exercise or enforcement thereof preclude any other or future exercise or enforcement thereof or the exercise or enforcement of any other provision, right, power or remedy hereunder.
22. These Terms and Conditions are governed by and construed in accordance with the laws of the Hong Kong Special Administrative Region of the People's Republic of China ("**Hong Kong**"). You agree to irrevocably submit to the exclusive jurisdiction of the courts of Hong Kong to resolve any claim or dispute arising out of or in relation to these Terms and Conditions.

Copyright © 2024 Hong Kong Baptist University. All Rights Reserved.