DCB BANK

DCB Bank Business Banking (Mobile) App - Security Guidelines

Please read this document to understand the responsibilities that accompany the use of mobile banking app.

Security for your banking transactions is the Bank's maximum priority. DCB Bank has implemented robust measures to secure your digital transactions. Safe, secure, and seamless is the result of this effort.

This document outlines the key security practices and guidelines followed by DCB Bank and recommended steps that you the user must take to protect your business banking experience.

DCB Bank Security Commitment

1. Secure Application Design

The DCB Business Banking App is developed using global best practices and regular security assessments are conducted.

2. Safe Mobile Application

The App can only be downloaded from trusted sources (Google Play Store or Apple App Store).
Older App versions are phased out quickly to keep you protected.
The App is designed to detect compromised devices and may restrict use on such devices for your safety.

3. Strong Authentication

Multi-factor authentication (MFA) is used for login and transactions.
Critical activities (adding beneficiaries, high-value payments, profile updates) require additional verification. In addition, a cooling period is observed for addition and modification of beneficiaries discouraging any unauthorised payments.

4. Transaction Monitoring

All transactions are monitored real-time to detect unusual activity.
Alerts and notifications are sent instantly for transactions and security events.

5. Data Protection

All sensitive data is encrypted both while in transit and rest.
Your account details, passwords, and PINs are never stored on the device in plain text.

6. Business Banking Controls

Higher transaction limits are protected by additional approvals and layered security.
Dual authorisation feature (maker and checker) is made available to business users. The Bank will not be held responsible for any loss incurred owing to fraudulent or any unauthorised activities.

7. Incident Response

In the event of any suspected security incident, customers are advised to immediately report the same with DCB Customer Care available 24x7 for prompt assistance and fraud mitigation.

Your Role in Keeping Banking Safe

To maximise security, we encourage you to follow these simple best practices:

- Always download or update the App from official app stores only.
- Never share your User ID, password, OTP, or PIN with anyone, including bank staff.
- Avoid using the App on rooted or jailbroken devices.
- Ensure that your phone has the latest operating system and security patches.
- Log out after each session and avoid using public Wi-Fi for transactions.
- Report any suspicious messages, links, or unauthorised transactions immediately to DCB Bank.

Customer Protection & Grievance Redressal

- DCB Bank is committed to protect accounts and transactions against unauthorised electronic transactions, as per RBI guidelines.

- Business banking customers are advised to:
  a) Regularly review transaction alerts, account statements, and notifications.
  b) Immediately report any unauthorised or suspicious activity.
  c) Not delay in reporting suspect transactions, as it may impact the Bank's ability to mitigate losses.

- If you notice suspicious activity, immediately please reach out to DCB Customer Care 24×7 at 022-6899 7777, 040-6815 7777 or email customercare@dcb.bank.in

- For more information, please visit the Bank's website: ***https://www.dcb.bank.in***

Indicative Guidelines:

- The business banking customer shall, at their own risk and consequences, access and use the application services by following the safe and secure guidelines prescribed by the Bank from time to time, including the use of user credentials or OTPs or any other suitable means of authentication as decided by the Bank.

- Device & SIM integrity: The App is designed to function securely on the registered mobile number and device environment.
  Business banking customers must ensure:
  a) The SIM in use matches the mobile number registered with the Bank for DCB Business Internet Banking.
  b) The device is free from malware, unauthorised applications, or rooting/ jailbreaking.
  c) Not to use compromised or unverified devices, it may lead to restricted access or blocking of services.

- Transaction authorisation & OTP usage: All financial and sensitive transactions require multi-factor authentication, including OTP validation.
  OTPs are:
  a) Strictly confidential
  b) Valid only for a limited duration
  c) Meant only for one time use
  d) Sharing OTP will be treated as authorised consent, and the Bank will not bear liability for resulting transactions.

- The business banking customer and the users shall keep all OTPs, MPIN and passwords confidential and well protected, and should not reveal the same to any unauthorised person or other third party. The Bank shall in no manner be held responsible, if the customer incurs any loss as a result of the user credentials being disclosed by the customer or user to any authorised or unauthorised person or other third parties.

- The business banking customer acknowledges that technology/ies used including the internet, usage of public and shared facilities is susceptible to a number of risks, such as hacking, fraudulent transactions, data breach, any or all of which could affect the application services and that the Bank shall not be held responsible, if the customer incurs any loss owing to any of these aforesaid factors.

- App Usage & Availability: The Bank endeavours to provide uninterrupted services; however, the business banking customer agrees that:
  a) Availability may be affected due to system maintenance, technical issues, or force majeure events.
  b) The Bank is not liable for any losses arising from temporary disruption of services.

- Transaction Limits & Controls: The business banking customer agrees that the transactions conducted through the App are subject to:
  a) Regulatory limits prescribed by authorities.
  b) Internal limits set by the Bank.
  c) The Bank reserves the right to modify limits without prior notice in line with risk management practices.

- The Bank will not be responsible for any loss, delays or failures caused to or incurred by the business banking customer/user in the processing of instructions on account of such risks.

- The business banking customer shall refrain from performing transactions in the application via shared computer or through unprotected public network (e.g., open Wi-Fi) as it could be leveraged to compromise the user's account.

- In case of web application, business banking customers must log out from the application or close the browser when the application is not in use. The business customer also agrees to log off the App safely if not in use.

- The business banking customer shall be vigilant with respect to phishing*, vishing** and smishing*** attacks

* A technique for attempting to acquire sensitive data, such as bank account numbers, internet banking passwords, other critical credentials/ information through a fraudulent solicitation in email or on a web site, or WhatsApp, in which the perpetrator masquerades as a legitimate business or reputable person.
** A technique for attempting to acquire sensitive data, such as bank account numbers, internet banking passwords, other critical credentials/ information through a fraudulent solicitation over a voice call, in which the perpetrator masquerades as a legitimate business or reputable person.
*** A technique for attempting to acquire sensitive data, such as bank account numbers, internet banking passwords, other critical credentials/ information through a fraudulent solicitation through SMS, in which the perpetrator masquerades as a legitimate business or reputable person.

- The business banking customer shall note that the Bank employee/ staff, will not request the customer to share the transaction OTP or MPIN or passwords with the Bank employee/ staff.

- Reporting & Customer Support: In case of suspected fraud or unauthorised access, the business customers must immediately:
  a) Contact DCB Customer Care at 022-6899 7777, 040-6815 7777 or email customercare@dcb.bank.in
  b) Block access via available channels if required.
  c) Prompt reporting is critical for dispute resolution and risk mitigation.

- The business banking customer shall ensure the application is up to date and update or re-download (if required) the application only via authorised channel/ play store.

- The business customer must refrain from downloading application files from the internet.

- Updates & Amendments: The Bank reserves the right to modify these guidelines at any time. Continued use of the App constitutes acceptance of updated terms.

Compliance Assurance

The DCB Bank Business Banking (Mobile) App fully complies and adheres to industry standards for cybersecurity. We continuously review and strengthen our systems to provide you with safe and seamless digital banking experience.

By proceeding to use the DCB Business Banking (Mobile) App, you acknowledge that you have read, understood, and agreed to abide by the above guidelines and disclaimers.

Thank you for banking with us.

DCB Bank Limited