



## **TERMS AND CONDITIONS FOR INTERNET BANKING**

### **1. INTRODUCTION:**

Pursuant to provide better customer services, the Authority of the Tamluk Ghatal Central Co-Operative Bank Ltd has adopted the decision to extend the platform as well as the channel to provide with the facility of Internet Banking to the capacitive customers of the Tamluk Ghatal Central Co-Operative Bank Ltd. This policy shall establish the basic principles & terms of operationalization's as is/are/be necessary for securing usage and management of the internet banking transactions & governance.

### **2. OBJECTIVES:**

With the rapid and significant growth in online (anywhere any time) Banking, electronic commerce and digital payments, it is obvious that electronic (Internet) banking and payments are likely to advance and shall stand in demanding platform. The impact of Internet banking on cost savings, revenue growth and increased customer satisfaction is tremendous which can be leveraged as a potential tool for building a sound strategy in banking platform.

The objectives of this policy is to -

- (i) provide internet banking as an efficient system of instantaneous banking taking into consideration the availability of technology and infrastructure to support the new model of banking;
- (ii) built in adequate mechanism to tackle the security risk and operational risk aspects;
- (iii) adhering to the legal and regulatory framework to take care of the rights and obligation of the consumers; and
- (iv) to strategically adopt the Internet to access and transact in customer's account by himself/herself/themselves;

Towards these objectives, Tamluk Ghatal Central Co-Operative Bank Ltd would like to offer internet banking and financial services as one of the channels for consumers on a 24 X 7 basis on a real time basis through extended implementation of Core Banking Solution (CBS) and appropriate web technology and incorporated securities thereof.

This Internet Banking Policy of the Tamluk Ghatal Central Co-Operative Bank Ltd shall govern the introduction, usage, monitoring, supervision and overall bindings & controls of the extension of the Banking products and services through the channel of Internet.

### 3. DEFINITIONS:

In this Policy Document, unless the context repugnant the subject otherwise, the here-in-under terms, words, expressions and phrases shall have the meanings indicated against them as follows:

- a. The **Bank** shall mean and refers to the “**Tamluk Ghatal Central Co-Operative Bank Limited**”, a “District Central Co-Operative Bank” in the state of West Bengal within the meaning assigned in clauses (e) and (h) of Section 2 of the Reserve Bank of India Act, 1934 and in clause (u) of Section 2 of the National Bank for Agriculture and Rural Development Act., 1981, registered under the Cooperative Societies Act, 1912 and deemed to be registered under the West Bengal Cooperative Societies Act, 2006 and Cooperative Credit Structure Entity in terms of Section 134B of the said Act, hereinafter referred to as “**TGCCBL**” synonymously which expression shall unless excluded by or repugnant to the subject or context or meaning thereof be deemed to mean and include its successors, associates, nominees, representatives, permitted assigns and other legal substitutes of the one part having it’s Registered address and Head Office at Tamluk, Purba Medinipur, West Bengal, Pin – 721636, India.
- b. “**Customer**” shall mean as the Customer of the TGCCBL wherein the Customer shall require registering in said Application and or sending request for such registration with applicable form & perquisites and shall wherein the context requires, include any authorized representative of the Customer for the purpose.
- c. “**User**” shall mean as the said respective capacitive customer of the TGCCBL who has wished and as authorized to use the facility of the said online Internet Banking platform of the Bank as after necessary acceptance of relevant terms and conditions of said services and facility of the Bank.
- d. The communicative website of the Bank site shall mean <https://www.tgccb.bank.in> and/or any other website as may be notified by TGCCBL from time to time.
- e. Internet Banking facility and services shall refer to the services offered by the TGCCBL through which a registered Customer / user may conduct enquiries or perform transactions on / through the designated site / channel / platform;
- f. The online Banking site shall mean <https://onlinetgccb.tgccb.bank.in/OnlineTGCCBL/> and/or any other site URL (Uniform Resource Locator) as may be notified by TGCCBL from time to time.
- g. Wherein above said **OnlineTGCCBL** shall mean the gateway platform of Internet Banking facility as offered by the Bank.
- h. The facility of Internet Banking will be provided to a customer only after obtaining his/her written application. All requests received from the customer shall be logged and transmitted by his/her/their home branch. The requests become effective from the time when the services are configured and activated by the respective Branch. While registering the request, the customer shall be informed about the time normally taken by the bank for fulfilment of

such requests. The branch shall not offer facility of Internet banking to customers who do not provide mobile numbers to the bank.

- i. Service and Facility of Internet Banking shall be the Bank's services which would provide access to account information, products and other services (including Transaction of financial and non-financial in nature) as be advised by the Bank from time to time to the customers through the internet banking website of the Bank as at <https://onlinetgccbl.tgccb.bank.in/OnlineTGCCBL/>.
- j. Confidential Information refers to the information obtained by the customer through the Bank for availing various services through said **OnlineTGCCBL**.
- k. Personal Information refers to the information about the User obtained by the Bank in connection with the Internet Banking Services of the Bank.
- l. **"Account(s)"** shall mean any or more accounts held and/or facilities provided to the Customer by TGCCB including but not limited to Savings Accounts, Current Accounts, Term Deposit Accounts, Cash Credit & Loan Account and/or such other accounts and/or facilities as may be determined by TGCCB from time to time, for which the facility is being offered or may be offered in future. Accordingly, it shall simultaneously refer to the User's Savings and/or Current Account and/or Fixed Deposit or any other type of account so designated by the Bank to be eligible account(s) for the operations through the use of Internet Banking.
- m. **"Other Holders of Accounts"** refers to such holders other than the first named holder of the Account. The Internet Banking Services of the Bank for Account is available to a customer who has a Account in his name. The Bank reserves its rights to consider any deviation to the above at its sole discretion. The Account will be attached to the UserID and will be accessible through **OnlineTGCCBL**. Wherever the Account is jointly held by the Customer, the Bank will construe that the other holders of the Account have authorized the first holder to either query on the account or initiate transaction on the account and it will be binding on them.
- n. **JOINT ACCOUNTS** : The Internet Banking Services will be available in case of Joint accounts only if the mode of operation is indicated as 'either or survivor' or 'anyone or survivor' or 'former or survivor'. For 'former or survivor' account, Internet Banking facility may be available only to the 'former'. For 'either or survivor' and 'anyone or survivor' accounts, Internet Banking may be provided to each one of the joint account holders on their request. In case of 'either or survivor' and 'anyone or survivor' accounts if any of the joint account holder(s) gives "stopping of operations" instructions for the use of Internet Banking Service in writing, on any of the Internet Banking Services, it will be discontinued for the User. In case of 'former and survivor' account, such instructions will not be issued by other account holder. In the case of joint Account(s) with mode of operation 'Jointly', this facility shall not be available. The facility can also be offered to Corporate Customers having mode of operation as per the constitution of their firm/company.
- o. **Minor Account(s) / Accounts in the name of Minor(s)** : Where if, the terms of accounts as opened for and on behalf of minors children; the Internet Banking facility of TGCCBL shall not be made available to the minor. The natural guardian of the minor shall be permitted to use Internet banking with facility only 'Limited Transaction' rights. The natural guardian shall

undertake to give all instructions relating to the operation of the account and further undertake not to reveal the User ID and Password to the minor, which if done so, will be at the risk and consequences of the guardian and the Bank shall not be liable for any loss on that account in case the account is operated by the minor. In such an event the transaction will be deemed to have been undertaken by the guardian.

- p. **Future Accounts:** In the event of opening of accounts by the User under the same CIF in furtherance and future, then the applicable Terms of Service (Terms & Conditions) shall apply automatically to all such further accounts through the Internet Banking by the User.
- q. **“Alert(s)”** shall mean the customized messages as a One Time Password (OTP) / SMS in response of the set triggers in banking applications of the TGCCBL and as has/be sent to the registered Mobile phone number and / or to E-mail (Electronic mail) address of the customers / user as has registered by the customers / Users at the Bank. One Time Password (OTP) through Short Messaging Systems (SMS) refers to one time **6 to 8 digit pass code** that would be sent to a customer’s mobile number registered on the Bank’s record.
- r. Third party product refers to any product and/or service of third party which is offered by or through the intermediary of the Bank.
- s. **LIMITS:** The User is aware that the Bank may from time to time impose maximum and minimum limits including daily limits on transfer of funds that may be transferred or amount of the Demand Draft/ IOI (Inter Office Instruments) that can be issued by virtue of the payment instructions given hereunder. The User acknowledges that the same is to reduce the risks on him/her. For instance, the Bank may impose transaction restrictions within particular periods or amount restrictions within a particular period or even each transaction limits. The User shall be bound by such limits imposed and shall strictly comply with them. The Bank shall put an appropriate message on the relevant page or the website.
- t. **CHARGES :** The Bank at its discretion from time to time may specify charges for usage of Internet Banking Services and/or additional charges for selected services which is published on the Website of the Bank (<https://www.tgccb.bank.in>) and any further changes in the charges/fees shall also be notified on the above sites. All out of pocket expenses where-ever applicable will be borne by the User. The User and the other account holder(s)(in case of joint accounts) hereby authorize(s) the Bank to recover all charges related to Internet Banking Services as determined by the Bank from time to time by debiting the User(s) account or any of joint account holder’(s) account(s).
- u. Instruction means any request or instruction that is received from the customer by the Bank through Internet Banking services.

#### 4. APPLICABILITY OF TERMS:

These Terms mentioned herein & above shall form the contract between the User using the Internet Banking services and the Bank. By applying for Internet Banking Services and accessing the service the User acknowledges and accepts these Terms of Service (Terms & Conditions). Any conditions relating to the accounts of customer other than these Terms will

continue to apply except that in the event of any conflict between these Terms and the account conditions, these Terms will continue to prevail. The agreement shall remain valid until it is replaced by another agreement or terminated by either party or account is closed, whichever is earlier.

## **5. GENERAL INFORMATION ON SCOPES OF INTERNET BANKING SERVICES:**

- i. The Bank may offer Internet Banking Service to selected customers at its discretion. The customer would need to be Internet User or have access to the Internet. The acceptance of the application and the acknowledgement thereof does not automatically imply the acceptance of application for Internet Banking Services. The Bank may advise from time to time the Internet software such as Browser, which are required for using Internet Banking Services. There will be no obligation on the part of the Bank to support all the versions of this Internet software.
- ii. The Bank shall endeavor to provide to the User through Internet Banking services such as inquiry about the balance in his/her account(s), details about transactions, statement of account, request for issue of cheque books, request for transfer of funds between accounts of the same User and other accounts in the same Bank and transfer to the other Bank also and many other facilities as the Bank may decide to provide from time to time. These facilities shall be offered in a phased manner at the discretion of the Bank. The Bank at its sole discretion may also make additions/deletions to the Internet Banking Services being offered without giving any prior notices or reasons. The availability /non-availability of a particular service shall be advised through the web page of the Bank or written communication or any other mode as the Bank thinks fit & proper thereon. The Bank shall take reasonable care to, ensure the security of and prevent unauthorized access to the Internet Banking Services using technology reasonably available to the Bank. The User shall not use or permit to use Internet Banking Service or any related service for any illegal or improper purposes.
- iii. The user would be allotted a User-id only by the Bank in first time and the password would require to be generated at the time of first login by the user in the first instance. The user will be required to change the User-Id mandatorily on accessing of Internet Banking Services as in scheduled first time framed login.
- iv. As a safety measure the user shall have held the liabilities and responsibilities to change the password as frequently as possible, at least once in 90 days, if the user does not change the password by himself/herself then the password will automatically expire after 180 days. In addition to User-id and Password the BANK may, at its discretion, advice the user to adopt any other means of authentication including but not limited to smart cards, One Time SMS Password and/or Digital certification issued by Bank for the user, licensed or approved Certifying Authorities or vendors.
- v. The user shall not attempt or permit others to attempt accessing the account information stored in the computers and computer networks of the Bank through any means of the Internet Banking Services.
- vi. The facility of Internet Banking will be provided to a customer only after obtaining his/her written application. All requests received from the customer shall be logged and transmitted

by his/her/their branch. The requests become effective from the time when the services are configured and activated by the respective Branch Office and subsequently by the Systems department / IT Department at the Head Office of the Bank. While registering the request, the customer shall be informed about the time normally taken by the Bank for fulfillment of such requests.

- vii. Considering the prevailing legal position, there is an obligation on the part of the Bank not only to establish the identity but also to make enquiries about the integrity and reputation of the customer opting for internet banking. Therefore, even though request for opening an account may be accepted over Internet, accounts are opened only after verification of the recorded identity of the customer and adherence to the KYC (Know Your Customers) and AML (Anti Money Laundering) guidelines of the Regulating Authorities.
- viii. From a legal perspective, security procedure adopted for authenticating a user needs to be recognized by law as a substitute for signature. The provisions of the Information Technology Act, 2000 / Information Technology Amendment Act 2008 and other legal requirements should be scrupulously adhered to.
- ix. Under the present regime, there is an obligation on the bank to maintain secrecy and confidentiality of customers' accounts/information. In the Internet banking scenario, the risk of the bank not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, the bank may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking / technological failures. The Bank shall therefore place in adequate risk control measures to manage all such risks.
- x. Hyperlinks from the bank's websites will be confined to only those portals with which they have a payment arrangement. Hyperlinks to the bank' websites from other portals are normally meant for passing on information relating to purchases made by the bank's customers in the portal. The bank will follow recommended security precautions while dealing with requests received from other websites relating to customers' purchases.

#### **6. SSL server certificate warning:**

- i. Internet banking customers are made aware of and shown how to react to SSL or EV-SSL certificate warning.

#### **7. USER-ID AND PASSWORD:**

- i. It would be the primary responsibility and liability of the user who shall
  - a. Keep the User-id and password totally confidential and not reveal them to any third party.
  - b. Create a password of at least 8 characters long and shall consist of a mix of alphabets, numbers and special characters which must not relate to any readily accessible personal data such as the user's name, address, date of birth, telephone number, vehicle number, driver license etc. or easily guessable combination of letters and / or numbers;
  - c. Commit the User-id and password to memory and not record them in a written or electronic form; and

- d. Not let any unauthorized person have access to his computer or leave the computer unattended while using Internet Banking Services.
  - e. Not disclose/reveal his/her personal or confidential information to anyone over email/SMS/phone call even if its purportedly inform from Tamluk Ghatal Central Co-Operative Bank Ltd. TGCCBL or any of its employees and or representatives will never send emails/SMS or call over phone to seek personal information like Username, passwords, One Time SMS passwords etc of the user.
  - f. Not access Online TGCCBL if his/her computer device is not free of malware (Viruses, Trojans, etc.).
- ii. In the event of forgetting of User-id and/or password or expiry/ disability of password(s) respective user can request for change of the password by sending a written request to the TGCCBL. The selection of a new password and/ or the replacement of User-id shall not be construed as the commencement of a new contract. The User agrees and acknowledges that Bank shall in no way be held responsible or liable if the User incurs any loss as a result of compromise of User-id and password by the User himself/herself/themselves or User has failed to follow the Internet Banking Service instructions as published by the TGCCBL on the site from time to time. User agrees to fully indemnify and hold harmless to TGCCBL in respect of the same.

**iii. Locking of User ID:**

Internet Banking Password / User ID shall get locked after a number of incorrect conjugative attempts, up to such number (at present 3 failed attempts) as may be decided by the Bank from time to time. The same shall be available on the next day. In case of emergency, the User ID / password can be unlocked through the Bank Branch channel.

**iv. Deactivation of User ID**

The Bank has the discretion to deactivate a User's Internet Banking ID, if the same has not been used for a period defined by the Bank. Also the Bank has the right to deactivate the Internet Banking login of user due to unsatisfactory behavior in the account.

**8. One Time Password Generators:**

- i. This security is personal to the customer / user and can only be used with password. It provides an additional level of security for certain transactions and cannot be shared with anyone else.
  - a. Retail customer to set a fresh login & profile password with an OTP authentication while registration on INB. Corporate customer prompted to change the password sent on registered mobile number at the time of first login. Without setting a new password system will not allow to login in INB.
  - b. Since activation of the Internet Banking facility and services of the user, the customer will need to commence using the one-time security password when the customer uses the service. The customer will need to enter the code displayed which shall have with validity once per occasion when the customer shall perform any transaction in the said platform.

- c. The customer must keep his/her/their security safe and secure and advise the bank immediately if it is lost, stolen or misused. Until the bank's actual receipt of such notification, the customer shall remain responsible for any and all use of the Online Net Banking by un-authorized persons or for un-authorized purposes. The bank will deactivate his/her/their service as immediate after receiving of such notice / information from the user.
- d. If the customer(s) have any questions about the security, he/she may approach /call the bank between 10.00 am and 5.00 pm, Monday to Saturday (excluding second and fourth Saturdays and Gazette Holidays).

#### **9. Two-factor authentication and other security measures for Internet banking:**

- i) In view of the proliferation of cyber-attacks and their potential consequences, two-factor authentication for internet banking operations to be implemented (where to be deemed applicable).
- ii) The implementation of appropriate authentication methodologies shall be based on an assessment of the risk posed by Internet banking systems.
- iii) For two-factor authentication, One Time Password – OTP is used. The OTP is personal to the customer and can only be used with password. It provides an additional level of security for certain transactions and should not be shared with anyone else.
- iv) There shall be a legal risk in not using the asymmetric cryptosystem and hash function for authenticating electronic transactions. For carrying out critical transactions like fund transfers, the bank, at the least, shall implement robust and dynamic two-factor authentication through User id and Transaction Password combination and second factor by the way of One Time Password (OTP) sent as SMS over registered mobile phone / email of the registered user / customer.
- v) To enhance online processing security, confirmatory second channel procedures (like telephone, SMS, e-mail, etc.) are applied in respect of transactions above pre-set values, creation of new account linkages, registration of third party payee details, changing account details or revision to funds transfer limits. In devising these security features, the bank takes into account their efficacy and differing customer preferences for additional online protection.
- vi) Based on mutual authentication protocols, customers could also authenticate the bank's web site through security mechanisms such as personal assurance messages/images, exchange of challenge response security codes and/or the Secure Sockets Layer (SSL) server certificate verification. In recent times, Extended Validation Secure Sockets Layer (EV-SSL) Certificates are increasingly being used. These are special SSL Certificates that work with high security web browsers to clearly identify a website's organizational identity. It should, however, be noted that SSL is only designed to encrypt data in transit at the network transport layer. It does not provide end-to-end encryption security at the application layer.
- vii) An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. Else, in the event of interference, the session should be terminated and the affected transactions resolved or reversed out. The customer should be promptly notified of such an incident as the session is being concluded or subsequently by email, telephone or through other means.

## **10. Second channel notification / confirmation:**

- i. The bank shall notify the customer, through SMS and or Email of the user, for all transactions.

## **11. MAINTENANCE OF SUFFICIENT BALANCE:**

- i. User shall ensure that there are sufficient funds (or drawing power for credit facilities) in any Account for transactions through the Internet Banking, and the Bank shall not be liable for any consequences arising out of its failure to carry out the instructions due to inadequacy of funds and/or credit facilities provided always that Bank shall at its sole discretion, be entitled to carry out the instructions notwithstanding such inadequacy without seeking the prior approval from or notice to user and the user shall be responsible to repay with interest the resulting overdraft, advance or credit thereby created and for all related to costs and charges at the rates as may be determined by the Bank. Bank may, at its discretion, levy penal charges for non-maintenance of the minimum balance / average balance for set frequencies in period. Bank may withdraw the provision of Internet Banking, wholly or partly, if at any time the amount of deposit falls short of the required minimum as aforesaid and / or if the service charges remain unpaid, without giving any further notice to the user and / or without incurring any liability or responsibility whatsoever by reason of such withdrawal.

## **12. FUNDS TRANSFER:**

- i. The User shall not use or attempt to use Internet Banking Services for funds transfer without sufficient funds in the relative account or without a pre-existing arrangement with the Bank for the grant of an overdraft. The Bank will endeavor to affect such funds transfer transactions received through Internet Banking services provided there are sufficient funds available in the user's account. The Bank shall not be liable for any omission to make all or any of the payments or for late payments due to circumstances beyond the control of the Bank. In the event of overdraft created due to oversight/inadvertently, the User will be liable to pay the interest on such overdrawn amount, as decided by the Bank from time to time.

### **a. TRANSFER OF FUNDS TO OTHER ACCOUNT(S) / PERSON(S):**

- i. The User shall accept that he/she/they will be responsible for keying in the correct account number(s)/other particulars of the beneficiary for the funds transfer request. In no case, the Bank will be held liable for any erroneous transactions incurred arising out of or relating to the User entering wrong/incorrect/incomplete account number, information of the beneficiary and/or any other particulars.
- ii. If funds transfer would have made available to the User, it may be used for transfer of funds between user's own accounts and/or from user account to accounts belonging to third parties maintained at the Bank and/or at other Banks. In such event, transfer of funds into accounts belonging to other third parties as be maintained at any other Bank, which falls under the network of Reserve Bank of India's Electronic Fund Transfer System, the same shall be governed by the Terms of Service (Terms & Conditions) as be applicable to National Electronic Fund Transfer ("NEFT") and Real-Time Gross Settlement System ("RTGS") of the Reserve Bank of India and or its subsidiaries / organizations and structural systems and setup.

b. **Payment and fund transfer security:**

Digital signatures and Key-based Message Authentication Codes (KMAC) for payment or fund transfer transactions could be considered for detection of unauthorized modification or injection of transaction data in a middleman attack. For this security solution to work effectively, a customer using a hardware token would need to be able to distinguish the process of generating a one-time password from the process of digitally signing a transaction. What he signs digitally must also be meaningful to him, which means the token should at least explicitly show the payee account number and the payment amount from which a hash value may be derived for the purpose of creating a digital signature. Different crypto keys should be used for generating OTPs and for signing transactions.

c. **BILL PAYMENTS:**

The user agrees and accepts the Internet Banking services as provided by the Bank at his/her requests to carry out his/her bill payments through Internet Banking services of the Bank as be made available to him/her/them from time to time. If the bill amount exceeds the maximum limit set up by the User for "Auto Pay", the bill will be set for manual payment. The User has to provide correct identification details as registered with the biller. In case of any change in the identification details, it would be the User's responsibility to register the changes immediately. Any dispute on bill details will be settled directly by the user with the Biller and the Bank's responsibility is limited to provision of information only. The user shall make arrangements of funds payments at least few **may mean 1 to 5 working days, depending upon biller and varies from biller to biller.** working days prior to the due date of the bill. The User shall be liable for late payment charges and other consequence as may be enforced by the Biller. The User has no objection whatsoever to the billing company providing his/her billing details to the Bank.

The User unconditionally agrees that he/she shall not hold the Bank liable for:

1. Such transactions that are carried out on his/her instructions by the Bank in good faith.
2. Not carrying out such instructions where the Bank has reason to believe (which decision of the Bank he/she shall not question/dispute) that the instructions are not genuine or are otherwise unclear, improper, vague or doubtful.
3. Accepting instructions given by any one of the users in case of joint accounts.
4. For any loss or damage incurred or suffered by him/her due to any error, defect, failure or interruption in the provision of bill payment services arising from or caused by any reason whatsoever.
5. Withdrawing/suspending the facility wholly/partially. However, the Bank will endeavor to notify the User through its website or through any legally recognized medium of communication or otherwise as found suitable by the Bank.

The User agrees that the record of instructions given and transactions with the Bank shall be conclusive proof and binding for all purposes and can be used as evidence in any proceedings.

d. **MERCHANT PAYMENTS:**

The Bank provides the facility of payment for transactions executed on Internet through different sites. The Bank will execute such transactions and will be responsible for transferring the amount debited from the User's account to the Service /merchants' account. The Bank

shall not be held responsible for failure of such transactions. In no event shall the Bank be held responsible/liable for any informational content provided on any such site or for any deficiency in the services/products offered by such sites.

e. **STANDING INSTRUCTIONS/SCHEDULED PAYMENTS:**

The user can set 'Standing Instructions' or 'Schedule Payments' as on a required date i.e. the date on which the users account shall get debited in the functionality where it is available. If the User wishes to modify / cancel this 'Standing Instruction / Scheduled Payments', the same should be done at least 1 (One) day's prior to the schedule date.

**13. TRANSACTION PROCESSING TIME:**

- **Instantaneous Transactions:**

All the instructions for instantaneous transactions received before the cut off time of the specified transaction, will be given effect to instantaneously unless until some processing work or maintenance activity is being done or some unavoidable circumstances beyond the control of the Bank occur. E.g.: Fund Transfer, Third Party Fund Transfer, stop payment etc.

- **Non-Instantaneous Transactions:**

Non-instantaneous transactions and transactions requiring manual intervention by the branch, the Bank would endeavor to give effect to such transactions at the earliest.

**14. DOCUMENTS REQUIRED FOR TRANSACTION PROCESSING:**

The user shall be responsible for submitting necessary documents and information as the Bank may require along with any request for any service under Internet Banking. If any request for a service is such that it cannot be given effect to unless it is followed up by requisite documentation, the Bank shall not be required to act on the request until it receives such documentation from the User.

**15. ACCURACY OF INFORMATION:**

A customer shall provide such information as the Bank may from time to time reasonably request for the purposes of providing the services. The User is responsible for the correctness of information supplied to the Bank through the use of Internet Banking Services or through any other means such as electronic mail or written communication. The Bank accepts no liability for the consequences arising out of erroneous/incomplete/incorrect information supplied by the User. If the User suspects that there is an error in the information supplied to the Bank by him/her, he/she shall advise the Bank at the earliest. The Bank will endeavor to correct the error wherever possible on a 'best efforts' basis. If the User notices an error in the account information supplied to him/her through Internet Banking Service, he shall advise the Bank at the earliest. The Bank will endeavor to correct the error promptly and adjust any interest or charges arising out of the error.

## 16. CYBER CRIME:

The Internet per se is susceptible to various cybercrimes like phishing, vishing (Voice phishing), SMS (phishing through SMS), compromise of user's system security etc., that could affect Payment Instructions / other instructions to the Bank. Whilst the Bank shall endeavor to protect the interest of the customers, there cannot be any guarantee from such cybercrimes and other actions that could affect Payment Instructions / other instructions to the Bank including but not limited to delay or failure in processing the instructions. The user shall separately evaluate all such risks and the Bank shall not be held responsible for the losses arising out of such cybercrimes. The User understand that doing a Net-Banking transaction at any Cyber cafe/shared computer terminal is risky and shall avoid using the services of any Cyber cafe/shared computer terminal to do any Net-Banking transactions.

## 17. ERRORS OF OMMISION & COMMISSION:

The filling in of applicable data for transfer of funds and/or issue of cheque would require proper, accurate and complete details. For instance, the customer is aware that:

- a. he/she/they would be required to fill in the correct account number of the person to whom the funds are to be transferred.

- b. he/she/they would be required to fill in the correct Card number while making Credit Card payments.

In the event of any inaccuracy in this regard, the funds could be transferred to incorrect accounts or the Cheque may be incorrectly issued or sent to a wrong address and there is no guarantee of recovery of the same thereafter. The User shall therefore take all care to ensure that there are no mistakes and errors and that the information given by him/her to the Bank in this regard is error free, accurate, proper and complete at all points of time. The User indemnifies the Bank from any loss due to an error on his/her part. **As per RBI instructions credit will be affected based solely on the beneficiary account number information and the beneficiary name particulars will not be used there for.** On the other hand, in the event of the User's account receiving an erroneous credit by reason of a mistake committed by some other person or for any other reason, the Bank shall be entitled to reverse the erroneous credit at any time whatsoever without his/her consent. The User shall be liable and responsible to the Bank and accede to accept the Bank's instructions without questions for any unfair or unjust gain obtained by him/her as a result of the same.

## 18. TECHNOLOGY RISKS:

The site of the Bank may require maintenance and during such time it may not be possible to process the request of the customers. This could result in delays and/or failure in the processing of instructions. The User understands that the Bank disclaims all and any liability, whether direct or indirect, whether arising out of loss or otherwise arising out of any failure or inability by the Bank to honor any customer instruction for whatsoever reason.

## 19. AUTHORITY TO THE BANK :

Banking transactions in the User's account(s) are permitted through Internet, only after authentication of the User-id and password of the User. The User irrevocably and unconditionally authorizes the Bank to access all his/her account(s) for effecting banking and

other transactions performed by the User through the Internet Banking services. The instructions of the User shall be effected only when such information is in accordance with the prescribed procedure. The User grants express authority to the Bank for carrying out the banking transactions performed/requested by him/her through Internet Banking Services. The Bank shall have no obligation to verify the authenticity of any transaction received from the User through Internet Banking Service or purported to have been sent by the User via Internet Banking Services, other than by means of verification of the User-id and the password. The display or printed output that is generated by the User at the time of operation of Internet Banking Services is a record of the operation of the Internet access and shall not be construed as the Bank's record of the relative transactions. The Bank's own records of transactions maintained through computer systems or otherwise shall be accepted as conclusive and binding for all purposes. All transactions arising from the use of Internet Banking Services to operate a joint account, shall be binding on all the joint account holders, jointly and severally, notwithstanding that one amongst such joint account holders only operates the accounts through Internet Banking Services.

The Bank may at any time without giving notice or reasons, suspend or terminate all or any of the Internet Banking services or their use by the User.

## **20. RIGHT TO SET OFF AND LIEN:**

- a) Bank shall reserve the right to set off and lien, irrespective of any other lien or charge, present as well as future, on the account(s) held by user(s) or in any other account, whether in single name or joint names to the extent of all outstanding dues, whatsoever arising as a result of the Internet Banking services extended to and/or used by the User.
- b) Normally the customer can access his/her/their accounts through the Online Net Banking only after the customer acknowledges to the respective branch the receipt of the User Name and Password (if any) sent to the customer / user.
- c) The Online Net Banking service cannot be claimed as a Customers' right. The bank may also convert the service into a discretionary service (being a service which may be discontinued by the Bank) anytime, if so warranted, after it has been made available to the customer. The bank may also impose and vary any restrictions on the use of the service at any time including any minimum and maximum daily limits for transactions effected over it.
- d) Transactions over the internet may be subject to interruption, transmission blackout, delayed transmission due to internet traffic, or incorrect data transmission due to the public nature of the internet. The bank cannot assume responsibility for malfunctions in communications facilities not under our control that may affect the accuracy or timelines of messages the customer send.
- e) The Online Net Banking is offered only in jurisdictions where and when it may be lawfully offered. The service and information relating to the service are not intended for access or use by persons in other jurisdictions.

## 21. Internal Control System:

The bank may also consider prescribing suitable monetary limits for the customer on transactions put through internet banking. The internal control system should cover the following:

- a. This would include internal inspection / audit of systems and procedures related to internet banking as also ensuring that adequate safeguards are in place to protect integrity of data, customer confidentiality and security of data. The bank has also considered prescribing suitable monetary limits for the customer on transactions put through internet banking. The internal control system covers the following:
  - i. **Audit Policy to include IS Audit:** IS audit is an integral part of the internal audit of the bank. Through Audit Department, the bank has put in place a system to ensure that a robust audit trail is generated to facilitate conduct of audit, serving as forensic evidence when required and assist in dispute resolution.
  - ii. **Reporting and Follow-up:** Any breach or failure of security systems and procedures is reported to the next higher authority and to the Audit Committee. IS Auditors preparing an audit summary memorandum providing overview of the entire audit processing from planning to audit findings, discuss the findings with auditee and obtain responses.
  - iii. The bank has a communication plan for escalating/reporting to the Board/Senior Management/ RBI/NABARD to proactively notify major cyber security incidents.
  - iv. **Monetary Limits:** Bank sets daily transaction limit for existing transaction option available in the internet banking like own account transfer, third party transfer, NEFT, RTGS, IMPS transfer and also for the any other transaction facility introduced in the future. These limit will be approved by the management and will be subject to change from time to time as per the discretion of the bank.
  - v. The bank shall maintain records in this regard for reconciliation of the entries and settlements required from SBI in the dedicated account opened for this purpose.

## 22. Bank's Terms:

- a. The rules and regulations applicable to the banking transactions done in traditional way at the branch of Tamluk Ghatal Central Co-Operative Bank Ltd. will be applicable for the transactions done through the service.
- b. Disputes between the registered user of this service and the bank with regard to the transactions done through Online Net Banking will be subject to the jurisdiction of the Court of Tamluk where Head Office of the bank is situated.
- c. The bank will take reasonable care to make use of the available technology for ensuring security and preventing unauthorised access to any of the services offered through the Online Net Banking.

- d. The Online Net Banking service is a secure site. It assures that during the session the customers are dealing with website of TGCCB, the two-way communication is secured with 128-bit SSL encryption technology, which ensures the confidentiality of the data during transmission. The access-control methods designed on the site afford a high level of security to the transactions conducted on Online Net Banking.
- e. The bank reserves the right to modify, change, add or cancel any of the services offered through Online Net Banking without prior notice to the users or the terms of service listed in this document by reasonable prior notice to the customer. The changes will be notified to the customer / customers through a notification on the site.
- f. The bank does not warrant or represent that the Online Net Banking is free from virus or other destructive features which may adversely affect customer's hardware, software or equipment.

### **23. Customers' Obligations:**

- a) Password of the customer's choice must replace the password given by the bank at the time of FIRST log-in. This is mandatory.
- b) The customers are free to choose the password of his/her/their choice as per the guidelines on the site. However, the customers are advised to avoid choosing a password that is generic in nature, guessable / inferable from the personal data such as name, date of birth, address, telephone number, driving license / car number etc. The customer should not use the password for accessing other services (for example, connection to the internet or accessing other websites).
- c) The customers are welcome to access Online Net Banking from anywhere anytime where it is legal to do so in the relevant place. However, as a matter of precaution and safety, the customer should avoid using PCs with public access or internet café computers.
- d) There is no way to retrieve the password from the system. In case the customer forgets his/her/their password, the customer shall exercise the forget password link therein the site and or in ultimate situation the customer will have to approach the branch to reset the password, in other way customer can change his /her password through Internet Banking. In that case authentication procedure would be either debit card / secret question/ OTP or any other method.
- e) The customer must keep the User Name and Password strictly confidential and known only to himself / herself. The customer should destroy the original printed copy of the User Name and Password, should not allow anyone else to use the User Name and Password, should not write down the User Name or Password on any device for accessing the Online Net Banking service or on anything usually kept with or near it, and should not write down or record the User Name or Password without disguising it. The customer should refer to the security advice provided by the bank from time to time. The bank will

not be responsible for any loss sustained by the customer arising out of a breach of this condition.

- f) The bank presupposes that log-in using valid User Name and Password is a valid session initiated by none other than the customer to whom they said User Name and Password belong. An authenticated session, together with its encryption protocol, remains intact throughout the interaction with the customer. Else, in the event of interference, the session is terminated and the affected transactions resolved or reversed out. The customer is promptly notified of such an incident by email, telephone, SMS or through other means as the session is being opening /transfer fund and concluded.
- g) Changes in mobile phone number can be done only at branch level.
- h) Virtual keyboard is implemented. At the time of beneficiary addition, OTP is sent via SMS alert for each beneficiary added.
- i) If the customer notices that any information relating to his/her/their account(s) is incorrect or discrepant, the customer should visit the home branch to rectify the same.
- j) An online session is automatically terminated after a fixed period of 10 minutes of time unless the customer is re-authenticated for the existing session to be maintained. This prevents an attacker from keeping an internet banking session alive indefinitely.
- k) Specific OTPs for adding new beneficiary: For new beneficiary addition, the customer requires an OTP for authorization.
- l) Individual OTPs for value transactions (payments and fund transfers): For each value transaction, the customer requires a new OTP for authorization.
- m) OTP time window: Time-based OTPs provide strong security because their period of validity is controlled entirely by the bank and does not depend on user behavior. The bank does not allow the OTP time window to exceed 10 Minutes on either side of the server time.
- n) In internet banking scenario, there is very little scope for the bank to act on stop-payment instructions from the customers. Hence, the bank clearly notifies to the customers the timeframe and the circumstances in which any stop-payment instructions could be accepted.
- o) All transactions executed through a valid session as defined above will be construed to have been emanated from the customer and will be legally binding on the customer. The customers are cautioned against leaving the computer unattended during a valid session.
- p) Should the customer notice that any information relating to his/her/their account(s) is incorrect or discrepant the same should be immediately brought to the notice of the branch(es) by telephone/personally.
- q) The customer must inform the bank as soon as reasonably practicable by telephone / through Bank's website / branch visit, if the customers find or believe that his/her/their

User Name or Password has been compromised, lost or stolen, or that unauthorized transactions have been conducted over the account.

- r) The customer will not attempt or permit others to attempt accessing Online Net Banking through any unlawful means or use or attempt to use Online Net Banking for any unlawful purposes.
- s) The customer shall not attempt to decompile reverse-engineer, translate, convert, adapt, alter, modify, enhance, add to, delete or in any way tamper with, or gain access to, any part of Online Net Banking or any internet site or any software comprised in it.
- t) Customers should be advised to adopt various good security precautions and practices in protecting their personal computer and to avoid conducting financial transactions from public or internet café computers.
- u) The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. The rights and liabilities of customers availing of internet banking services need to be clearly explained to customers opting for internet banking. Considering the banking practice and rights enjoyed by customers in traditional banking, the banks' liability to the customers on account of unauthorized transfer through hacking, denial of service on account of technological failure, etc. needs to be assessed and banks providing internet banking should insure themselves against such risks.
- v) Hyperlinks from banks' websites often raise the issue of reputational risk. Such links should not mislead the customers into believing that banks sponsor any particular product or any business unrelated to banking. Hyperlinks from banks' websites should be confined to only those portals with which they have a payment arrangement. Hyperlinks to banks' websites from other portals are normally meant for passing on information relating to purchases made by banks' customers in the portal. Banks must follow recommended security precautions while dealing with requests received from other websites relating to customers' purchases.
- w) Banks should put in place risk-based transaction monitoring and surveillance process. Study of customer transaction behaviour pattern and stopping irregular transaction or obtaining prior confirmation from customers for outlier transactions may be incorporated in the software

#### **24. Disclosures:**

The User shall have to agree that the Bank or its service providers may hold and process his/her Personal/Technical Information on Computer or otherwise in connection with Internet Banking Services as well as for statistical analysis. The User agrees that the Bank may collect User system related information. The User also agrees that the Bank may disclose, in strict confidence, to other institutions, such Personal Information as may be reasonably necessary for reasons inclusive of, but not limited to, the following:

- a. For participation in any electronic clearing network.
- b. In compliance with legal and/or Reserve Bank of India's directive.

- c. The products under internet banking are restricted to account holders only.
- d. The services are included only in local currency products.
- e. The bank adheres to the KYC guidelines / AML standards and the provisions and directions issued under the PMLA 2002.

## **25. Compliance**

i. This policy generally conforms to “Internet Banking Policy” of Reserve Bank of India / NABARD / Govt. Departments & latest guidelines on Internet /electronic banking and information security, wherever a specific mention is not made herein, details provided in RBI/ NABARD guidelines to such context shall hold good as far as it is applicable to the environment.

ii. System Department of the Bank with the approval of CISO, may devise / modify the reporting formats for Information Systems Audit, as and when required.

## **26. Entitlement & Review of the Policy:**

The Board of Directors of the Bank reserves the sole right of the policy and also reserves the right to Review / Amend / Alteration / Modification / Delete the applicability in/of this policy at its sole discretion. Any change in Internet Banking policy is to be effected only by the approval of the Broad of Directors of the Bank and this change would be executed by the Chief Executive Officer (CEO) of the Bank.