SAURASHTRA GRAMIN BANK

Internet Banking Policy

1) PREAMBLE:

With a view to provide better customer service it has been decided to extend the facility of internet banking to bank's customers. This policy establishes basic principles necessary for secure use and management of the bank's internet banking transactions.

2) GENERAL INFORMATION:

a. 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 Region Office. While registering the request, the customer shall be informed about the time normally taken by the bank for fulfillment of such requests.

b. 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 identity of the customer and adherence to the KYC guidelines.

c. 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, and other legal requirements should be scrupulously adhered to.

d. 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, therefore, has in place adequate risk control measures to manage such risks.

e. 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.

f. **Second channel notification / confirmation:** The bank notifies the customer, through SMS, for all payment or fund transfer transactions.

g. **SSL server certificate warning:** Internet banking customers are made aware of and shown how to react to SSL or EV-SSL certificate warning.

h. **Implementation of 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 fund transfers through internet banking has been implemented.
   ii. The implementation of appropriate authentication methodologies is based on an assessment of the risk posed by Internet banking systems.
   iii. There is 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, has implemented robust and dynamic two-factor authentication through user id/password combination and second factor by the way of One Time Password (OTP) sent as SMS over registered mobile phone.
   iv. 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.

i. The registration form(s) should be addressed and sent directly to the branch (the "bank") where the applicant(s)maintain his / her / their account(s). The customer is expected to provide necessary KYC documents and to fulfill KYC procedures.

j. Separate registration is required in case the accounts are maintained at different branches. Separate registration is allowed for single and joint accounts at customer's option.

k. 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 sent to the customer.

l. Each account holder in a joint account with "Either or Survivor" type mode of operation may register himself/ herself as a user of the Online Net Banking facility.

m. All other accounts not listed in the registration form will be available for the purpose of enquiry only. The customers may approach Branch for enabling transaction rights on such account any time.

n. The Online Net Banking service cannot be claimed as a 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.

o. 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.

p. 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.

3) 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 prepare 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.

4) One Time Password Generators:

a. The security is personal to the customer and can only be used with password. It provides an additional level of security for certain transactions and cannot be shared with anyone else.

b. Once activated, 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 (once per session) when the customer adds a third party beneficiary or sends funds to a third party beneficiary.

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-authorised persons or for un-authorised purposes. The bank will deactivate his/her/their service.

d. If the customer(s) have any questions about the security, he/she may call the bank between 10.30 am and 5.30 pm, Monday to Saturday (excluding second and fourth Saturday).

5) Bank's Terms :

a. The rules and regulations applicable to the banking transactions done in traditional way at the branch of Saurashtra Gramin Bank 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 Rajkot 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 SGB, 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.

6) Other Issues and Disclosures:

The existing regulatory framework for the bank is extended to Internet Banking also. In this regard, it is advised that:

a) The products under internet banking are restricted to account holders only.

b) The services are included only in local currency products.

c) The bank adheres to the KYC guidelines / AML standards and the provisions and directions issued under the PMLA 2002.

7) 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 customer 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 will have to approach the branch to reset the password.

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 the 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 as the session is being concluded or subsequently by email, telephone or through other means.

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. 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.

j. 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.

k. 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.

l. The customer must inform the bank as soon as reasonably practicable by telephone 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.

m. 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.

n. 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.

o. 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.

8) Customer's Liabilities :

We have made it compulsory for the customers to enable SMS facility before registering for Internet banking and mobile banking. The customers are advised to notify the bank of any unauthorized electronic banking transaction at the earliest. To facilitate this, we have provided toll free number to customers, which is available during office hours (We are in processing for implementing 24 hour Customer help desk, through C-edge, bank's ASP).

Broadly, the electronic banking transactions can be divided into two categories:
(i). Remote/ online payment transactions (transactions that do not require physical payment instruments to be presented at the point of transactions e.g. internet banking, mobile banking, card not present (CNP) transactions), Pre-paid Payment Instruments (PPI), and
(ii). Face-to-face/ proximity payment transactions (transactions which require the physical payment instrument such as a card or mobile phone to be present at the point of transaction e.g. ATM, POS, etc.)

(a) Zero Liability of a Customer

A customer's entitlement to zero liability shall arise in case of unauthorized transaction occurs in the following events:-

(i) Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).

(ii) Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within **three working days** of receiving the communication from the bank regarding occurrence of that transaction.

(b) Limited Liability of a Customer

A customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:

(i) In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the bank.

(ii) In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in Table 1, whichever is lower.

Table 1	
Maximum Liability of a Customer	
Type of Account	**Maximum liability (Rs.)**
• BSBD Accounts.	5,000
• All other SB accounts. • Pre-paid Payment Instruments. • Current/ Cash Credit/ Overdraft Accounts of MSMEs. • Current Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 Lakhs.	10,000
• All other Current/ Cash Credit/ Overdraft • Credit cards with limit above Rs. 5 Lakhs	25,000

Further, if the delay in reporting is beyond seven working days, the customer liability will be 100 percent. Banks shall provide the details of their policy in regard to customers' liability formulated in pursuance of these directions at the time of first login

by the customer in the internet banking. Banks shall also display their approved policy in public domain for wider dissemination.

Overall liability of the customer in third party breaches, as detailed above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarised in the Table 2:

Table 2	
Summary of Customer's Liability	
Time taken to report the fraudulent transaction from the date of receiving the communication	**Customer's liability (₹)**
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned in Table 1, whichever is lower.
Beyond 7 working days	100 percent liability

The number of working days mentioned in Table 2 shall be counted excluding the date of receiving the communication.

(c) Reversal Timeline for Zero Liability/ Limited Liability of customer

On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any). Banks may also at their discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence. The credit shall be value dated to be as of the date of the unauthorised transaction.

Further, banks shall ensure that:

i. where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs 8(a) to 8(c) is paid to the customer; and

ii. In case of debit card/ bank account, the customer does not suffer loss of interest, and in case of credit card, the customer does not bear any additional burden of interest.

Burden of Proof

The burden of proving customer liability in case of unauthorised electronic banking transaction shall lie on the bank.

Reporting and Monitoring Requirements

In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system, which will include transaction like card present transactions, card not present transactions, internet banking, mobile banking, ATM transactions, etc. Any such case, if occurred, will be reported to Board on quarterly basis. The reporting to Board of Director will include all transactional details such as type of transaction, transaction reference number, amount involved, date of transaction, date of reversal of transaction, interest paid, if any, and brief narration of each case.

If such transaction amount is up to Rs 50,000/-, General Manager will be the competent authority to give permission and if it exceed 50,000/-, Chairman will be the competent authority.

9) Privacy Policy :

In line with recognized international practice and for the information of customers and others who visit the bank's website we believe it is necessary to post a privacy statement. The information shared with the bank will be treated as private. We also desire to say explicitly that adequate precautions have been taken to protect information relating to the customer and their dealings with the bank from the mischievous and the fraudsters. Customer confidentiality and privacy is of utmost concern to SGB. Our employees treat the information we have concerning customers' accounts in the same responsible and confidential way that we want our own financial affairs treated.

10) Recognition of customer(s)' expectation of privacy:

We recognize that our customers expect privacy and security for their personal and financial affairs. We understand that, by selecting us for customers' banking needs, the customer have entrusted us to safeguard his/her/their personal financial information. We want the customer to be informed of our commitment to protect the privacy of his/her/their personal financial information, which includes customer name, address, email addresses, KYC details, details of nominees, PAN etc.

11) Cookies:

a. A cookie is a data file that certain web sites write to customer computer's hard

drive when the customer visit such sites. A cookie file can contain information such as a user identification code that the site uses to track the pages the customer has visited and use the information commercially. We do not use cookies on our web site.

b. How we use, collect, and retain customer information

   i. On our site we collect, retain, and use information about the customer only when we reasonably believe that it will help administer our business or provide products, services, and other opportunities to the customer. We collect and retain information about the customer only for specific business purposes.

   ii. We use information to open and administer customers' accounts and to protect customer's records and funds, comply with all applicable laws and regulations, help us design or improve our products and services for customer's benefit. Understand customer's financial needs so that we can provide the customer with quality products and superior services. To comply with laws, guidelines and regulations that governs financial services in the country. To quote examples we need to obtain passport number for NRI account & PAN for deposit accounts in respect of resident customers.

12) How we keep customer information accurate:

It is in the customer's interest, and it is our objective for us to have accurate, current and complete information concerning the customer and customer's accounts. We have strict procedures that our employees abide by to meet this objective. While some procedures are required by Central, State laws or RBI regulations, we have implemented additional procedures to maintain accurate, current, and complete financial information, including processes to update information and remove outdated information. If the customer believes that we have incorrect information about the customer or customer's accounts, he / she can email us through the feedback mechanism provided on the website or modify the profile information on the site as permissible. We will correct any erroneous information as quickly as possible.

13) How we limit access to customer information by our employees:

We have procedures that limit access to personally identifiable information to those employees with a business reason for knowing such information about the customer. We educate our employees on their responsibility to protect the confidentiality of customer information and hold them accountable if they violate this privacy policy.

14) Our security procedures to protect customer information:

a) We follow best security practices to prevent unauthorized access to confidential information about the customer.

b) Re-establishment of any session after interruption requires normal user identification, authentication, and authorization. Moreover, strong server side validation are enabled.

c) Multifactor authentication methods are in place. The principal objectives of two factor authentication are to protect the confidentiality of customer account data and transaction details as well as enhance confidence in internet banking by combating various cyber attack mechanisms like phishing, key logging, spyware/malware and other internet based frauds targeted at the bank and their customers.

d) As an integral part of the two factor authentication architecture, the bank has also implemented appropriate measures to minimize exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack.

e) The bank considers, and if deemed appropriate, implement the following control and security measures to minimize exposure to man-in-the middle attacks:

i. **Specific OTPs for adding new payees**: Each new payee should be authorized by the customer based on an OTP from a second channel.

ii. **Individual OTPs for value transactions (payments and fund transfers)**: For each value transaction determined by the customer requires a new OTP.

iii. **OTP time window:** Challenge-based and 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 60 seconds on either side of the server time since the smaller the time window, the lower the risk of OTP misuse.

iv. 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.

15) How we restrict the disclosure of customer information:

SGB does not release customer information except as directed by law or as per customer's mandate. We do not share specific information about customer accounts or other

personally identifiable data with non-affiliated third parties for their independent use unless:

i) The information is provided to help complete a transaction initiated by the customer;
ii) The customer request or authorize it;
iii) The disclosure is required by/or directed by law; or
iv) The customer(s) have been informed about the possibility of such disclosure for marketing or similar purposes through a prior communication and have been given the opportunity to decline.

16) Other information about our website:

a. For customers using our SGB Internet Banking, all visitor information is collected along with any information that the customers volunteer as a customer while using SGB's web site, links to or from SGB's web site.

b. SGB is not responsible for information practices employed by web sites linked with our web site. Generally, links to non-SGB web sites are provided solely as pointers to information on topics that may be useful to users of SGB's website.

17) Encrypted information:

Information provided by the customer on SGB's web site is encrypted or scrambled in order to secure information. Privacy policy is subject to change periodically.

18) Bank will follow all the instructions and guidelines from RBI regarding Net Banking Services for ensuring smooth functioning of the scheme. Bank to maintain records in this regard for reconciliation of the entries and settlements required from SBI in the dedicated account opened for this purpose.

19) Monetary limit

Bank will set daily transaction limit for existing transaction option available in the internet banking like own account transfer, third party transfer and NEFT transfer and also for the any other transaction facility introduced in the future. These limit will be approved by the management and will be subjected to change from time to time as per the requirement of the bank.