

The logo of Saurashtra Gramin Bank is a circular emblem. It features a central map of Gujarat in shades of yellow and green. Above the map is a golden lion. The text 'SAURASHTRA GRAMIN BANK' is written in Devanagari script at the top. Below the map, the acronym 'SGB' is visible. The words 'SAFETY - SECURITY - GROWTH' are written in a semi-circle above the map. The entire emblem is framed by a blue border with yellow wheat stalks on the sides and a grey industrial building silhouette at the bottom.

SAURASHTRA GRAMIN BANK

Internet Banking Policy

Version-2.0

Table of Contents

1.	Preamble	3
2.	Application	3
3.	Eligibility	3
4.	Obligation of Bank.....	3
5.	Bank's Right.....	4
6.	Bank's Work Flow.....	4
7.	Customer's Work Flow & Obligations	5
8.	Limited Liability of Customer	6
9.	Internal Control System	9
10.	Governing Laws.....	9
11.	Security	10
12.	Privacy Policy	12
13.	Other information about INB website	14
14.	Review of Policy	14

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 facility.

2) Application

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.

3) Eligibility

The facility is available for customers having a satisfactory running account. The Facility shall be offered to resident individuals (including Minor Accounts above the age of 10 years) with mode of operation 'Self, Either/ Survivor'. 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.

4) Obligation of Bank

- a. 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 only after verification of the identity of the customer and adherence to the KYC guidelines.
- b. 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 an agreement with ASP to safeguard the details of the customers.

5) Bank's Right

- a. The rules and regulations of the normal banking transactions will be applicable for the transactions done through INB service.
- b. The Internet Banking service cannot be claimed as a right of customer. 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.
- c. 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 internet. The bank shall not assume responsibility for malfunctions in communications facilities not under control of the bank that may affect the accuracy or timelines of messages the customer send.
- d. The bank reserves the right to modify, change, add or cancel any of the services offered through Internet Banking without prior notice to the users or by reasonable prior notice to the customer. The changes will be notified to the customer(s) through a notification on the bank's website / Branch Notice Board / SMS.
- e. The bank does not warrant or represent that the Internet Banking is free from virus or other destructive features which may adversely affect customer's hardware, software or equipment.

6) Bank's Work Flow

- a. The application form(s) should be held with 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 fulfil KYC procedures.
- b. Internet Banking can be registered only at customer's home branch of SGB and all the accounts associated with customer's CIF will be auto registered for INB, hence separate account wise registration is not required. All the accounts linked with the CIF of customer will be made available on Internet Banking.
- c. The customer's Internet Banking services will be activated after receipt of the application by the Home branch. The branch will verify the application and after necessary due-diligence, the services will be activated for the customer.

7) Customers' Work Flow And Obligations

- 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. The customers are free to choose the password of his/her/their choice as per the password policy of Bank. 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 Internet 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. 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.
- d. In terms of keeping security, there is no possibility to retrieve the existing password from system. Retail customer has to perform forgot password option to reset the password and Corporate Customer need to approach the home branch to reset the password.
- e. The customer must keep the User Name and Password/OTP strictly confidential and known only to himself / herself. The customer should not allow anyone else to use the User Name and Password/OTP, should not write down the User Name or Password/OTP on any device for accessing the Internet 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 such 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 by SMS as the session is being concluded.

- g. 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.
- h. 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.
- 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. The customer should intimate the bank immediately over telephone/e-CMS / branch visit, if the customers finds or believe that his/her/their User Name or Password/OTP has been compromised or stolen, or that unauthorized transactions have been conducted in the account.
- m. The products under internet banking are restricted to account holders only. The customer will not attempt or permit others to attempt accessing Internet Banking through any unlawful means or use or attempt to use Internet 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 Internet Banking or any internet site or any software comprised in it.

8) Limited Liability of Customer

Bank has 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, bank has provided toll free number to customers, which is available during office hours.

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 where the unauthorised transaction occurs in the following events:

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

(b) Limited Liability of a Customer

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

- 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.
- 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 under Limited Liability	
Type of Account	Maximum liability (₹)
• BSBD Accounts	5,000
• All other SB accounts • 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 lakh	10,000
• All other Current/ Cash Credit/ Overdraft Accounts	25,000

Further, if the delay in reporting is beyond seven working days, the customer liability will be 100%. Bank shall provide the details of the policy in regard to

customers' liability at the time of opening the accounts. Bank shall also display board approved policy in public domain for wider dissemination.

Overall liability of the customer in third party breaches, as detailed in paragraph 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 % Liability

(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). Bank may also at its 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, bank shall ensure that:

- Where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraph 8(a) to 8(c) is paid to the customer; and
- In case of debit card/bank account, the customer does not suffer loss of interest, and in case of cash credit/overdraft bank account, the customer does not bear any additional burden of interest.

(d) Burden of Proof

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

(e) Reporting and Monitoring Requirements

Bank shall report 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, ATM transactions etc. to the 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.

9) Internal Control System

The Internal Control System 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 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 top Management of the bank and to the Audit Committee of the board. 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. **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.
- iv. 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.
- v. The bank has a communication plan for escalating/reporting to the Board/Senior Management/ RBI/NABARD to proactively notify major cyber security incidents.

10) Governing Laws

The existing regulatory framework for the bank is extended to Internet Banking also. Bank will follow all the instructions and guidelines from RBI regarding Internet Banking Services for ensuring smooth functioning of the scheme

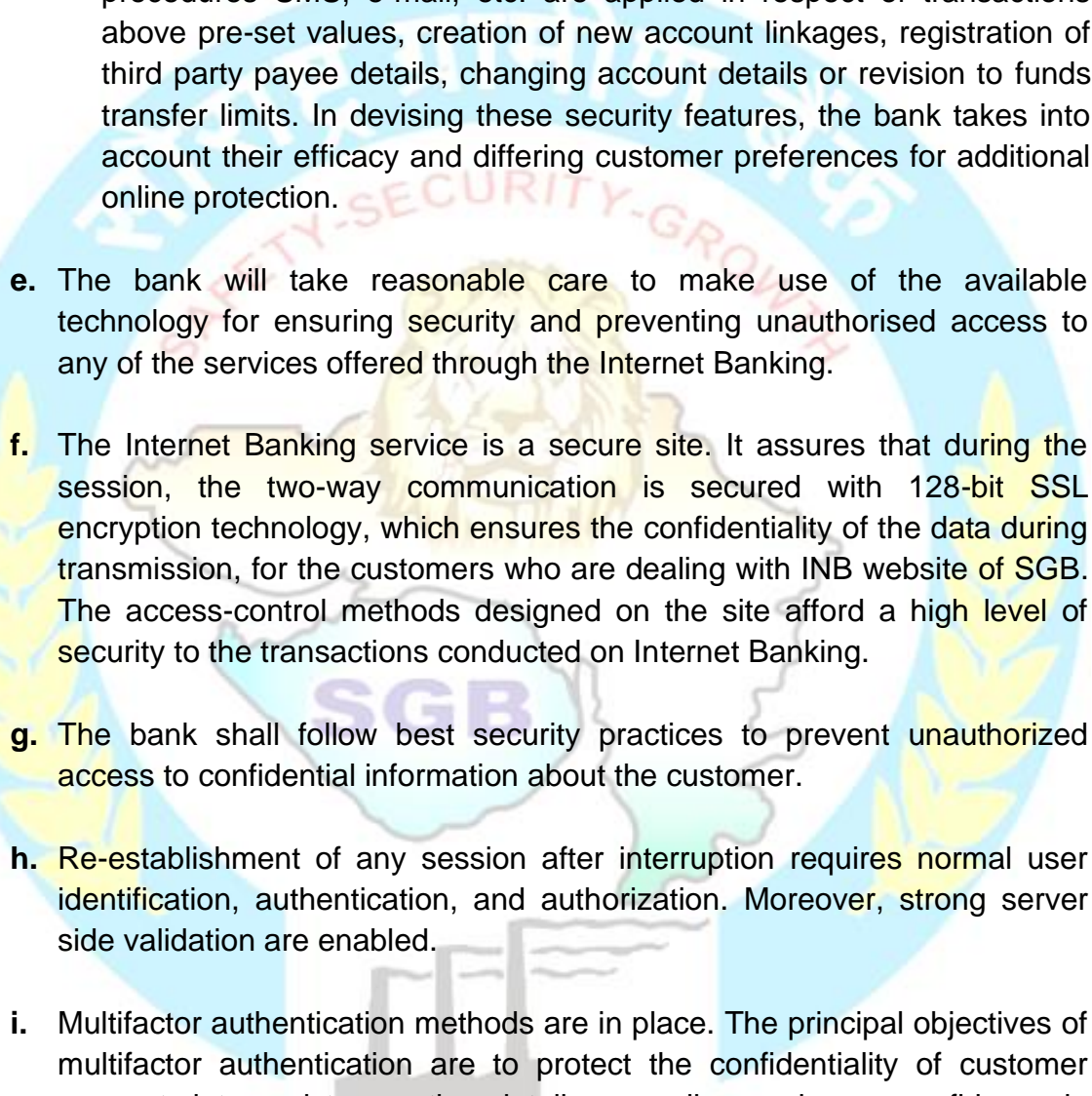
From a legal perspective, security procedure adopted for authenticating a user needs to be recognized by law as a substitute for signature. The provisions of the Information Technology Act 2000, Information Technology Amendment Act 2008 and other legal requirements should be scrupulously adhered to.

The Internet Banking is offered only in jurisdictions where and when it may be lawful. The service and information relating to the service are not intended for access or use by persons in other jurisdictions. The jurisdiction for disputes between bank and the customer shall be as per the guideline of Consumer Protection Act, 2019.

The bank shall adhere to the KYC guidelines / AML standards and the provisions and directions issued under the PMLA 2002.

11) Security

- a. Hyperlinks from the INB website will be confined to only those portals with which bank has a payment arrangement. Hyperlinks to the INB 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.
- b. **Second channel notification / confirmation:** The bank notifies the customer, through SMS, for all payment or fund transfer transactions.
- c. **SSL server certificate warning:** Internet banking links are registered with SSL or EV-SSL certificate.
- d. **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. 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.
 - iii. The implementation of appropriate authentication methodologies is based on an assessment of the risk posed by Internet banking systems.

- 
- iv. There is a legal risk in not using the asymmetric cryptosystem and hash function for authenticating electronic transactions. For carrying out critical transactions like financial transactions, the bank, at the least, has implemented robust and dynamic two-factor authentication through user id/password combination for Login & Profile access and second factor by the way of One Time Password (OTP) sent as SMS over registered mobile number.
 - v. To enhance online processing security, confirmatory second channel procedures 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.
 - e. 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 Internet Banking.
 - f. The Internet Banking service is a secure site. It assures that during the session, the two-way communication is secured with 128-bit SSL encryption technology, which ensures the confidentiality of the data during transmission, for the customers who are dealing with INB website of SGB. The access-control methods designed on the site afford a high level of security to the transactions conducted on Internet Banking.
 - g. The bank shall follow best security practices to prevent unauthorized access to confidential information about the customer.
 - h. Re-establishment of any session after interruption requires normal user identification, authentication, and authorization. Moreover, strong server side validation are enabled.
 - i. Multifactor authentication methods are in place. The principal objectives of multifactor 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.
 - j. As an integral part of the multifactor 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.

- k. The bank implements following control and security measures to minimize exposure to man-in-the middle attacks:
- i. **Specific OTPs for adding new beneficiary:** For new beneficiary addition, the customer requires an OTP for authorization.
 - ii. **Individual OTPs for value transactions (payments and fund transfers):** For each value transaction, the customer requires a new OTP for authorization.
 - iii. **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 behaviour. The bank does not allow the OTP time window to exceed 10 Minutes on either side of the server time.
 - 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.

12) Privacy Policy

In line with recognized international practice and for the information of customers and others who visit the bank's Internet Banking website, bank believes it is necessary to post a privacy statement. The information shared with the bank will be treated as private.

a. Recognition of customer(s)' expectation of privacy

Bank recognise that customers expect privacy and security for their personal and financial affairs. Moreover, bank shall understand that the customer have entrusted them to safeguard his/her/their personal financial information.

Bank shall take adequate precautions 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 the bank. The bank shall handle the customer information in the same responsible and confidential way that bank do for their own financial affairs.

b. Cookies

A cookie is a data file that websites 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. Bank do not use cookies on Internet Banking site.

How bank use, collect, and retain customer information

- i. On the INB website, the bank shall collect, retain, and use information about the customer only when the bank reasonably believe that it will help administer our business or provide products, services, and other opportunities to the customer. Bank collects and retain information about the customer only for specific business purposes.
- ii. The bank shall use information to open and administer customers' accounts and to protect customer's records and funds, comply with all applicable laws, guidelines and regulations, help us design or improve our products and services for customer's benefit, understand customer's financial needs so that bank can provide the customer with quality products and superior services.

c. Keeping customer information accurate

It is in the customer's interest, and it shall be the bank's objective to have accurate, current and complete information concerning the customer and customer's accounts. Bank shall have strict procedures that employees abide to meet this objective. While some procedures are required by Central, State laws or RBI regulations, bank shall implement processes to update latest information and remove outdated information. If the customer believes that bank has incorrect information about the customer or customer's accounts, he / she can raise ticket through the e-CMS feedback mechanism provided on the website or modify the profile information on the site as permissible. The bank will correct any erroneous information as quickly as possible.

d. Limiting access to customer information by bank's employees

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

e. Restricting the disclosure of customer information

The Bank does not release customer information except as specified in the Bank's Customer Rights policy.

13) Other information about INB website

- a. For customers using SGB Internet Banking, all the information feed is collected along with any information that the customers volunteer as a user while using SGB's INB website and its links.
- b. SGB is not responsible for information practices employed by web sites linked with our INB website. Generally, links to non-SGB websites are provided solely as pointers to information on topics that may be useful to customers.

14) Review of Policy

Technology Department shall put up the policy for review to the Board on annual basis. Any instructions/circulars received from regulators in respect of this policy shall form part of this policy and shall be implemented / amended suitably at the time of periodical review.

