SECURITY STATE BANK
Independence, Urbana, Dysart Iowa

Internet / Mobile Banking Agreement and Disclosure

Requirement: You must have an account with Security State Bank to access Internet/Mobile Banking.

Enrollment Instructions: If you are currently an accountholder with Security State Bank we invite you to enroll in Internet/Mobile Banking. Please contact Security State Bank to enroll for the Internet/Mobile Banking Service. Or, if you prefer to enroll through a mail-in enrollment form please read through the following Agreement and Disclosure. At the end of this Agreement is an enrollment form you can print, fill out completely, sign, and send to Security State Bank, P.O. Box 511, Independence, IA 50644. After a verification period we will contact you with enrollment information.

Preface
Security State Bank is pleased to offer you Internet/Mobile Banking. Our Internet/Mobile Banking product allows you to conduct your banking at your convenience from home, work, or wherever you may have access to the world-wide web. We are located on the world-wide web at www.ssbindee.com. Security State Bank’s Internet/Mobile Banking consists of a mobile banking website, text messaging service, downloadable mobile app, and an online banking web site that provides a complete array of financial services to our customers.

Security State Bank’s Internet/Mobile Banking system currently allows our customers to:
- View accounts (Balances, transaction history, loan payment history, etc.)
- Schedule a one-time transfer between accounts
- Schedule a recurring transfer between accounts
- Make payment transfers to your SSB loan accounts (principal & interest basis)
- Print account statements and histories
- Send E-mails to SSB
- Pay Bills

**Important Note**
Internet/Mobile banking transactions have a cut-off time of 6:00p.m. If you conduct an internet/mobile transaction before 6:00pm on Monday through Friday on a business day that we are open, we will consider that day to be the day of your transaction. However, if you conduct a transaction after 6:00pm on Monday through Friday or on a day we are not open, we will consider that the transaction was made on the next business day we are open.

**Important Note**
All loan payment transfers through Internet/Mobile Banking are automatically paid to principal and interest. If you would like to pay off a loan please stop in or call Security State Bank.

1. Introduction.
This Online banking Agreement and Disclosure governs your use of Online/Mobile Banking. Throughout this agreement the Agreement and Disclosure will be referred to as “Agreement”. By using Online/Mobile Banking, you agree to all of the terms of this Agreement. Please read it carefully and retain a copy for your
records.

2. The Service.
In consideration of the Online/Mobile Banking services ("Services") to be provided by Security State Bank ("Bank"), “Customer”, “You”, “Your”, refers to the person(s) subscribing to or using the Service. “We”, “Us”, “Our”, refers to Security State Bank and any agent, independent contractor, designee, or assignee Security State Bank may involve in the provision of Online/Mobile Banking. “Business Day” refers to any calendar day other than Saturday, Sunday, or any holidays recognized by Security State Bank.

3. Privacy Policy
Security State Bank recognizes and respects our responsibility to protect our customers’ private information. In continuing our commitment to provide quality service to our customers, Security State Bank has adopted the following privacy policy. This privacy policy applies to individuals, and Security State Bank reserves the right to amend it at any time. If your relationship with Security State Bank changes and/or is terminated, we will continue to adhere to the privacy practices described in this policy.

Our Collection, Use and Retention of Customer Information
We collect, use, and retain information about our customers only where we reasonably believe it would be useful in administering our business, and providing products, services, and other opportunities to our customers. We collect and retain information only for specific business purposes – and will tell you why we are collecting and retaining it upon your request. We use information to protect and administer our customers’ records, accounts, and funds; to comply with certain laws and regulations; to help design or improve our products and services; and to understand your financial needs in order to provide you with quality products and outstanding service. Nonpublic personal information is nonpublic information about you that we obtain in connection with providing a financial product or service to you. For example, nonpublic personal information includes information regarding your account balance, payment history, etc. We may collect nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other loan and account forms;
- Information about your transactions with us, our affiliates, or others; and
- Information we receive from third parties such as credit bureaus.

Disclosure of Customer Information
We are permitted under law to disclose specific information about your accounts or other personally identifiable data to either affiliated or non-affiliated third parties in the following circumstances:

- When you have requested or authorized it;
- When the information is provided to help complete a transaction initiated by you;
- When the information is provided to a reputable credit bureau or similar credit reporting agency;
- When the disclosure is lawfully permitted or required (for instance, in accordance with a court order, or a regulatory examination);
- When the information is disclosed to either affiliated or non-affiliated third parties to assist us in servicing your loan or account with us;
- When the information is disclosed to our affiliates and the information is about our experiences or transactions with you or your accounts; and
- In any other circumstance permitted or required by law.

Information We Disclose for Joint Marketing Purposes
We may disclose all of the information we collect, as described above, to companies that perform marketing services on our behalf or to other financial institutions with whom we have joint marketing agreements.
Safeguarding the Security of Customer Information
We maintain physical, electronic, and procedural information safeguards that comply with federal standards to protect nonpublic personal information. We continually evaluate and assess new technology for protecting information.

Limited Employee Access to Information
We have procedures and security levels that limit employee access to personally identifiable information to those with a business reason to know such information. The importance of confidentiality and customer privacy is addressed with utmost seriousness. Appropriate measures are taken to enforce employee privacy responsibilities.

Maintenance of Accurate Information
We have implemented procedures to ensure that our customers’ financial information is accurate, current, and complete in accordance with commercial standards and federal law. We also have procedures for responding to requests to correct inaccurate information in a timely manner, and to update information and remove non-current information. Customers should notify us immediately at (319) 334-7035/P. O. Box 511, Independence, IA 50644-0511 if they believe our records contain inaccurate or incomplete information.

Our Privacy Policy and You
If you have any questions about this policy or concerns about the privacy of your information, please contact us at (319) 334-7035.

4. Your User Code and PIN.
Each individual who has access to Online/Mobile Banking, including each individual named on joint accounts, must designate a User Code and a Password. Your Password must be a minimum of 6 characters and a maximum of 9 characters. It must have at least 3 numeric characters and 3 alpha characters. For example, your Password maybe: JOB123. You will be given a random temporary Password to access the system the first time. Upon logging in for the first time you will be prompted to change your password immediately. Your User Code can be changed once upon initial log in. This is the only opportunity to change your User Code. It is recommended that you change your Password periodically to enhance security. If you leave your online/mobile banking session and do not log out manually you will automatically be logged out after ten minutes and will need to enter your user code and password again to regain access to the system. If there are three consecutive failed log-in attempts to Internet/Mobile Banking the user will be locked out of the system and will need to call Security State Bank to regain access to the system.

5. Internet Security
Security State Bank is pleased to offer Internet/Mobile banking. Delivering these services requires a solid security framework that protects you and our institution’s data from outside intrusion. We are committed to working with our internet service and communication providers to produce the safest operating environment possible for our customers. The information below summarizes our security framework, which incorporates the latest proven technology. A section at the end also summarizes your responsibilities as a user of the internet/mobile banking system with regard to security. There are several levels of security within our security framework. User Level deals with cryptography and Secure Socket Layer (SSL) protocol, and is the first line of defense used by all customers accessing our Banking Server from the public Internet. Server Level focuses on firewalls, filtering routers, and our trusted operating system. Host Level deals specifically with our internet banking services, and the processing of secure financial transactions.
User Level
There are several components of User Level security that ensure the confidentiality of information sent across the public Internet. The first requires your use of a fully SSL-compliant 128 bit encrypted browser or Microsoft Internet Explorer. SSL is an open protocol that allows a user’s browser to establish a secure channel for communicating with our Internet server. SSL utilizes highly effective cryptography techniques between your browser and our server to ensure that the information being passed is authentic, cannot be deciphered, and has not been altered en route. SSL also utilizes a digitally signed certificate that ensures that you are truly communicating with the Online Banking Server and not a third party trying to intercept the transaction. After a secure connection has been established between your device and our server, you then provide a valid User ID and Security Code to gain access to the services. This information is encrypted, logged by the server forming complete physical security layer to protect the server’s information, and a request to log on to the system is processed. Although SSL utilizes proven cryptography techniques, it is important to protect your User ID and Security Code from others. You must follow the Security Code parameters we specify at the time you sign up for an Internet Banking account. We also recommend changing your Security Code often. Session time-outs and a limit on the number of logon attempts are examples of other security measures in place to ensure that inappropriate activity is prohibited at the user level.

Server Level
All transactions sent to our Banking Server must first pass through a filtering router system. These filtering routers automatically direct the request to the appropriate server after ensuring the access type is through a secured browser and nothing else. The routers verify the source and destination of each network packet, and manage the authorization process of letting packets through. The filtering routers also prohibit all other types of Internet access methods at this point. This process blocks all non-secured activity and defends against inappropriate access to the server. The Banking server is protected using the latest firewall platform. This platform defends against system intrusions and effectively isolates all but approved customer financial requests. The platform secures the hardware running the Online applications and prevents associated attacks against all systems connected to the Banking Server. The system is monitored 24 hours a day, seven days a week for a wide range of anomalies to determine if attempts are being made to breach our security framework.

Host Level
Once authenticated, the customer is allowed to process authorized internet/mobile banking transactions using host data. In addition, communication timeouts ensure that the request is received, processed, and delivered within a given time frame. Any outside attempt to delay or alter the process will fail. Further password encryption techniques are implemented at the host level, as well as additional security logging and another complete physical security layer to protect the host information itself.

User Responsibilities
While our service provider continues to evaluate and implement the latest improvements in Internet security technology, users of the online/mobile banking system also have responsibility for the security of their information and should always follow the recommendations listed below:

- Utilize the latest 128 bit encryption version of your Internet Browser.
- Your Security Code must be kept confidential. You must follow our specific parameters for a Security Code and change it frequently to ensure that the information cannot be guessed or used by others. Be sure others are not watching you enter information on the keyboard when using the system.
- Never leave your computer/device unattended while logged on to the online/mobile banking system. Others may approach your computer/device and gain access to your account information if you walk away.
- Click Exit when you are finished using the system to properly end your session. Once a session has been ended, no further transactions can be processed until you log on to the system again.
- Close your browser when you are finished, so that others cannot view any account information displayed on your computer/device.
• Keep your computer/device free of viruses. Use virus protection software to routinely check for a virus on your computer/device. Never allow a virus to remain on your system while accessing the online/mobile banking system.
• Report all crimes to law enforcement officials immediately
• Do not choose an easily guessed password, and never write down your password

When you follow these simple security measures, your interaction with the online/mobile banking system will be completely confidential. We look forward to serving your online/mobile banking needs both today and into the future – securely!

6. Equipment
You are solely responsible for the equipment (including, in the case of Online/Mobile Banking, your personal computer/device and software) you use to access the Services. We are not responsible for errors or delays or your inability to access the Services caused by your equipment. We are not responsible for the cost of upgrading your equipment to stay current with the Services nor are we responsible, under any circumstances, for any damage to your equipment or the data resident thereon.

7. Virus Protection
Security State Bank is not responsible for any electronic virus or viruses that you may encounter. We encourage our customers to routinely scan their PC/device and diskettes using a reliable virus product to detect and remove any viruses. Undetected or un-repaired viruses may corrupt and destroy your programs, files and even your hardware. Additionally, you may unintentionally transmit the virus to other computers.

8. Business Days/Hours of Operation
Our lobby hours are 8:30a.m.- 4:30p.m. Monday – Thursday, 8:30a.m.- 5:00 p.m. –Friday, 5:00 p.m. – 6:00 p.m. Friday (Drive Up Only), and 8:30a.m. – 11:30p.m. Saturday (Drive Up Only). Everyday is a business day, except for Saturdays, Sundays, and Security State Bank holidays. Our policy is to make funds available to you on the first business day after the day we receive your deposit/transfer. However, Internet/Mobile banking transactions have a cut-off time of 6:00p.m. If you conduct an internet/mobile transaction before 6:00pm on Monday through Friday on a business day that we are open, we will consider that day to be the day of your transaction. However, if you conduct a transaction after 6:00pm on Monday through Friday or on a day we are not open, we will consider that the transaction was made on the next business day we are open. You are free to schedule internet/mobile transfers/payments 24 hours a day, seven days a week with Internet/Mobile banking, except during maintenance periods.

9. Notice of Your Rights and Liabilities
Security of your transactions is important to us. Use of the Services may therefore require a PIN or password. If you lose or forget your PIN or password, please call (319) 334-7035 or 1-888-384-7780 during normal business hours listed above. We may accept as authentic any instructions given to us through the use of your password or PIN. You agree to keep your PIN and password secret and to notify us immediately if your PIN or Password is lost or stolen or if you believe someone else has discovered your PIN or password. You agree that if you give your PIN or password to someone else, you are authorizing them to act on your behalf, and we may accept any instructions they give us to make transfers or otherwise use the Services. Online/Mobile Banking Services enables you to change your password and we require that you do so regularly. We may be liable for certain security breaches to the extent required by applicable law and regulation. We do not assume any other liability or otherwise guarantee the security of information in transit to or from our facilities. Please note that we reserve the right to (1) monitor and/or record all communications and activity related to the Services; and (2) require verification of all requested transfers in the manner we deem appropriate before making the transfer (which may include written verification by you).
You agree that our records will be final and conclusive as to all questions concerning whether or not your PIN or password was used in connection with a particular transaction.

If any unauthorized use of your PIN or password occurs you agree to (1) cooperate with us and appropriate law enforcement authorities in identifying and prosecuting the perpetrator; and (2) provide reasonable assistance requested by us in recovering any unauthorized transfer of funds.

Notify us immediately if you believe your PIN or password has been lost or stolen. Telephoning is the best way to keep your possible losses down. You could lose all of the money in your account (plus your maximum line of credit). If you tell us within two (2) business days you can lose no more than $50.00. If you do NOT tell us within two (2) business days after you learn of the loss or theft of your PIN or password, and we can prove we could have stopped someone from using your PIN or password without your permission if you had told us, you could lose as much as $500.00. Also, if your statement shows transfers that you did not make, tell us at once. If you do not tell us within sixty (60) days after the statement was mailed to you, you may not get back any funds you lost after the 60 days if we can prove that we could have prevented someone from taking the funds if you had told us in time. If you believe your PIN or password has been lost or stolen or that someone has transferred or may transfer money from your account without your permission, call (319) 334-7035 or 1-888-384-7780 during normal business hours listed above. **WE CANNOT ACCEPT NOTIFICATION OF LOST OR STOLEN PINS OR PASSWORDS OR UNAUTHORIZED TRANSFERS VIA E-MAIL.**

10. Errors and Questions

In case of errors or questions about your electronic transfers call us at (319) 334-7035 or write us at:

Security State Bank
231 1st St. E P.O.Box 511
Independence, IA 50644-0511

Notify us immediately if you think your statement or receipt is wrong or if you need more information about a transaction listed on the statement or receipt. We must hear from you no later than 60 days after we sent the FIRST statement on which the problem or error first appeared.

(1) Tell us your name and account number.
(2) Describe the error or the transfer you are unsure about, and explain as clearly as you can why you believe it is an error or why you need more information.
(3) Tell us the dollar amount of the suspected error.

If you tell us orally, we may require that you send us your complaint or question in writing within 10 business days.

We will determine whether an error occurred within 10 business days (20 business days for new accounts) after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days (90 days for new accounts or point-of-sale or foreign-initiated transfers) to investigate your complaint or question. If we decide to do this, we will credit your account within 10 business days (20 business days for new accounts) for the amount you think is in error, so that you will have use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within 10 business days, we may not credit your account for 30 days after the first deposit is made, if you are a new customer.

We will tell you the results within three business days after completing our investigation. If we decide that there was no error, we will send you a written explanation.

You may ask for copies of the documents that we used in our investigation.

11. Disclosure of Account Information to Third Parties

We may disclose information to third parties about your account or the transactions you make:

a) where it is necessary for completing transactions or resolving errors involving the Services; or
b) in order to verify the existence and condition of your account for a third party, such as a credit bureau or a merchant; or

c) in order to comply with government agency rules, court orders, or other applicable law; or
d) to our employees, service providers, auditors, collection agents, affiliated companies, or attorneys in the course of their duties and to the extent allowed by law; or  
e) if you give us permission.

12. Authorization to Obtain Information.  
You agree that we may obtain and review your credit report from a credit bureau or similar entity.  You also agree that we may obtain information regarding your Payee Accounts in order to facilitate proper handling and crediting of your payments.

13. Termination  
If you want to terminate your access to the Services, call us at (319) 334-7035 or toll free at (888) 384-7780. After receipt of your call, we will send a written termination authorization for your signature and return to us.  In the case where a fee is being charged in order to avoid imposition of the next monthly fee, we must receive your written authorization to terminate 3 (three) days before your service charge is scheduled to assess.  
**Recurring transfers will not necessarily be discontinued because you terminate access to the services.**  
We reserve the right to terminate the Services, in whole or in part, at any time with or without cause and without prior written notice.  In that event, or in the event that you give us a termination notice, we may (but are not obligated to) immediately discontinue making previously authorized transfers, including recurring transfers and other transfers that were previously authorized but not yet made.  We also reserve the right to temporarily suspend the Services in situations deemed appropriate by us, in our sole and absolute discretion, including when we believe a breach of system security has occurred or is being attempted.  We may consider repeated incorrect attempts to enter your PIN or password as an indication of an attempted security breach.  Termination of the Services does not affect your obligations under this Agreement with respect to occurrences before termination.

14. Limitation of Liability  
Except as otherwise provided in this Agreement or by law, we are not responsible for any loss, injury, or damage, whether direct, indirect, special, or consequential, caused by the Service or the use thereof or arising in any way out of the installation, operation, or maintenance of your PC equipment.

15. Waivers  
No waiver of the terms of this Agreement will be effective, unless in writing and signed by an officer of this bank.

16. Assignment  
You may not transfer or assign your rights or duties under this Agreement.

17. Governing Law  
The laws of the State of Iowa shall govern this Agreement and all transactions hereunder.  Customer acknowledges that he/she has reviewed this Customer Agreement, understands the terms and conditions set forth herein, and agrees to be bound hereby.

18. Indemnification  
Customer, in consideration of being allowed access to the Services, agrees to indemnify and hold the Bank harmless for any losses or damages to the Bank resulting from the use of the Services, to the extent allowed by applicable law.

19. Security Procedures  
By accessing the Services, you hereby acknowledge that you will be entering a protected web site owned by the Bank, which may be used only for authorized purposes.  The Bank may monitor and audit usage of the System, and all persons are hereby notified that use of the Services constitutes consent to such monitoring and auditing.  Unauthorized attempts to up-load information and/or change information on these web sites are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986.
INTERNET BANKING ENROLLMENT FORM

I agree to all of the terms and conditions of Security State Bank’s Internet Banking Agreement and Disclosure and would like to access my account information online at www.ssbindee.com. (Please place a check and sign below.)

Signature

Print Full Name

Address

Account Number

Social Security Number

Email Address

Phone Number

Please send this enrollment form to:
Security State Bank
PO Box 511
Independence, IA 50644

For Institution Use Only:

Date Taken: ____________  By: ____________
Date Approved: ____________  By: ____________
Login Name Assigned: ________________
PW Assigned: ________________
Data Entry Date: ____________  By: ____________