**SECURITY STATE BANK**
**"SECURITY STATEMENT"**

SECURITY STATE BANK is pleased to offer our online banking service. Delivering this service 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 communications 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 on the online banking system with regard to security. There are several levels of security within our security framework. User Level deals with cryptography and Secure Sockets 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 online banking service, 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 such as Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome. 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 which 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 browser and our server, you then provide a valid Username and Password to gain access to the services. This information is encrypted, logged by the server forming another 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 Username and Password from others. You must follow the Password parameters we specify at the time you sign up for an Online Banking account. We require you to change your password every 3 months. 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 Online banking transactions using host data. In addition, communication time-outs 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 banking system also have a responsibility for the security of their information and should always follow the recommendations listed below:

- Utilize the latest 128 bit encryption version of browsers such as Microsoft Internet Explorer, Mozilla Firefox, or Google Chrome. The online banking system is best viewed and is most secure when you use one of these three browsers, as they are certified for use at our site.
- Your Password must be kept confidential. You must follow our specific parameters for a Password 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 unattended while logged on to the online banking system. Others may approach your computer and gain access to your account information if you walk away.
- Click Log out 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.
- Keep your computer free of viruses. Use virus protection software to routinely check for a virus on your computer. Never allow a virus to remain on your computer while accessing the online banking system.
- Report all crimes to law enforcement officials immediately.

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