Security Policy
dtd. 1/1/16

GNB Bank is pleased to offer online banking and bill payment services. Delivering these online services requires a solid security framework that protects GNB Bank and our customers from outside intrusion. In order to provide the most effective security and service, GNB Bank has evaluated many products and vendors based on the vendors' security, reliability, and functionality. The service provider we have chosen performs continuous monitoring and auditing of its systems and the transactions that flow through those systems. We are committed to working with our service bureau and communications providers to provide the safest operating environment possible.

The information below summarizes our security framework, though it is not a comprehensive list of all the measures put into place to protect your financial information. GNB Bank would also like to emphasize that you have some responsibility in protecting your financial information. At the end of this page you will find some recommendations to use that will help protect your financial information. While nothing guarantees security success, these measures and best practices go a long way in protecting GNB Bank and more importantly, you our customer.

Security Framework

There are several layers of security in place to create a more robust and responsive framework to protect your data. Server controls, transmission controls, and access & monitoring controls all play important parts in the framework. Each serves a purpose in protecting your data and when used together are better at protecting your data than each on its own.

Server Controls

Accessing GNB's online services is very similar to making a phone call. Your computer finds our website using the website's listed number and starts communicating with our servers on the other end. To secure the servers our provider implements the latest technologies to protect unauthorized access. Server updates and maintenance as well as physical access to the servers are all tightly controlled. The network is designed so that multiple layers of monitoring and filtering technology are in place between your computer and the server where your data resides. Firewalls, antivirus, and intrusion detection and prevention technologies are in place to make certain the servers are further protected from malicious attacks.

Transmission Controls

Transmission controls focus on securing the connection between your computer and our servers. If the connection was not secure, any one could potentially look at the information traveling between your computer and our electronic services. Our provider uses SSL/TLS cryptographic technologies that encrypt the transmission and provide validation that you are connecting to GNB's services. Our servers will reject any transaction information that is not received securely. When you have completed your session, the server will terminate the transmission so that someone cannot access your information without providing the correct authentication information. Other transmission controls prevent a wide variety of known malicious attacks to circumvent the SSL/TLS technologies.

Authentication and Monitoring Controls

The first step in the authentication process is to provide a usercode and password. These two pieces of information are unique to each user and serve to limit access to only that user's accounts. Usernames and

passwords should not be shared. Additional authentication information may be required depending on the capabilities available to a user within our system.

The system also monitors and retains anonymous information from your previous site visits. It uses this information to create an electronic fingerprint that is unique to you. If a connection is made using your username and password but does not match your electronic fingerprint, the system will require the person creating the connection to answer security questions. The questions and their answers should be known only to you. If the questions are answered incorrectly, the connection is refused.

Once you have successfully authenticated with the system, you are authorized to conduct home banking and bill payment transactions. All transactions that are processed within the system are monitored to ensure they are correct, timely, and legitimate.

What you can do to help

While our service provider continues to evaluate and implement the latest improvements in Internet security technology, you also have a responsibility for the security of your information and should always follow the recommendations listed below:

• Continually update and patch your computer and web browser as patches and updates become available.

• Never give out your account number, usernames, passwords, or answers to security questions. It is also recommended you do not write any of this information down. Try to pick security answers that are not easily guessed or obtained through social media. Questions like 'Mother's Maiden Name' or 'Hometown' are too easy to find online.

• Avoid connecting to public wireless network connections or using public computers to access your online services.

• Never leave your computer unattended while logged on to the online banking system. Also be aware of your surroundings and make sure no one is watching you type in your information.

• Click Log Off when you are finished using the system to properly end your session.

• Close your browser when you are finished, so that others cannot view any account information displayed on your computer.

• Use virus protection software. Keep the software up to date and scan for viruses regularly.

• Report all crimes to law enforcement officials immediately.

Please enjoy the convenience and safety of these online services. GNB prides itself in providing banking for a lifetime and will continue to bring those services that best fit our customers' needs.