Security Policy

Security Policy

We have taken significant measures to help ensure that your personal information remains confidential and secure within our data center. We use state-of-the-art network, data, and physical security practices to protect your data to the best of our ability.

Security Overview

We make every effort to ensure that your information is protected. We use current industry standard encryption and employ SSL encryption to insure that information passed between our site and your browser is secure.

Physical Security

All servers involved in gathering, storing, and providing the data to you are operated in a secure data center that has restricted access to authorized personnel only. Our data center is monitored 24 hours per day and only certified employees are permitted on premises. A record is kept of all personnel who have entered the secure data center.

Access to servers requires multiple levels of authentication. Sensitive data including your access credentials and account numbers are always stored in encrypted format at all times.
Our employees are made aware of our security policies, procedures and practices and confirm, on a yearly basis, that they have carefully reviewed and abide by it.

Firewalls

All external access to our internal network must go through firewalls. Additional firewalls are used to secure access to the application and database from internal sites within our institution. Our firewalls are regularly tested to insure that they are able to protect your personal information from unauthorized external and internal access.

Intrusion Detection

We use an Intrusion detection system to continuously monitor unauthorized attempts to access our site.

Secure communications between systems

We use SSL to securely encrypt and protect all communications between your browser and our web servers.

Internal Business Practices

We store all access credentials in an encrypted format on a secure data warehouse. Only a few authorized individuals have access to the data warehouse and no one except you can ever see the access credentials that you have provided.

We require all users to provide ids and passwords using alpha/numeric characters to prevent easy guessing of passwords by unauthorized individuals. If you ever lose or forget your password, we allow only you to reset it by first accessing a token sent only to your email address on record and then providing the answer to your secret question.

Questions

If you have any questions about our security procedures you can contact us via email at info@nextierbank.com or by phone at 1-800-262-1088. Be sure to provide your name, contact information, and clearly state the question. We will make every effort to answer your questions.