ENHANCED BUSINESS INTERNET BANKING
PROTECTING YOUR INFORMATION

Thank you for using Enhanced Business Internet Banking (EBIB) at Renasant Bank. EBIB enables you to conduct many business banking functions conveniently from wherever you or your users happen to be.

As with any internet-based service you use to conduct financial transactions or other private matters, we urge you to be cautious, as there are a growing number of security threats that could expose your account information or transaction capabilities to outsiders, some of whom have malicious intent.

Your user agreement for EBIB and related services lays out certain Security Procedures which are based on good, common sense measures you can take to protect your technology environment. Please be familiar with the security best practices listed below, and use them in your organization.

ESTABLISH PHYSICAL CONTROLS:

- Never walk away from the computer while logged in to EBIB.
- Shut down computers when they are not in use.
- If practical, use a dedicated computer and network for EBIB to avoid exposing it to malware from other internet activity.
- Do not log in to EBIB at a public computer or a computer that might be unsecured.

ESTABLISH PASSWORD CONTROLS:

- Memorize the password and do not share with anyone even if they identify themselves as an employee of the bank. The bank never needs to know your password.
- Choose a password that is not easy to guess.
- Use a minimum of eight characters with a combination of numeric and alphabetic characters.
- Do not use the names of family members or pets alone or followed by a number.
- Do not use words in a dictionary or common character sequences such as "12345678."
- Personal details such as a spouse's name, license plate, social security number, or birthday should not be used unless accompanied by additional unrelated characters.
- Passwords should also not be any proper names, geographical locations, common acronyms, or slang.
- Choose a password that contains at least one lower case and one upper case alphabetic character and use non-alphabetic characters where feasible, such as a numeral (0-9) or punctuation character.
- Change Passwords often, at least every six months.

MAINTAIN UP-TO-DATE SECURITY OF COMPUTER EQUIPMENT:

- Employ and keep up-to-date professionally installed and maintained virus and spyware protection for all equipment.
- If a computer becomes infected with a virus:
  - Immediately notify the bank and cease using the computer.
  - Have all equipement professionally examined to ensure that any virus threat has been eliminated.
  - Change all passwords immediately after the virus has been removed.
- Have a professional remove all data from the hard drive of retired computers.
- Ensure that any wireless network utilized for EBIB is secure.
- Establish a firewall in order to monitor incoming and outgoing traffic either to or from your computer to ensure unauthorized access is denied no matter from what point it is initiated.

ESTABLISH ADMINISTRATOR AND USER CONTROLS:

- Choose your administrator(s) carefully based on their levels of authority in your organization.
- Since an administrator can establish and modify the authority of other EBIB users, have each Administrator set up a separate user password to limit the number of occasions in which the administrator sign-on is used.
- Use the "multitude" alerts that may be established through EBIB such as alerts for:
  - Password changes
  - Changes in a user's role (for example, when someone is given the approval or administrative role)
  - Changes in email addresses
  - Changes in a wire template
- Review account information frequently and promptly report any questionable activity to the bank.
- Control to whom wire transfers may be sent by using locked down wire templates, which are available through EBIB.
- Set wire transfer transaction limits or daily limits as low as practical.
- Limit the ability to send international wires.
- Establish multiple approval requirements for wire transfers and ACH.
- Limit the authority of users to those functions that are essential to their job duties.
- Confirm the last sign on date on the EBIB welcome page and make sure it is inline with your expectations.
- Do not use account numbers when providing nicknames for your Designated Accounts.
- Register computers so the challenge questions will not be asked on every login.