FSSB
FIRST SECURITY STATE BANK

Made in Texas, Stayed in Texas

Member FDIC

Business Best Practices and Fraud Prevention Checklist

At First Security State Bank, we want to partner with you to protect your company from fraudulent activity. Developing a layered approach of education, technology, business rules and procedures is the best way for you to achieve that protection. While not all inclusive, this checklist is a great way to get started.

User Security

- Restrict entitlements to all systems and review these settings periodically.
- Require Dual Control for all steps of cash handling.
- Require Dual Control for all payment initiation and payment file handling.
- Require Dual Control to set up profiles for payment initiation.
- Require documentation for all internal requests for payments.
- Document all procedures, and train for them.
- Audit User activities regularly.
- Educate your employees about email, text and other scams.
- Implement good hiring practices, include background checks.
- Lead a strong ethics policy by example.

Separation of Duties

- Employees who write checks or initiate electronic payments do not reconcile accounts.
- Employees who initiate electronic payments do not approve them.
- Employees who maintain profiles for electronic payment initiation do not initiate or approve payments.
- Employees opening the mail do not prepare or make deposits.

Computer Security

- Require use of a segregated computer for banking activities; allow no internet surfing or email use.
- Protect your network using a properly configured firewall.
- Keep your industry standard Anti-Virus and Malware software up-to-date.
- Apply latest security updates from operating system vendor, e.g. Microsoft.
- Restrict access to the computer’s administrative privileges.
- Disable CD/DVD/USB access if not needed.
- Implement procedures to protect laptops when away from the office and before reconnecting them to the network.
- Establish unique log-in and passwords for all systems and require periodic change.
- Impose strong password rules. Use special characters, and no words or names.
- When using online banking systems always log in through your corporate infrastructure, not outside the network, at home or on a public computer.
- Close Pop-Up-Windows by clicking on the X, never click inside the window.
- Never send sensitive information via unsecured email.
- Implement procedures for when an employee suspects infection.
- Delete on-line users when employee terminates employment.