Self-Audit Questionnaire for Cash Managers

Citizens State Bank is concerned about your privacy and security regarding your confidential financial information. This worksheet is being provided as a tool to evaluate the risks and security issues related to certain activities or behavior in your daily life. All the answers should be "Yes" and any "No" answers indicate that you may be at greater risk for an attempted or successful fraud attack. If you have any questions about the security of your accounts at the bank, please contact any of our Customer Service Representatives at 979-885-3571 Ext 256

Yes	No	
□	□	Your computers have anti-virus, spyware and malware protection software that is updated regularly with scheduled scans performed at least on a weekly basis. Your operating systems and web-browsers are also updated with the latest patches and you have activated your personal firewall rules. [If No, check with your IT support for options.]
□	□	You implement Internet access usage rules for your employees. [If No, check with your IT Support for options.]
□	□	When using email, you never include confidential information about your financial accounts or other information that could provide access to your banking accounts. This would include your account numbers, bank name, login IDs, passwords and other confidential information. You do not click on links in emails unless you are sure they are from a legitimate or trusted source. [If No, stop including this information – email is insecure and can be intercepted.]
□	□	When discarding statements or other documents that contain confidential information, you always shred the document or destroy the information that is confidential. This information typically is the account number, name, address, bank or other identifying data that could be used to allow unauthorized access to your account. [If No, start shredding or masking data – dumpster diving is a big ID theft threat.]
□	□	You reconcile your monthly statements and report any discrepancy or suspicious activity immediately. You receive e-Statements to reduce the risk of mail theft. [If No, review transactions daily and balance statements monthly; request e-Statements.]
□	□	You have alerts set up on your deposit account when your balance changes significantly. [If No, contact your institution to set up balance alerts on your accounts.]
□	□	Your Supervisor password has never been shared with anyone in the office. [If No, change your password today]
□	□	You implement dual control decisions for processing Wires and ACH files. [If No, contact your financial institution for dual control options]
□	□	You restrict access to use of the USB port and you know what information is being saved. [If No, check with your IT support for options.]
□	□	Your computer is located in a secure area in your office. [If No, consider as more secure location]
□	□	Access to the cash management pc is only available during normal business hours. [If No, consider options to implement new procedures for office personnel.]
□	□	You encourage employees to lock their computer when leaving their desk. [If No, check with your IT support for procedures.]
□	□	You have security cameras in your office. [If No, consider installing security equipment.]
□	□	Customer account information is not viewable on your desk. If No, implement clean desk policy to secure customer information.]

Additional Security measures you have implemented that are not listed:

Answering "Yes" to all these questions will not guarantee that you will not be a victim of fraud, but it should lower your exposure to many of the common threats and risks in the marketplace.