Annual Self-Assessment

OsgoodBank

ACH/RDC & General Security - To ensure you have controls in place to protect your organization, please use this assessment to assist with your yearly fraud prevention procedures review. – *review all that applies*

ACH

❒ Do not share logins – each user should have their own login, PIN, and soft token.
❒ Apply online banking alerts to monitor ACH origination activity
❒ Preauthorize high dollar value amounts before items are sent
❒ Obtain written authorization for all ACH transactions – debits and credits.
❒ Validate all requests to change payments or payment instructions from vendors, customers, and company personnel (including senior officials); don't simply reply or respond to email. Use a secondary method, text or call back to a known number is best.
❒ Ensure users are familiar with system screens and functionality, so suspicious screens are easier to spot and reported quickly to the bank

RDC

❒ Secure scanned deposit items in a locked area
❒ Reconcile deposits weekly or monthly to ensure deposits are posted
❒ Destroy deposited items every 60 days (shredding the items is the most preferred method)
❒ Ensure users are familiar with system screens and functionality, so suspicious screens are easier to spot and reported quickly to the bank

General Security – Online & Internal

❒ Train personnel on fraud prevention best practices – we recommend KnowBe4
❒ Use multi-factor authentication (MFA) whenever possible
❒ Review employee access privileges and limit administrative rights on company computers and login accounts; only provide employees with access to financial data if there is a business need.
❒ Practice clean desk policy – don't leave out information that anyone could access.
❒ Lock your screen when not at your desk.
❒ Protect login information, specifically passwords.
  ○ Use password protection applications such as LastPass.
  ○ Don't share them with anyone – even IT support. If you can't remember your password, it's best to reset it.
❒ Review your Cyber Security Insurance Policy.
❒ Have a plan and responses prepared for when there is an incident
  ○ Communication to employees should only be what they need to know to prevent panic or misinformation, possibly making a bad situation worse.
  ○ Be careful what you share on social media about your business and/or any incidents that occur – it could give the bad guys leverage to exploit your systems.
❒ Keep workstations current with security updates.
❒ Apply operating system updates promptly; beware of download requests from pop-ups or advertisement.
❒ Prevent malware infection.
  ○ Use caution when downloading applications or documents, installing software and opening email attachments.
  ○ Limit internet use on computers used for online banking activities.
  ○ Block bad websites
❒ Limit personal email on company computers.
❒ Remove USB/external media access on company computers
❒ Email security
  ○ banner alert for external emails, reminder to be extra careful when opening or clicking on any links
  ○ Set up email backups
  ○ Reduce the amount of emails stored in inboxes
  ○ Avoid using email to send confidential information; truncate all but last four digits of account/social security numbers.
  ○ Report suspicious emails to your IT team.
❒ Review your accounts online, at any time at https://www.osgoodbank.com
❒ Monitor account balances and activity daily.
  ○ Report any suspicious activity immediately to your bank.
  ○ Review transactions before they leave the company.
  ○ Review and update bank signature cards routinely.