DARTBANK

Commercial Online Banking Risk Assessment

1.) Management understands responsibilities and liabilities per the financial institutions account agreement

☐ Yes

☐ No

2.) Employees are educated on use of application(s), IT security standards and best practices, common fraud schemes and procedures for contacting the FI in case of suspected security incident

☐ Yes

☐ No

3.) Employees are on the alert for rogue emails

☐ Yes

☐ No

4.) Employees have segregation of duties, a separate approval process and dual control utilizing two separate PCs for online transactions

☐ Yes

☐ No

5.) Employees close out the browser session of their banking session as soon as they are finished

☐ Yes

☐ No

6.) Strong passwords are in use with 8-10 characters that use combination of upper and lower case letters along with numbers and special characters

☐ Yes

☐ No

7.) The default password on all network devices has been changed

☐ Yes

☐ No

8.) Online banking passwords are not shared with anyone

☐ Yes

☐ No

9.) The same passwords are not used to access different systems

☐ Yes

☐ No

10.) Passwords are changed every 60-90 days

☐ Yes

☐ No

11.) Accounts are monitored and reconciled daily

☐ Yes

☐ No

12.) Public computers are not used to conduct online banking transactions

☐ Yes

☐ No

13.) Each online banking session is confirmed to begin with https indicating a secure browser setting

☐ Yes

☐ No

14.) The internet browser's cache is cleared before starting an online banking session

☐ Yes

☐ No

15.) The PC used for online banking is not used to surf the web or email

☐ Yes

☐ No

16.) Real-time anti-virus and anti-spyware, desktop firewall, malware detection and removal software w/automatic updates and scheduled scans are installed

☐ Yes

☐ No

17.) Installed anti-virus, anti-spyware and malware software is from a professional source. Free software is not robust enough

☐ Yes

☐ No

18.) Implement a dedicated firewall and router that are actively managed

☐ Yes

☐ No

19.) Options offered by the FI to detect or prevent out-of-pattern activity have been discussed

☐ Yes

☐ No

20.) Changes in the online banking PC's performance are investigated that signify a machine has been compromised.

☐ Yes

☐ No

21.) A vulnerability assessment from a security expert has been considered or executed to determine any potential security issues

☐ Yes

☐ No

22.) Internet browsers are set to block all pop ups

☐ Yes

☐ No

23.) User rights for online banking computers are limited. For example, administrative rights are restricted so that not every user can download software onto the computer

☐ Yes

☐ No

24.) Security patches are up to date for operating system and other software applications

☐ Yes

☐ No

25.) Computers are never unattended while logged into an online banking session

☐ Yes

☐ No

26.) The online banking computer is shut down and/or disconnected from the internet while not in use for significant time periods.

☐ Yes

☐ No

27.) Remembrance features are avoided such as writing down user name and password

☐ Yes

☐ No

Once you have completes the assessment online please save/scan and attach the completed document, then email to **banking@dartbank.com**