Charles G. Cooper
Commissioner

TEXAS DEPARTMENT OF BANKING

2601 North Lamar Blvd., Austin, Texas 78705
512-475-1300 /877-276-5554
www.dob.texas.gov

Media Contact:
media@dob.texas.gov

INDUSTRY NOTICE 2020-05
Date: March 30, 2020

Business Continuity Planning Considerations – COVID-19

To assist in the review of your operational preparedness in response to the issues presented by COVID-19, the following has been developed in conjunction with the Independent Bankers Association of Texas and the Texas Bankers Association. Each community and therefore, each bank may be experiencing the COVID-19 emergency in unique ways, so this set of recommendations does not constitute required action. This guide contains a list of important areas to consider as you maintain essential business operations during the pandemic.

It is important to view bank business continuity from the enterprise perspective in order to ensure that interdependent operations and the personnel to carry them out are considered.

As you work through the guide, your situation may lead you to other factors that should be evaluated.

Have you identified your critical systems and processes?

Critical systems and processes to consider:

- Core Processing System
- ATM Processing and Replenishment
- ATM / POS Limits (Can these be adjusted remotely?)
- Online Banking System
- Debit/Credit Card Processing
- Cash Letter/Returns
- ACH Processing/Returns
- Wire Processing

Do you have remote access for your critical systems and processes?

Items to consider:

- Virtual Private Network Access (VPN) (Is the capacity adequate?)
- Internet access (Web-based software/applications)
- Telephone system
- Secure remote desktop/laptop
- Remote security:
    - Are there security controls that need to be adjusted for expanded remote operations?
    - Use of multi-factor authentication to minimize risks of remote operations?
    - Have you considered both off-site and off-line backup strategies?
    - Network segmentation policy – Can you control the access and movement of your data with employees working remotely?

- Data backup policy – Have you eliminated unnecessary connections into or out of your backup storage site?

Have you tested remote access of each critical system and process?

Items to consider:

- Multiple users accessing the system at one time
- Remote location Internet capabilities (bandwidth, security, etc.)
- Alternate remote location availability (Internet bandwidth, security, etc.)
- Ability to connect to critical systems and processes from new remote IP addresses and alternative devices

Do you have employees who are trained and cross-trained for all your critical systems and processes?

Items to consider:

- Primary and backup employees who work in the same area could become sick simultaneously.
- Authority and authentication requirements and devices should be current and accessible.
- Written processes and procedures should be current and accessible.
- Remote access devices should have all necessary software and applications installed and updated.
- Training should be current.

Are you prepared to take other staff actions to maintain business continuity?

Items to consider:

- Implementation of staggered shifts (e.g. Employees A and B X hrs. or days; Employees C and D work the opposite).
- Community banks with a smaller staff might explore potential mutual aid agreements to **supplement possible staffing needs,** and other arrangements in order to deliver customer services to the community.
- Adherence to local ordinances regarding social distancing and hygiene – for both employees and customers.
- Enforcement of regular cleaning of surfaces on a rigid schedule throughout the day – particularly at any shift changes.
- Utilization of staff logs to screen for potential employee health (Template).
- Distribution of employee credentials should local authorities close or restrict access by Department of Homeland Security (DHS)/U.S. Treasury designated essential bank personnel (Note: U.S. Treasury recommends the following for credentialing: The combination of the employee's bank ID or letter from bank supervisor + DHS Guidance document + U.S. Treasury Secretary Mnuchin's statement).

Other Important Considerations:

- What other business processes must function to perform these critical processes?
- What is the minimum staff required to be able to serve customers during a business interruption?
- What vendor services do you need to be able to perform these critical processes?
- What systems/equipment do you need to perform these critical processes?
- What software do you need to perform these critical processes?
- What supplies do you need to perform these processes?
- What instructions/manuals do you need to perform these processes?
- Are there alternate ways to perform these critical processes in order to serve your customers?
- Third-party service providers must adhere to the same security policies and protocols for the organization.

Resources:

Centers for Disease Control and Prevention (CDC) – Businesses and Employers
U.S. Department of Homeland Security – Business Continuity Planning
U.S. Department of Homeland Security – CISA Essential Workforce Guidance
U.S. Department of the Treasury – Statement on Financial Services Essential Workforce