BUSINESS CONTINUITY POLICY

01.28.2020 | Responsible Party: Director of IT

Table of Contents

Overview

The Business Continuity Policy enables and charges Community First Bank to prepare for, respond to, and recover from disruptions to the delivery of services and business processes by implementing procedures to manage a disaster or disruption of service. Procedures include identifying business processes, assessing the impact disruptions will have on business processes, and preparing for and recovering from disruptions.

Purpose

The purpose of the Business Continuity Policy is to establish measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures. The Business Continuity Policy is also intended to retain the trust and confidence of customers, limit the impact of service disruptions, and maintain continuity of business.

Responsibilities

As with all emergency preparedness planning processes, business continuity management is not simply an information technology issue; a business interruption poses a significant risk to the entire business. As such, business continuity management activities shall involve senior management from all business areas, including administrative, human resources, IT support functions, and key business services

Board of Directors

The Board of Directors is responsible for the oversight and approval of business continuity efforts that support the continued delivery of services. The Board of Directors is also responsible for the review of testing results to ensure that sufficient resources are invested to implement and test the approved controls. This policy shall be reviewed and approved by the Board of Directors at least annually.

Senior Management

Senior Management is responsible for developing the Business Continuity Management Plan and its associated procedures and additional resources. Additionally, Senior Management is responsible for evaluating the continued effectiveness and relevance of the plan.

Information Security Officer

The Information Security Officer is responsible for consistent and up-to-date training of business continuity procedures and ensuring that all employees understand their roles and responsibilities in the event of a disaster or other disruptive event.

Business Continuity Management Team

The Business Continuity Management Team is responsible for executing recovery procedures including leading and managing resources, prioritizing recovery efforts, and communicating with the public.

Employees

It is the responsibilities of all employees to be aware of the Business Continuity Policy, as well as to support and comply with the controls defined within.

Applicable Third Parties

Third parties supporting critical business functions shall be expected to prepare for disasters and other disruptive events by implementing comparable controls that support this policy regarding provided services and equipment.

Risk Management

The potential impact of a disaster or other disruptive events on the delivery of critical business functions and services shall be incorporated into ongoing risk management processes. Risk management shall evaluate the Business Impact Analysis (BIA) assumptions using various threat scenarios including the impact and probability of a disaster or disruption to business operations, as well as determine mitigating controls. Potential business disruptions shall be prioritized based on the risk posed to critical business operations.

The Business Continuity Management Plan shall be revised, if needed, to reflect the conclusions of risk management results. Additionally, the business continuity management efforts of applicable third parties shall be evaluated and monitored to ensure continued support and service for contracted items.

Business Continuity Management

Business Impact Analysis

The first step in managing business continuity efforts is to perform a Business Impact Analysis. The Business Impact Analysis shall identify business processes, classify potential

impacts of disruptive events on business processes, and determine recovery-time objectives. To ensure recovery efforts are properly allocated, Community First Bank shall conduct a Business Impact Analysis that identifies business processes and includes an analysis of estimated recovery time objective, recovery point for maximum acceptable level of data loss, maximum allowable downtime, and resource requirements for each business processes.

Business Continuity Management Plan

Effective business continuity planning establishes the basis for the continuity and recovery of business processes when operations have been disrupted. Community First Bank shall implement a comprehensive Business Continuity Management Plan to prepare for and respond to disruptions, including considerations for disaster recovery and pandemic events.

The Business Continuity Management Plan is a comprehensive, written plan used to manage the continuity and recovery of business processes in the event of a disruption. To ensure minimal disruptions to services and business processes, Community First Bank shall document and maintain a Business Continuity Management Plan based on the results of the Business Impact Analysis. The plan shall include a comprehensive framework of facilities, systems, and procedures to ensure Community First Bank is able to maintain critical operations following a disaster or other disruptive events.

Testing

As systems, networks, services, and third parties change, the Business Continuity Management Plan shall be adjusted to incorporate new information and risk mitigation approaches. To accomplish this, a testing process shall be developed to ensure policies, standards, and procedures include up-to-date, relevant information provided by ongoing review and updates to the Business Continuity Management Plan. Business continuity practices and capabilities shall be tested annually to ensure they remain effective and will allow critical operations to continue. Testing shall provide a high degree of assurance that critical business processes, including supporting infrastructure, systems, and applications, can be quickly restored following a disaster or disruption of services.