Very Safe Bank Contingency Plan Policy

Geldi Omeri
ITMS-588

Overview

A contingency plan is a necessary step in preparing Very Safe Bank for a variety of disasters. The contingency plan is not limited to tackling only natural disasters such as tornados and blizzards but also include any potential black-outs or brown-outs and any other event that could delay business operations and services. The contingency plan aims to identify the critical business systems, operations, and assets and enable an effective recovery process if normal business operations are affected by a disaster. Managements support and attention during contingency planning for disasters is required for this policy to be successful.

Purpose

The contingency policy provides a path forward in recovering business systems, operations, and assets during and after a disaster. The policy establishes the minimum requirements necessary for Very Safe Bank to develop and implement a successful contingency plan.

Scope

This policy sets the expectation for a contingency plan to be established for the Very Safe Bank Chicago Headquarters location. This policy does not detail the specifics of the contingency plan.

Policy Statements

The focus of a contingency plan is to protect confidentiality, integrity, and availability of critical VSB systems, operations, and assets during an emergency or disaster. The responsibility for contingency planning and funding falls on IT management and senior leadership. The responsibility to develop and maintain the plan falls on the policy champion and/or the contingency plan coordinator.

The plan will be periodically tested on an annual basis to identify and analyze unforeseen problems and areas for improvement. The plan will be updated and revised in response to

these tests and to changes in the organization and technology. Revisions will be documented as they are incorporated.

The following requirements must be met:

- Criticality/Priority List: Identify and prioritize business critical systems, operations, and assets. Detail relevant information regarding each item including factors such as confidentiality.
- Natural Disaster Contingency Plan: Determine how disasters such as floods, fires, and tornados would affect business functions. What actions would be taken? What resources are needed to combat each situation?
- Data Backup Plan: Identify and detail critical systems, data assets, and where they are stored. Develop backup strategy for systems and data assets. Develop process for creation, maintenance, and retrieval of backups. Set requirements for periodically testing the integrity and availability of backups.
- Succession Plan: Determine and detail the flow of responsibility for staff duties in the absence of normal staff.
- Equipment Replacement Plan: Document a list of business-critical equipment. Detail factors such as where to purchase from, who uses it, and serial number/part number if necessary.
- Public Relations Management: Establish person in charge of providing information to media regarding the incident/disaster.
- Emergency Mode Plan: Develop emergency procedures in the case following an incident that jeopardizes the business and/or human life. Develop alternative site fallbacks for essential business operations. Establish plan for exiting emergency mode and returning to normal business operations. Develop training program to train staff on emergency mode operations and procedures.

Related Policies

None

Definitions and Terms

- Disaster/Incident – A sudden event, either accidental or a natural, that causes significant downtime or damage to business operations, systems, or assets.
- Business Critical – Necessary for the core functions of the business to continue running.

Revision History

Date	Responsible	Comments