AFTER ACTION REPORT

INTRODUCTION

A Tabletop Exercise was conducted for the TowerView Health Information System Contingency Plan (CP) on 9-5-2016.

The participants and their assigned roles are listed below.

Name	Organization	Roles/Responsibility	Phone Number
Hareesh Ganesan	TVH	Exercise Facilitator	301-943-6475
Rahul Jain	TVH	CP Coordinator	715-771-9831
Emily Cerciello	TVH	Data gatherer	610-573-6809
Osuvaldo Ramos	TVH	Recovery Management Team Member/Technical Lead	817-914-8218

The CP tabletop exercise was conducted in accordance with the TowerView Health CP Exercise Plan, dated 9/1/2016.

The exercise plan was developed around the following scenario:

Over the past three months, rainfall has saturated the ground in Oregon, elevating water levels in rivers, creeks, and waterways. Rainfall has resulted in warnings of inconsistent power and connectivity in areas where the primary TVH datacenters are located if massive rainfall continues. The National Weather Service predicts that a major storm is projected make landfall within the next 2 days.

The exercise was developed to determine the following:

- Determine weaknesses in the contingency plan.
- Identify gaps in coordination/communication of plan or actions

The CP exercise evaluated the status of contingency planning for the system and provided a forum for identifying outdated contingency planning information and for providing updates as required.

Summary of Exercise Results

Significant results from the exercise were:

- Data recovery from cold storage occurred very quickly
- Our version control infrastructure is maintained in the cloud. In the event of a service disruption, we reverted to local repositories.
- We spent 1.5 hours setting up security groups and configuration for the servers that we would fail over to.
- Technical testing did not have any errors in recovery, though configuration was slower than expected.

The following recommendations are provided as a result of the exercise:

- We need to maintain a local backup of the full version control to ensure the correct code branches are available if the version control infrastructure is also compromised.

- We need to maintain a more robust infrastructure in the event that every region of our cloud hosting provider (AWS) is affected by a natural disaster, or more likely, a timed DDOS attack on their systems.
- A redundant security policy should be maintained in a different region to more quickly spin up and transfer production instances.
- The engineering team should explore containerizing the system to more easily launch into a different cloud hosting provider.

Approved By:

Signature

Date