**qwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmrtyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnmqwertyuiopasdfghjklzxcvbnm**

|  |
| --- |
| System Documentation & Improvement  Newtown Fire Dept.  9/27/2018  K.P.I. Shenesh Perera IDM |

Contents

[Introduction 2](#_Toc532314997)

[General guidelines 3](#_Toc532314998)

[Hardware design plan 4](#_Toc532314999)

[Hardware disaster recovery 5](#_Toc532315000)

[Software Design Plan 6](#_Toc532315001)

[Improvements 7](#_Toc532315002)

# Introduction

This document will contain steps and procedures to take during particular situations, it will not contain any particular networking guidelines. This documentation also contains improvements to the network.

# General guidelines

* Watch Officers are granted the task of initial recovery troubleshooting for the network. They will be treated as the administrators of the network and be granted with an individual user account to the server, but they will not have permissions to delete any files on the server.
* Civilian staff does not have permission to access the server room.
* Civilians must adhere to and obey all procedures declared by watch officers in the case of a network emergency.
* The watch that is under each watch officer will interact with the civilian staff if they require any information about a particular situation, they need not interact with the clients in the network.
* The Chief Fire Officer is the only administrator that has all permissions to operate the server on a medium-scale without altering any network software infrastructure.

# Hardware design plan

All switches that will be used must be level 3 manageable switches; they must be connected with RJ45 cables and be connected to a router, then through a firewall to the server.

1. The Control Center will be equipped with 3CX IP phones that will allow direct calls from public liaisons, police and any other foreign base that the fire department is responsible for.
2. The watch officer must always be equipped with a 3CX softphone at all times. This is so that the watch officer is instructed by the control center at all times.
3. The controllers must always have their softphone equipped and have an IP enabled hard phone by them at all times.
4. All systems in the control center must be networked and plugged into a 16 port level 3 switch. Only 3 will be used but in case the control center is expanded the switch doesn’t have to be replaced.
5. All switches and routers must be rack mounted and be fitted with patch panels and in turn plugged with keystones so that the ports aren’t damaged.
6. The civilian client systems must be networked through a 16 port level 3 switch, and connected to the router.
7. The civilian client systems must have a networked IP enabled printer to take any printouts.
8. To maintain 2 way communications between in the vehicles, a 3CX IP hardphone must be placed with additional speakers and a softphone stored inside each vehicle.
9. All vehicles must be fitted with GPS units, all monitoring must be done by the 3 controllers in the control center.
10. The control center will contain the rack mounts that will have all the network devices but under lock and key, the key must always be with the one of the administrators.

# Hardware disaster recovery

1. In the event of a natural disaster, the administrators must take a list of all damaged devices and replace them immediately per the service agreement with the fire department’s network device providers.
2. In the event of a security breach, the administrators of the network must immediately take necessary logs of the network that explain the breach, and then temporarily disable all access to the server till the breach has been mitigated. In such instances if the administrators cannot recover from the breach, the network administrator must be immediately called for.
3. In the event of bad connectivity or cable damages, administrators are forbidden to attempt anything. The network administrator must be contacted and be given this system documentation, per the documentation and these failsafe protocols, he is to analyze, log and then repair the issue.
4. In the event of the identification that a networking device is not functioning properly, Chief Watch Officer must contact a network technician from the provider and then ask them to verify the problem, log it and then proceed to repair it. If the problem is unfixable then the network administrator should either decide to replace unit itself or the device.

# Software Design Plan

1. All client systems must be installed with MalwareBytes Business version, and configured to scan once in every 3 days.
2. The server must be installed with Windows Server 2012, and the administrators are supposed to update it as soon as an update is available but a system restore point must be created and backed up.
3. The network administrator must use WireShark to sniff packets going in and out of the server to check if the networking is functioning as it is supposed once in every week.
4. All client systems must be installed with Windows 8 licensed versions and updated when updates are available.
5. The client systems must be restricted from surfing the internet unnecessarily, only department websites, services and related interfaces must be allowed to be searched.
6. If a client system is infected by any form of virus, then until the risk has been mitigated all notably infected client systems must be disconnected from the network.
7. Administrators must make regular backups of the content in the server, and store them in external storage devices stored under lock and key.
8. All sensitive soft information must be encrypted with AES 256-bit in CCM mode with randomly generated 8 alphanumeric character passwords.
9. The passwords of the client systems must be changed once in every month.
10. Server administrator passwords must be changed once in every 2 weeks.
11. Server administrators are only given permissions to **read and modify** files in the server, with the exception of Chief Watch Officers.
12. All client systems can only access the server to **read and download** files from the server.
13. All the fire department staff must be trained properly by the network administrator and his staff, whenever a new implementation is introduced to the network.

# Improvements

* The control center must be assigned as a separate VLAN.
* The civilian office must be assigned as a separate VLAN.
* A router must be installed to enable inter-VLAN communication between the above stated departments.
* A router with firewall and vpn technology must replace the additional firewall in the server room.
* Distribution of a mobile application that can only call the fire department in the case of an emergency.
* Control center staff must be increased in order to ensure maximum efficiency during work.
* All client users must be denied of plugging in any external media to the client systems.
* A hybrid topology of bus topology and star topology must be implemented, bus in the civilian office and star in the control center then directly connected to the router in the server room.
* A physical security expert must be hired to rigorously increase the physical security of the fire department in such a way that the network’s maximum security is ensured.
* Mitigation from local storage to cloud storage, that will store all information encrypted and hashed.
* A Metropolitan Area Network is designed in such a way that the fire department can directly communicate with the police and other emergency services.
* A Wireless Access Point must be introduced in the civilian office so that staff is encouraged to use their own devices to access the network instead of client systems.
* IPSec must be implemented when the newtown fire department communicates with external services like the police so that sensitive information is not sniffed.