

# PC Security/Backup Proposal

Susan and Gil Kleinwechter met with Mike Young from Computer CPR in Southlake. The purpose of the meeting was to determine if their services would be of use to St. Martin's. The initial meeting was used to review the computer and network configuration as well as the security and backup processes and procedures in place at St. Martin's. It was no surprise that we are sorely lacking in computer security and backups. Susan and Gil asked Mike to write up a proposal and return for another meeting. At the second meeting Mike proposed 4 objectives as well as providing a cost estimate (see attachments). After reviewing the four objectives Susan and Gil agreed that while doing all of them would be ideal, we recommend that #1, 3 and 4 be done at a minimum.

1. **Centralize data and user administration:** Install a new PC that would be a central file server and control PC access to the data. All data used at St. Martin's would be on this PC. It would have internal backup storage as well as perform regular backups to external storage as well as to a cloud account. This would protect St. Martin's information against multiple potential problems.
2. **Upgrade Wireless Network:** A nice to have, not needed right now.
3. **Virus protection:** Upgrade our existing virus software to be centrally managed and monitored.
4. **Replace Verizon FiOS Router:** Install a new router that would enhance the security of the network and help prevent data theft.

A summary of the estimated costs for #1, 3 and 4 are as follows:

One time:

Router:	\$1,200
Data Server	\$3,500
<u>Setup:</u>	<u>\$2,178</u>
<b>Total:</b>	<b>\$6,878</b>

Recurring Cost (Monthly):

Monthly Monitoring of Data Server:	\$159
<u>Antivirus + monitoring:</u>	<u>\$ 70</u>
<b>Total:</b>	<b>\$229</b>

What does this give us?

- **Security:** We would have centralized control over who has access to church and school computer. Groups of users can be defined and their access restricted as needed. The data would now be centralized and available to all with the proper access. Assuming that we paid for monitoring we could detect and isolate PCs that were infected. The network would be monitored and intrusions would either be prevented or detected.
- Backups. The data would be backed up both locally and in the cloud. If any of the data were to be compromised, deleted or destroyed the backs could be used to restore what was lost.

As we grow roles change and more people are becoming involved. We need to be able to manage our IT assets better than we have been doing. This proposal is inclusive of the church and school. I would recommend that if we proceed that the cost be allocated over both the church and school.