In this newsletter to the Pastors of the Diocese of Buffalo, the Internal Audit Department offers advice on how to reduce overall financial and administrative risk to your parish in regards to Computer Safeguards (this is in addition to Section 4 of the Diocese of Buffalo Business Administration – Best Parish Practices Manual. Please refer to that Manual for additional list of Safeguards).

Computer Safeguards:

1. In General:
   - To protect confidential parish and parishioner data, all computers should be checked weekly to ensure they are current with Microsoft's critical security patches, anti-virus definition list and anti-spyware definition list.
   - Computer backups should be performed weekly on a rotating set of four disks (or other media). Backups should be locked in a secure area of another building on parish premises. The year-end backup should be performed and maintained with the parish's permanent records.
   - Microsoft no longer issues security updates for XP and Office 2003 as of April 2014. Windows Vista will no longer be supported as of April 2017. The impact of this will be that for each passing week after the end of support date the risk of having a computer compromised by malware will steadily increase. As such, the parish should take an inventory of their computers and develop a plan to phase out or upgrade those computers that are no longer supported to protect confidential parish and parishioner data, a "Windows" password should be established on all office computers.

2. Parish Data System (PDS) Office Management (including, Church, School, Faith Formation (referred to as "Office")) and Ledger (Desktop and On-Demand versions). Contact Ray Beaudry of Diocesan Computer Services at 847-5591 for assistance with "Office" software and Rick Dychowski at 847-8395 for "Ledger" assistance.
   - Appoint a security administrator, this should be someone offsite (i.e., Finance committee chairperson). Only the administrator should have the ability to delete funds. The administrator should also be the only person designated to establish new users and passwords.
   - User names, profiles, and passwords should be established to ensure that only authorized individuals have access to this information.
   - On-Demand users should use passwords for log in to the ACSTechnologies (ACST) icon AND the individual programs (Church, School, Formation Office, and Ledger).

- Only one individual should have access to record parish contributions or school/faith formation tuition and fees. All other persons besides the security administrator should have "view only" access to funds and contribution information.
- All Office users should be blocked from making direct posts, deleting batches and resetting batch numbers.
- All Office and Ledger users should be blocked from deleting the user log.
- To preserve the integrity of the PDS Office systems, families should never be deleted. Instead, they should be marked inactive.
- As of August 1, 2013 PDS no longer supports Ledger version 5. Both PDS Ledger and Office software should be upgraded to the latest version (version 7, as of May 2016). There is no cost if the monthly Perferred Client Program (PCP) fee is being paid to ACSTechnologies for each product and doing so will enable the parish or school to utilize various enhancements.
- Calendar and fiscal year-end computer backups of PDS Office and Ledger, respectively, should be performed on a flash drive and maintained with the permanent records. **These backups are not performed or retained through the automatic backup function in the On-Demand software.**

3. Vulnerability Management (Protecting electronic data)
   - Perform security updates when notified for non-operating software which includes Java, Adobe Reader, Adobe Flash, Firefox, Chrome, Safari, etc.
   - Limit internet browsing searches to work related credible web sites (many web sites have malware on them).
   - Do not electronically store any credit card information. If stored on paper, make all information illegible.

4. Protecting Personal Identifying Information (PII)
   - PII includes a full name, home address, social security number, vehicle registration plate number, driver's license number, credit card number, date of birth, gender, medical, educational, financial, employment and criminal information. Basically any single piece or combination of information that may identify an individual. This information may be in electronic or paper/hard copy form.
   - Your parish must not electronically store, process, or transmit credit card numbers. Your parish may accept credit card payments, but only through a third party (such as PayPal). PDS Church Office can be setup to accept credit card donations for registered parishioners. PDS works with a third party provider that will process the payments for you. Please contact Parish Data Systems or Ray Beaudry (Diocesan Computer

Service) for additional information. If you have questions with respect to credit card processing you should contact a third party provider or reference material found on the PCI Security Standards website: https://www.pcisecuritystandards.org/merchants/how_to_be_compliant.php

- PII Inventory – you may wish to take an inventory of PII that may be stored within your parish. The following questions may assist you in this process:
    - Where does your parish store PII? (Electronic form – computers, laptops, mobile devices, USB storage devices, removable media, the Internet cloud, on a vendor's computer, etc.?) (Paper form – local or remote individual/department rooms, desks or file cabinets?)
    - Is all PII stored within your Parish protected? (Electronic form – password protected, encrypted or secured in a room or file cabinet? (If password protected it is recommended that at least two (2) individuals within the parish have a file's password including the pastor)) (Paper form – secured in a room, desk or file cabinet?)
    - Is all PII that is housed or sent by your parish outside the Parish protected? (Electronic form – Excel, Word, Access, etc. documents are password protected (with password communicated to the receiver separately)? Does the vendor housing data on their computer on your behalf take reasonable measures to protect the parish's data? (You may wish to see the vendor's data protection agreement)) (Paper form – material should be sent with a cover letter specifying that contents contain PII and must be protected.)
    - Is all PII properly disposed of at the end of its useful life? (Electronic form – data should be erased or storage device destroyed.) (Paper form – shredded or otherwise rendered unreadable).

5. Your Checklist:
    a. Passwords
        i. Are my passwords STRONG (minimum of 7 characters consisting of a mixture of numbers, special characters and upper/lower case letters)?
        ii. I have not shared my passwords with anyone? (If I have I need to change my password.)
        iii. I did not leave my passwords on paper or post-ids in a public viewing area?
    b. Anti-Malware Protection
        i. I verify weekly that anti-malware software is functional and has current definition lists?

ii. I perform a full system scan monthly?

c. Apple and Microsoft Operation System Security Updates
    i. I make sure that I have installed all Microsoft or Apple critical patches?
d. Non-Operating Software Security Updates
    i. Other software includes Java, Adobe Reader, Adobe Flash, Firefox, Chrome, Safari, etc. I am performing updates when notifications are received or have set them to automatically update?
    ii. I am not downloading software from the Internet (like screensavers that are notorious for containing malware)?
e. Data Backup
    i. I have backed up my mission critical data this week?
    ii. I have verified the backup software is functional and backups are being done as expected.
f. Internet Browsing
    i. Based on my professional knowledge and needs have I limited my searches to work related credible web sites (many web sites have malware on them)?
    ii. I am not downloading pirated software?
g. E-mail
    i. I am suspicious of any unsolicited emails, phone calls, or text messages with an urgent request for personal financial information, from both known and unknown senders?
    ii. I delete spam and do not open it?
    iii. I never click on an embedded link or attachment in an unsolicited email?
h. Software
    i. I have obtained the System Administrators approval to install a new software application?
    ii. All software that I utilize has been purchased by the parish and the software license has been given to the System Administrator?
i. Credit Cards
    i. I have not electronically stored any credit card information?
    ii. I have made illegible all credit card information on paper?
j. HIPPA and Personally Identifiable Information (PII)
    i. All newly purchased non-Apple computers, laptops and servers should be encrypted. Windows 10 comes with encryption capabilities built-in.

ii. All non-Apple laptops currently in use should be encrypted. Priority should be given to those laptops containing PHI and PII

We recommend you share this information with your trustees and finance council / committee and document, in a memorandum, your computer safeguard procedures and communicate these to affected individuals during a periodic training session.

Next topic will discuss Auxiliary Organizations.