THE ROMAN CATHOLIC
ARCHDIOCESE OF ATLANTA

IT Questionnaire, Standards & Resources

The Office of Information Technology and Department of Internal Audit worked in collaboration to develop the IT Questionnaire, Standards & Resources document to assist parishes, missions, campus centers, and schools in assessing current cyber security preparedness status. Although the questionnaire will be include in each internal audit, we encourage each location to proactively evaluate their cyber security risk as soon as possible. If provided during an audit, please submit the completed questionnaire to the internal auditor. At the end of the questionnaire, you will find recommended IT standards, resources, and contact information.

Name of location: **Name of individual completing document:**

#	IT Questionnaire	Yes	No
	1. ON/OFF BOARDING EMPLOYEES		
1.1	Do you have documented policies and procedures for on/off boarding employees?		
1.2	Are users required to agree to and sign compliance with policies and procedures (i.e., Email and Internet Usage Policies; Social Media Policies; Remote Access, etc.) when on-boarded? If yes, are these documents maintained?		
1.3	Do you have an approval process in place to authorize access to parish/school IT resources such as email and individual applications? If yes, who manages this process?		
1.4	Are policies in place to redistribute or delete old user's files/data/access to other users upon an employee departure?		
1.5	Are old user IDs deleted from your system(s) when an employee departs?		
1.6	Provide a system report of users and their access type for: • Online giving Vendors (ex. Our Sunday Visitor) • Bill.com • Electronic Payment Processing Vendors (PayPal, Venmo, Square) • Parish/mission/campus centers donation software (ParishSoft Family Suite) • School – tuition management database (FACTS), student database software (RenWeb, PowerSchool), general ledger if using Blackbaud • School fundraising software – (could be a variety of vendors, such as Little Greenlight, Raiser's Edge, etc…) • Note: a list of users for ParishSoft Accounting is not required since access is managed at the Chancery level.		
	1.6.1 Does someone review & update access permissions to key financial and operational applications and IT resources on an annual basis to ensure that access permissions are still in line with job responsibilities?		

	IT Questionnaire Continued	Yes	No
2.	SUPPORT		
2.1	Is your email set up with its own specific domain account (example: @stmichael.org, @saintpeteratl.com) rather than using an outside account (examples: @live.com, @gmail.com)?		
2.2	Is your church/mission/campus center/school under some type of paid third-party support? **If "Yes" go to #2.3.** **If "No", skip to #2.4.**		
2.3	Do you have a written contract in place that clearly defines your terms with the Managed Service Provider (MSP)? If so…		
	2.3.1 WHO handles your requests for assistance (local personnel; outsourced help desk; designated support tech; etc.)? Response:		
	2.3.2 Has each individual that provides IT support through the third party vendor had a background check?		
	2.3.3 What does the support agreement cover?		
	• Hardware?		
	• Software?		
	• Infrastructure such as cabling; firewall; routers; switches; etc.		
	• Security?		
	2.3.4 WHERE does the support coverage exist (main office; rectory; remote user locations; etc.)? Response:		
	2.3.5 WHEN you can call them (24x7x365; M-F 9-5; etc.)? Response:		
	2.3.6 HOW are users able to submit a request for assistance (i.e. online help desk; e-mail; phone; etc.)? Response:		
2.4	If your church/mission/campus center/school does not have a third party support how is information technology administered? **Skip to #3 if paid third-party support is responsible for this.**		
	2.4.1 How is local/onsite equipment maintained (i.e., on-prem servers; workstations; printers and infrastructure like routers; firewalls; Wi-Fi access points; etc.)? Brief response:		
	2.4.2 IT Asset Management: Is the inventory of hardware tracked and monitored annually?		
	2.4.3 Who is designated as in charge of IT at the parish, mission, campus center or school? Brief response:		
	2.4.4 Are the servers on site? If so, how are they secured? Brief response:		
	2.4.5 If cloud-based servers/storage is used, where is data stored (examples: 365 {SharePoint/OneDrive}; Dropbox; Box: other?)		

#	IT Questionnaire Continued	Yes	No
3.	SECURITY		
3.1	Use of Firewall		
	3.1.1 Is there a managed (and updated) firewall in place at the office(s)? Please indicate the name of the firewall used:		
	3.1.2 If using MSP, is this included in the contract of services?		
3.2	Use of Anti-Virus Software		
	3.2.1 Are all of the workstations, servers, etc. protected by an updated antivirus subscription? If yes, what antivirus product are you using?		
	3.2.2 If using MSP, is management of antivirus software included in the contract of services?		
3.3	Who has access to the main credentials (passwords; keys; rooms; etc.)? Please indicate who has access & what they have access to: - Church/mission/campus center/school employees: - 3rd party support employees:		
3.4	Are the workstations and/or laptops used for church/mission/campus center/school use used only for business functions"? If equipment is shared for use with personal data, personal e-mail and/or any non-business information, please explain why: Brief response:		
3.5	Are USB drives, portable hard drives or any forms of removeable devices used to transfer data on business workstations? If so, how are these devices tracked? Note: The use of any portable devices is strongly discouraged as they can be used as a vehicle to introduce malicious content onto a system. Response:		
3.6	Are your employees required to create strong passwords to access IT resources, such as using a passphrase? See additional password strengths in IT Standards section below.		
	3.6.1 How often are users required to change their password?		
	3.6.2 Is multifactor authentication required for access to critical information, remote access, and Administrator and privileged?		
3.7	Has a phishing protocol been established?		
	3.7.1 Have employees and other church/mission/campus center/school personnel been briefed and educated on phishing scams?		
	3.7.2 Do you subscribe to or utilize some type of Awareness Training such as KnowBe4 or PhishingBox?		

	IT Questionnaire Continued	Yes	No
3.8	Are procedures in place to grant remote access to employees on a need-only basis?		
3.8	Are there measures in place to prevent personal email to be answered on church/mission/campus center/school computers?		
3.9	3.9.1 Is there a Wi-Fi network/access set up for visitors?		
	3.9.2 If the Wi-Fi is segmented, is all Wi-Fi "public" and access to the business network restricted?		
	4. DATA BACK UP & DISASTER RECOVERY		
4.1	Are backups of financial and operational data files (with the exception of ParishSoft Accounting & ParishSoft Family Suite) backed-up on a regular basis?		
	4.1.1 Are back-ups stored offsite or in the cloud?		
	4.1.2 Is this included in your MSP?		
4.2	Are the validity of backups being tested from time to time through a scheduled restore routine? If yes, is this documented and available for review? Response:		
4.3	Are vendor contact lists (with information including credentials; serial numbers; secret questions; etc.) being kept in a vault like LastPass or 1Password and accessible from somewhere other than the office?		
4.4	If a loss of continuity occurs WHO specifically leads the resumption of service?		
4.5	Is there a written disaster recovery protocol plan to step-by-step restored operations?		
4.6	Has the recovery protocol been tested?		

IT Standards & Resources

1. ON/OFF-BOARDING Employees

1.1 Develop & document IT policies and procedures that include procedures for requesting and granting system and application access permissions. These policies should also include guidelines for Password management, Internet Usage, Social Media Policies, and Remote Access.

1.2 Require users to agree to Internet Usage, Social Media and Remote Access policies when on-boarded. See the Archdiocese's Human Resources Employee manual for some guidance. https://archatl.com/offices/human-resources/business-managers-resources/

1.3 There should be a formal process with an audit trail for requesting, approving and granting access to IT resources. This can be implemented formally through the use of a help desk application or could be through email as long as the process is consistent and process owners are identified.

1.4 Delete unnecessary files and redistribute old user's files/data/access to other users upon termination for up to one year or more if needed.

1.5 Delete old user IDs from your system(s) when an employee exits.

1.6 Maintain a system report of users and their access type for: Parish Soft Family Suite, online giving vendors, Bill.com, and any other electronic payment processing vendors. Consider reviewing this report on an annual basis to ensure that access permissions are still in line with job responsibilities.

2. SUPPORT TIPS

2.1 Set up email using a parish, mission, campus center, or school specific domain account, (example: @stmichael.org, @saintpeteratl.com)

2.2 It is very important to retain a managed service provider (MSP) for IT support. When evaluating MSP's, ask if they have certified technicians that work for them and if so, what certifications do they hold (Microsoft; Cisco; etc.) The Archdiocese's IT department has a "suggested vendor's list" available for download on the Archdiocese' website. The latest version can be found at the following link: https://archatl.zendesk.com/hc/en-us/search?utf8=%E2%9C%93&query=vendor

2.3 Have a written contract in place that clearly defines your terms with the MSP. Consider the following:

2.3.1 Clarify who handles your requests for assistance: local personnel; outsourced help desk; designated support tech; etc…

2.3.2 Contact Safe Environment to have a background check on each individual that provides IT support.

2.3.3 Define exactly what the MSP covers, such as hardware; software; infrastructure (i.e. cabling; firewall; routers; switches; etc.), security. It's a good idea to meet with the MSP at least once each year to re-establish the guidelines in place and have them perform a site survey to be assured all technology is up-to-date and working properly.

Software updates should all be included in the parish's software license agreements, provided they are kept up to date. Assuming this, yes, it should be the responsibility of the MSP to make sure these updates are being applied, and this duty should be clearly detailed in the service agreement between the two parties. In order to save money, sometimes the MSP will pinpoint a parish employee to actually perform the work, but the MSP should manage the process as a mishap caused from outdated software/firmware/etc. should be the responsibility of the MSP.

2.3.4 Establish where the coverage exists: parish/school offices; rectory; remote user locations; etc.…

2.3.2 Agree on when you can call MSP for support: 24x7x365; M-F 9-5; etc.…

2.3.3 Establish how users are able to submit a request for assistance (i.e. online help desk; e-mail; phone; fax; etc.)

2.4 If your Parish does not have a third-party support, we highly recommend that you retain a managed service provider (MSP) for IT support immediately. In the meantime, you need to understand how information technology is administered.

2.4.1 Determine how local servers and computers maintained.

2.4.2 Take an inventory of hardware and monitor it annually; this can be maintained in an Excel spreadsheet or Smartsheet and should include the location, description (& serial number if applicable), purchase price, date acquired of each item.

2.4.3 Designate an employee in charge of IT.

2.4.4 Determine if there are servers on site, and if so, how they are secured.

3. SECURITY TIPS

3.1 There should be a firewall in place at the office and it should be managed and updated; Consider configuring the firewall to limit access to sites that may utilize significant bandwidth or malicious activity as well as the possibility of using GEO blocks from locations with known high threat levels (China, some middle eastern or South American countries); Consider including this as a responsibility of your MSP and ensure that it is included in the contractual services.

3.2 All of the workstations, servers, etc. should be protected by an updated antivirus subscription. Consider including this as a responsibility of your MSP and ensure that it is included in the contractual services. There are many, many low-cost alternatives out there to protect the PC. Some options to consider are:

https://www.webroot.com/us/en/home/products/av

CloudCare Managed Antivirus – 1-Year Subscription (techsoup.org)

3.3 Identify which church/mission/campus center/school employees and 3rd-party service provider employees have access to the main credentials (passwords; keys; rooms; etc.). **IMPORTANT**: Parish/mission/campus center/school employees need to control all credentials (usernames; passwords; etc. of common equipment such as switches, firewalls, servers, etc. - and be informed of any changes). NEVER should this information be solely handled by a third-party group). Each individual's job responsibilities should be review for ensure there is proper segregation of duties before access to the credentials are granted.

3.4 Document how is access to data handled: stays on workstations, on site servers or cloud servers designated for Church/mission/campus center/school use.

3.5 If USB drives and personal computers are utilized, establish how they are tracked. Consider blocking the use of USB drives and see 4.1 Backing up files for further discussion of risks related to these devices. If not blocked, consider enforcing virus scan of devices each time accessed. Simple cloud backup subscription services such as IDrive® : Cloud backup solutions for home and business or Cloud backup solutions for home and business | Carbonite are much better/safer options than using portable devices with may malfunction or become infected or compromised

3.6 Password guidelines should be documented in the IT Policies and Procedures, enforced through application and IT resource controls as may be possible.

Strong password tips:

- ✓ Are "Passphrases"
- ✓ Are at least 10 characters long
- ✓ Do not contain your user name or real name
- ✓ Do not contain a complete dictionary word
- ✓ Do not contain personal information, such as birthdates, names of family members or pets
- ✓ Are significantly different than previous passwords
- ✓ Contain uppercase letters, lowercase letters, numerals, and symbols

Examples: 1stSundayMa$$ -or- EyeM@Seven11 -or- BravesWin3-0!

3.6.1 Require that passwords are changed often - Enforce through application controls as may be possible. Changing your password often limits how long a compromised password can be useful. If your password is compromised and you are unaware of the unauthorized access, hackers can access your account until your next password change. Change your password immediately if you think it may have been compromised.

Sites like Secure Password Generator Passphrase Generator" **are informational, helpful and free of charge**!

3.6.2 Multifactor Authentication (MFA) provides an additional layer of security (such as a password and a verification code sent via text) and should be required for access to critical information, remote access, and Administrator and privileged information. Examples include email, Office 365 accounts, bank accounts,

Amazon business accounts, and on any app or platform that deals with money for which MFA is available. MFA is often a free component that must be set up or enabled as MFA has become a baseline of securing confidential information as cybercrime has continued to rise.

For more information on the MFA, visit the following sites:
What is Multifactor Authentication (microsoft.com)
Multi-factor authentication (MFA) | CISA

3.7 Develop a phishing protocol, which could include:

- ✓ Regular training of employees about phishing scams
- ✓ Deleting suspected email
- ✓ Alerting entire organization as to phishing scheme with a pre-produced phishing notice

3.7.1 Educate employees and other church/mission/campus center/school personnel on phishing scams. Consider subscribing to a training program like KnowBe4; Ninjio or the like https://www.gartner.com/reviews/market/security-awareness-computer-based-training

3.8 Put measures in place to prevent personal email to be answered on church computers. Consider using the functionality of your firewall to block personal email sites from their networked PC's or laptops as mentioned in 3.1 above.

3.9 Is there a guest network set up for visitors? This would be a separate place (segmented) on the network from where key operational and financial data resides.

4. DISASTER RECOVERY TIPS

4.1 If data files are not backed-up in the cloud or offsite, establish a back-up plan and monitor. DO NOT ever consider the use of USB drives to fall under best computing practices. The use of any USB-based storage device should be prohibited on business PCs as they can introduce malware to the environment. Contact your 3rd-party IT support group and have them block the use of these devices on your PCs. For more information on the risks involved, please refer to the following article: https://us-cert.cisa.gov/ncas/tips/ST08-001

Consider the use of a cloud backup service, such as like Carbonite and iDrive, for all essential business data. These automated services will create offsite, encrypted backups of your data and can be setup for auto backups that work around your employee's schedules. Again, contact your 3rd-party IT support services for their recommended options but should you want to research them yourselves, these links will provide you some great options …….

https://www.pcmag.com/picks/the-best-online-backup-services

https://www.tomsguide.com/best-picks/best-cloud-backup

https://www.nytimes.com/wirecutter/reviews/best-online-backup-service/

https://www.pcworld.com/article/3211435/online-backup-we-test-the-best-servicescarbonite-idrive-and-backblaze.html

4.2 Test the validity of backups from time to time through a scheduled restore routine.

4.3 Secure vendor contact lists: Information documented should include: vendor's contact information, contact information on those employees at the company that have credentials/permissions to parish/mission/school/campus center's systems/data; credentials (login, passwords, serial numbers; secret questions, etc…) needed to access any of the parish/mission/school/campus center's systems and online accounts in the event the 3rd party group maintaining this info for them were to disappear or go belly-up. Updates to the information should always be documented. This information should be kept in a vault like LastPass or 1Password that is accessible from somewhere other than the parish offices. There should always be more than one individual that has access to the online vault. Using an online vault would provide more flexibility to recovering this data than having it stored in a physical safe, especially if employees were not allowed to gain access to the building for some reason such as a flood or fire.

4.4 Have a loss of continuity plan, and determine WHO will specifically lead the resumption of service.

4.5 Create a written disaster recovery protocol plan that provides for detailed steps to restore the network in the event of cyberattack or natural disaster.

4.6 Include money in the annual budget for disaster recovery updates and testing.

QUESTIONS?

The IT Questionnaire, Standards, & Resource document was developed in collaboration by the Archdiocese Department of Internal Audit and the Office of Information Technology. If you have questions concerning the questionnaire, please let your auditor know. If you would like advice on topics addressed in this document, contact the Archdiocese Office of Information Technology. Although they will not act as your managed service provider for IT support, the Office of Information Technology offers consulting services, onsite walkthrough audits and central purchasing services. They will often share their policies, best practices, and lessons learned. For example, the Chancery requires all remote access users to abide by these guidelines and submit their acknowledgment. Remote Access Checklist

Contact: Tom Hardy
thardy@archatl.com
Director of Information Technology
Office of Information Technology
o: 404.920.7454
https://archatl.com/offices/information-technology/

Contact: Holly Orsagh
horsagh@archatl.com
Internal Audit Manager
Department of Internal Audit
o: 404.920.7906
Policies, Best Practices & Procedures - Roman Catholic Archdiocese of Atlanta | Atlanta, GA (archatl.com)