THE ROMAN CATHOLIC
ARCHDIOCESE OF ATLANTA

IT Questionnaire, Standards and Resources

Updated May 2025

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 their current cyber security preparedness status. Although the questionnaire will be included 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 and position of individual completing document: _____

#	IT Questionnaire	Yes	No
	1. ON/OFF BOARDING FOR IT RESOURCES		
1.1	Are the policies and procedures for on/off boarding parish/school employees or volunteers for IT resources (systems, applications, email) documented?		
1.2	Are users required to agree to and sign compliance with archdiocese IT policies and procedures (i.e., Email and Internet Usage Policies; Social Media Policies; Remote Access, etc.) when on- boarded by acknowledging receipt of the Employee Policy Manual or the Independent Contractor Packet? If yes, are these documents maintained at the parish/school in electronic or hardcopy form?		
1.3	Are users required to agree to and sign compliance with archdiocese IT policies and procedures (i.e., Email and Internet Usage Policies; Social Media Policies; Remote Access, etc.) when on- boarded by acknowledging receipt of the Employee Policy Manual or the Independent Contractor Packet? If yes, are these documents maintained at the parish/school in electronic or hardcopy form? Do the procedures include 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	Do the procedures include guidelines to redistribute, disable or delete old user's files/data/access to other users upon an employee or volunteer departure?		
	1.4.1 Are old user IDs disabled then deleted from your system(s) when an employee/volunteer departs? If yes, what is the time frame for disabling the user ID? _____ for deleting the user ID? _____		

#	**IT Questionnaire *(Continued)***	**Yes**	**No**
1.5	Provide a system report of users and their access type for: • General ledger if using Blackbaud (Note: a list of users for ParishSoft Accounting is not required since access is managed at the Chancery level.) • Online giving Vendors (ex. Our Sunday Visitor) • Electronic Payment Processing Vendors (PayPal, Venmo, Square, Clover) • Parish/mission/campus centers - donation software (ParishSoft Family Suite) • School – tuition management database (FACTS) • School - student database software (RenWeb, PowerSchool), • School fundraising software – (could be a variety of vendors, such as Little Greenlight, Raiser's Edge, etc…)		
	1.5.1 Does someone review and 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?		
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 IT support? **If "Yes" answer question #2.3** **If "No", answer question #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, please provide a copy. Also note that an example of MSP guidelines may be found at: https://help.archatl.com/hc/en-us/articles/28763302811284-Service-Level-Agreements-for-Managed-Service-Providers		
	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 on-site IT support through the MSP been safe environment certified?		

#	IT Questionnaire *(Continued)*	Yes	No
	2.3.3 What does the support agreement cover?		
	• Hardware?		
	• Software?		
	• Infrastructure such as cabling; firewall; routers; switches; WI-Fi access points, etc.		
	• Security: Anti-virus? Phishing awareness training?		
	2.3.4 WHERE does the support coverage exist? (i.e. main office; rectory; remote user locations; etc.)? Response: _____		
	2.3.5 WHEN is support available (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 you do not have third party support, how is information technology administered for the parish/school?		
	2.4.1 Who is designated as in charge of IT at the parish, mission, campus center or school? Name, title and IT background: _____		
	2.4.2 Which of the following is maintained onsite? Circle all that apply. - on-premises servers - workstations and/or laptops - printers - infrastructure like routers; firewalls; Wi-Fi access points; etc.		
	2.4.3 IT Asset Management: Is the inventory of hardware tracked and monitored annually?		
	2.4.4 Are the servers on site? If so, how are they secured? Brief response: _____		
	2.4.5 Which cloud-based servers/storage are used? _____ (examples: 365{SharePoint/OneDrive}; Dropbox; Box: other)		
3.	SECURITY		
3.1	Use of Firewall: Is there a managed (and updated) firewall in place at the office?		
	3.1.1 If yes, what is the name of the firewall used: _____		
3.2	Use of Anti-Virus Software: Are all of the workstations, servers, etc. protected by an updated antivirus subscription?		
	3.2.1 If yes, what antivirus product are you using? _____		

#	**IT Questionnaire *(Continued)***	**Yes**	**No**
3.3	Who has access to the main *IT administrator credentials* (usernames; passwords; etc. of common equipment such as switches, firewalls, servers, etc.; keys to server rooms; etc.)? Please provide a list of who within the organization has authorized access to this information and what they have access to: - Church/mission/campus center/school employees: _____ - 3rd party support employees: _____		
3.4	Are the workstations and/or laptops only used for business functions of the church/mission/campus center/school? 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? If yes, how is this enforced? _____		
	3.6.1 How often are users required to change their password?		
3.7	Where is multifactor authentication implemented for access to critical information? Circle all that apply: - remote access - email - financial services (banking/electronic payment apps (i.e. OSV) - Parish/School financial applications (i.e. PSA/PSFS/Bill) - Amazon Business accounts - Office 365 account - IT Administrator or privileged account access?		

#	IT Questionnaire *(Continued)*	Yes	No
3.8	Has a phishing protocol been established?		
	3.8.1 Have employees and other church/mission/campus center/school personnel been briefed and educated on phishing scams?		
	3.8.2 Do you subscribe to or utilize some type of Awareness Training such as KnowBe4 or PhishingBox?		
3.9	Are procedures in place to grant remote access to employees on a need-only basis?		
3.10	Are there measures in place to prevent personal email to be answered on church/mission/campus center/school computers?		
3.11	3.11.1. Is there a Wi-Fi network/access set up for visitors?		
	3.11.2. If the Wi-Fi is segmented, is all Wi-Fi "public" 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? Are the hard drives of laptops and desktops backed up on a regular basis?		
	4.1.1 Are back-ups stored offsite or in the cloud? Please specify: _____		
	4.1.2 Is there a scheduled testing of backups to confirm the validity of backups? If yes, is this documented and available for review? Response: _____		
4.2	Are vendor contact lists (with information including credentials as noted in 3.3 above; serial numbers; secret questions; etc.) being kept in a vault like LastPass or 1Password and accessible from somewhere other than the office?		
4.3	Is there a written disaster recovery protocol plan to step-by-step restored operations? 4.3.1Has the recovery protocol been tested? 4.3.3 If a loss of continuity occurs, WHO is responsible for coordinating the resumption of service? Name: _____		

THE ROMAN CATHOLIC
ARCHDIOCESE OF ATLANTA

IT Standards & Resources

Please be sure to reference the resources provided by the Information Technology Department of the Archdiocese of Atlanta on the Knowledge Base.

1. ON/OFF-BOARDING Employees

1.1 Develop & document IT policies and procedures that include: procedures for requesting and granting access to IT resources including system and application access permissions, procedures to redistribute, disable and delete access permissions, password and multi-factor authentication guidelines, Internet Usage, Social Media Policies, and Remote Access. Please see Onboarding Guidelines and Offboarding Guidelines resource documents for additional guidance.

1.2 Parishes and schools should include each employee's Acknowledgement of Receipt of the Employee Policy Manual in the personnel files. Independent contractors who access parish or school resources should complete the Independent Contractor Policies Acknowledgement form. The Employee Policy Manual and the Independent Contractor Packet provides guidelines for Internet Usage, Social Media and Remote Access and can be found on the Archdiocese's Business Manager HR Resources webpage for additional information and guidance.

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 Establish guidelines to for handling user files and access upon employee departure or termination to 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. Establish a timeframe to immediately disable then delete old user IDs from your system(s) when an employee or volunteer exits.

1.5 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 MSPs, ask if they have certified technicians and what certifications they hold (Microsoft; Cisco; etc.) Please visit the Archdiocese's IT webpage for a current list of Suggested IT Vendors.

2.3 Have a written contract in place that clearly defines your terms with the MSP. See Service Level Agreements for Managed Service Providers as a resource and also consider the following:

- Clarify who handles your requests for assistance: local personnel; outsourced help desk; designated support tech; etc…
- Contact your Safe Environment Coordinator to have a background check on each individual that provides IT support.
- 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 due to outdated software/firmware/etc. should be the responsibility of the MSP.
- Establish where the coverage exists: parish/school offices; rectory; remote user locations; etc.
- Agree on when you can call MSP for support: 24x7x365; M-F 9-5; etc.
- Establish how users submit a request for assistance (i.e. online help desk; e-mail; phone; fax; etc.)

2.4 If your Parish/School does not have third-party IT support, we highly recommend that you retain a managed service provider (MSP) for IT support immediately, please reference the list of Suggested IT Vendors who have had successful relationships with other parishes/schools within the archdiocese. In the meantime, you need to understand how information technology is administered.

- Designate an employee to be in charge of IT.
- Determine how and where hardware is maintained.
- Determine if there are servers on site, and if so, how they are secured.
- Take an inventory of hardware (workstations, laptops, printers, etc.) 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, and date acquired for each item. Please see the document IT Asset Management for additional information and guidance.

3. SECURITY TIPS

3.1 There should be a firewall in place at the office, and it should be managed and updated; Consider including the implementation, management and updates of the firewall as a responsibility of your MSP. You may also want

to 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. Please see the resource Cyber Security Best Practices and Guidelines for detailed information to consider when implementing IT security systems.

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 low-cost alternatives out there to protect equipment. 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 IT credentials such as 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, and servers) and be informed of any changes. NEVER should this information be solely handled by a third-party provider. Each employee's job responsibilities should be reviewed to ensure that there is proper segregation of duties before access to the credentials is granted.

3.4 It is recommended that parish/school IT resources are designated for business functions only. 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 The use of any USB-based storage devices should be prohibited on business PCs as they can introduce malware to the environment. Consider blocking the use of USB drives for backup or file sharing purposes. If USB drives and personal computers are utilized, establish how they are tracked and consider enforcing virus scans of devices each time they are 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 which may be lost, 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. The use of a password manager app can provide additional security; see Password Managers/Vaults for additional information and guidance.

In addition to Password Guidelines provided by the IT department, consider that strong passwords:

- ✓ Are "Passphrases"
- ✓ Are at least 10 characters long
- ✓ Do not contain your username 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!

- Require that passwords are changed often and enforce the changes through application controls to the extent possible. Changing your password frequently 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 and Passphrase Generator are informational, helpful and free of charge!

3.7 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. The Office of IT has developed Multi-Factor Authentication (MFA) Guidelines for your reference.

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

3.8 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

- 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
- Also consider the resources at CMG Connect offered through Catholic Mutual, instructions can be found at https://archatl.com/offices/finance/insurance/

3.9 Develop a remote access policy that includes consideration of antivirus protection, firewall access and a virtual private network (VPN) to ensure secure remote access to resources. Please reference the Work from Home/Remote Access Guidelines provided by the IT department for further information.

3.10 Put measures in place to prevent personal email from being answered on organization 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. Please also reference the Personal Email Guidelines/Policies provided by the IT department for further information.

3.11 Guest networks should be set up separately, that is segmented on the network, from where key operational and financial data resides.

4. DATA BACKUP and 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. As noted in 3.5, above, 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 Carbonite or iDrive, for all essential business data. These automated services will create offsite, encrypted backups of your data and can be set up for auto backups that work around your organization's schedule. Again, contact your MSP 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

- Test the validity of backups from time to time through a scheduled restore routine. Please see the document Testing Backups for additional information and an guidance.

4.2 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.

4.3 Include money in the annual budget for disaster recovery updates and testing. Please reference the Disaster Recovery Planning (DRP) Template available for download as provided by the IT department as a starting point.

- Create a written disaster recovery protocol plan that provides for detailed steps to restore the network in the event of cyberattack or natural disaster. Consider other business operations in the development of the plan as well.
- Test the plan.
- Determine WHO, specifically, will lead the resumption of service in the event of a loss of continuity.

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: Allegra Davis
adavis@archatl.com
Internal Audit Manager
Department of Internal Audit
o: 404.920.7906
Best Practices & Procedures (archatl.com)