THE ROMAN CATHOLIC
ARCHDIOCESE OF ATLANTA

IT Questions for Business Managers

5 areas of questions the parish business managers should be asked …

1. PASSWORD TIPS

- **Are your employees creating strong password that:**
    - 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
- **Are your employees changing their passwords often** - 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 are informational, helpful and free of charge**!

2. SUPPORT TIPS

- **Is your parish under some type of paid third-party support?**
    - Do you have a written contract in place that clearly defines your terms with the group? If so …….
        - **WHO** handles your requests for assistance (local personnel; outsourced help desk; designated support tech; etc.)
            - Have they had a background check?
        - **WHAT** they cover (hardware; software; infrastructure (i.e. cabling; firewall; routers; switches; etc.))
        - **WHERE** the coverage exists (parish offices; rectory; remote user locations; etc.)
        - **WHEN** you can call them (24x7x365; M-F 9-5; etc.)

        - **HOW** are users able to submit a request for assistance (i.e. online help desk; e-mail; phone; fax; etc.)
    - And, if you're not using a third-party IT group ….. **WHY**?!?
- If your Parish does not have a third party support how is information technology administered?
    - Local servers or computers – How are they maintiained?
    - Who is designated as in charge of IT at the Parish?
    - Are the servers on site?
        - If not how are they secured?

3. SECURITY TIPS

- **Is there a managed (and updated) firewall in place at the parish office(s)?**
- **Are all of the workstations, servers, etc. protected by an updated antivirus subscription?**
- **What employees have access to the main credentials (passwords; keys; rooms; etc.) What 3rd-party support employees have access to these items?**
    - ***IMPORTANT****: Parish 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)*
- **How is access to data handled? Does all data stay on workstations, on site servers or cloud servers designated for Church use? Or are USB drives and personal computer utilized?** If so how are they tracked?
- **Have employees and other Church personnel been briefed and educated on phishing scams?** Are there measures in place to prevent personal email to be answered on church computers? Has a phishing protocol been established
    - Phishing protocol could include:
        - Deleting suspected email
        - Alerting entire organization as to phishing scheme with a pre-produced phishing notice
- Subscribe to a training program like KnowBe4; Ninjio or the like https://www.gartner.com/reviews/market/security-awareness-computer-based-training

THE ROMAN CATHOLIC
ARCHDIOCESE OF ATLANTA

4. ONBOARDING/OFFBOARDING MANAGEMENT

- **Are users required to agree to policies and procedures (i.e. Internet Usage Policies; Social Media Policies; etc.) when onboarded? Do any policies/procedures even exist?**
- **Are old user IDs being deleted from your system(s) when an employee exits?**
- **Are policies in place to redistribute old user's files/data/access to other users upon a termination?**

5. DISASTER RECOVERY TIPS

- **Are backups of data files (with the exception of ParishSoft) being backed-up in the cloud or offsite?**
- **Are the validity of backups being tested from time to time through a scheduled restore routine?**
- **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 parish offices?**
- **Are all of the workstations, servers, etc. protected by an updated antivirus subscription?**
- **If a loss of continuity occurs WHO specifically leads the resumption of service? Is there a written disaster recovery protocol plan?**
- **Is there money budgeted annually for disaster recovery?**

Contact: Tom Hardy
<thardy@archatl.com>
Director of Information Technology
Office of Information Technology
2401 Lake Park Dr. SE • Smyrna, GA • 30080
o: 404.920.7454 • f: 404.920.7451