Parish Information and Technology Security Self-Assessment

Parish:

Address:

Parish Contact:

Email: Phone:

Date Assessment performed:

Person who performed assessment:

Parish employee \_\_\_ Volunteer \_\_\_ Vendor/Consultant \_\_\_\_\_

Email: Phone:

If person who performed assessment was volunteer or vendor/consultant please provide the following:

Address:

Website:

If there are any recommendation by the party that reviewed security to make improvements, please include with this assessment. These would be proposals for equipment, software, services to make the environment more secure.

Please send results of assessment to the attention of Deacon Ron Pirau, 1400 N. Meridian St., Indianapolis, IN 46202

## POLICIES AND PROCEDURES

1. Are effective security policies and procedures in place with clearly assigned responsibilities that protects sensitive data and technology resources?
2. Is the execution of security procedures verifiable through independent review?
3. Do the security procedures include training programs to educate staff on policies, procedures, and security risks?

## INFORMATION SECURITY

1. Do security procedures include appropriate disposal of old records and controlled access to electronic documents.
2. Are precautions in place such as encryption or additional access controls for viewing and transmitting sensitive information such as personal identity, health information, credit card information, and bank account numbers?
3. Is data backed up consistently on an appropriate schedule? Is recovery of backed up data tested to verify that it works?

## NETWORK AND DEVICE SECURITY

1. Is network administrative access appropriately limited and controlled?
2. Are strong passwords in place for all network and user accounts including WIFI?
3. Are network and peripheral devices including firewalls and wireless routers configured to protect systems and limit access to appropriate uses?
4. Are operating system and application system patches / updates installed and verified on all devices according to a set schedule?
5. Is anti-virus maintained and current on all devices?
6. Is an email spam filter in place to screen out email based security threats?
7. Are content filtering controls in place to prevent access to inappropriate Internet content or Internet content that poses security threats to the network.