RCAB Risk Management
Cyber Security Checklist

All locations should develop a cyber security plan and designate an individual responsible for keeping the plan up to date. Please use the checklist below as a guide.

- ☐ Document the names of employees with access to sensitive information.
- ☐ Educate employees about their privacy and security responsibilities before permitting access to sensitive information.
- ☐ Provide at least annual training sessions to ensure a continued understanding of responsibilities.
- ☐ Regarding personal information, collect only the information necessary.
- ☐ Have a plan in place to install security updates as early and often as possible. Make sure the automatic update feature is enabled on your computer systems.
- ☐ Educate staff regarding password protocols. Require staff to use complex passwords, to change them often, and to refrain from ever sharing passwords with others.
- ☐ Update/disable old and outdated computers and servers. Unsupported operating systems represent a significant risk.
- ☐ Frequently educate staff regarding email scams and ways to avoid falling victim.
- ☐ Be sure your parish/school owns its own website domain and social media accounts. Volunteers should not purchase IT-related services for your parish or school.
- ☐ Build and maintain a secure network by installing firewalls and antivirus software.
- ☐ Certify and accredit all information systems supporting the operations and assets of your organization, including those provided or managed by a third-party vendor.
- ☐ Ask all third-party vendors how they handle and store customer's data. Document the answer.
- ☐ Ensure that vendors have adequate liability insurance. Obtain a certificate of insurance for your files.

In the event you suspect a breach, contact the Office of Risk Management at 617-746-5740.

Office of Risk Management • 66 Brooks Drive, Braintree MA 02184 • Tel 617-746-5740 • www.rcabrisk.org
Questions: Email ormadmin@rcab.org