August 2019 A quarterly newsletter of the Diocese of Trenton Risk Management Program

Diocese of Trenton Risk Management Quarterly

Parishes, Schools, Cemeteries & Catholic Institutions

Fall Edition:

Child Protection Charter

The data collection for the USCCB Audit Report was recently completed. The Office of Child Protection is reviewing the data and preparing the required annual compliance report for Articles 12 and 13 of the Child Protection Charter.

Article 12: Requires that the Diocese maintain a "safe environment" program which the Bishop deems to be in accord with Catholic moral principles. The program is to be conducted cooperatively with parents, civil authorities, educators, and community organizations to provide education and training for children, youth, parents, ministers, educators, volunteers, and others about ways to make and maintain a safe environment for children and young people.

Dioceses are to make clear to clergy and all members of the community the standards of conduct for clergy and other persons in positions of trust with regard to children.

Article 13: Dioceses are to evaluate the background of all incardinated and non-incardinated priests and deacons who are engaged in ecclesiastical ministries in the diocese and all diocesan, parish, and school employees and volunteers whose duties include ongoing, unsupervised contact with minors and vulnerable adults.

Specifically, they are to utilize the resources of law enforcement and other community agencies.

Compliance with Article 12 and Article 13 is measured by auditing the number of employees and volunteers who have been background-checked and VIRTUS-trained in accordance with the Diocese of Trenton requirements.

The Diocese of Trenton strives to maintain full compliance at all times and appreciates the assistance of all the Safe Environment Coordinators, Pastors and Principals for their support of all Child Protection Programs for

PROMISE TO PROTECT
PLEDGE TO HEAL

Roof Access Hatches & Safety Surround – OSHA compliance

Recently, an employee of one of our schools was seriously injured when the safety surround on a building roof hatch incurred a material mechanical failure resulting in a fall of 14 feet from the roof opening to a concrete floor. The safety surround was approximately nine years old with no prior issues related to serviceability.

Due to this injury, the diocese is requiring that every building with roof hatches be inspected to determine if the hatch is a safe means of access to the roof and that the surround, hatch, and ladder access are compliant with current OSHA and building code standards.

Bill Wilson, retired Director of Buildings & Construction, is managing and leading this very important safety initiative. Be prepared to let him know how many building roof hatches exist on your campus buildings, how many have existing roof hatch surrounds, and how many have permanently-fixed ladders used for roof access. ■

Cyber Security
Plan for the Worst-Case Scenario

At least once a week there is a prominent story in the news regarding a cyber breach or ransomware event that strikes a school, city, government agency, or well-known company. We may have become numb to the news, but the effects can be devastating and not just disruptive. Some incidents are nothing more than mischievous acts that create mild to moderate inconveniences; others can be devastating to individuals who have had their identities compromised or businesses that have sustained irreparable reputational damage, losing the trust of the public.

During 2018, there were 122 cyberattacks[1] on K-12 educational institutions. Schools are targets of choice for cybercriminals because they manage significant quantities of highly-confidential personal information on students, their parents, staff, and faculty. The details contained in data files can include names, dates of birth, mailing and home addresses, Social Security numbers, phone numbers, banking information, health information, and other personal information. Student data is of particular interest as no credit history has been established and criminals have a blank slate to construct false financial histories and identities.

As with all security measures, common sense and clearly-defined operating procedures are the basic elements that require constant attention. As access almost always begins with a password, strong/complex passwords are an impediment to hackers, as are two step authentication requirements. **Never keep a file on a computer that lists passwords and IDs.**

Data encryption should be considered for all files that contain confidential and personally identifiable information (PII). Limit access to PII and confidential information only to those who need to have access. **Always consider the "Need to Know" as part of and data security program.**

Data backup is important for many reasons. There's nothing more frustrating than to work for hours, days, or weeks on a file that becomes corrupted or lost due to a hardware or software failure. A backup saves the day, not just when a system has been hacked or ransomware has invaded the network and your computer. **Backups are only good if they are retrievable—check backups regularly.**

Training is a critical component of cybersecurity. Many cyber events are triggered by an employee opening a malicious file or e-mail attachment, or by clicking on a website link disguised to appear as a familiar site often accessed by the employee for business or personal reasons. **Always be sensitive to the link provided to you by others. (See page 3 for more information on phishing and spear phishing.)**

The managed services provided by BlueVoyant/Blue Team Global are very effective in the mitigation of potential cyber intrusions. In addition to the active end point monitoring, management and mitigation, program participation limits the parish/school deductible for events that trigger Cyber Event insurance coverage to $5,000, which is well below the self-retained per occurrence cost of $100,000.

Any event that triggers insurance coverage or compromises personally identifiable information (PII) is reportable to the state of New Jersey and several other law enforcement agencies. In addition, a forensic investigation is required and legal representation is a necessity. Any reporting should be handled by the Office of Risk Management and the legal team engaged to oversee the incident. When the compromise of PII has been proven not to have occurred, expenses for legal and professional services typically range from $35,000 and $45,000. **Cyber events, including ransomware, cannot be ignored and must be reported to the Department of Risk Management at the Chancery office to either Joe Bianchi, 609-403-7208 (732-267-0381 cell) or Joe Cahill, 609-403-7189 (732-284-1600 cell) immediately.** Failure to act in the best interests of those potentially affected, including required timely notification, can result in unnecessary litigation and steep regulatory fines. The state of New Jersey has increased penalties for mismanagement of cyber events and greatly expanded the scope of what is considered personally identifiable information.

Planning for the worst-case scenario is prudent. Understanding the steps to take when the first signs of trouble appear is critical to containment, loss prevention, and minimizing business disruption. **Prepare a plan, review it regularly, and test it if possible.** Are your contracted computer service providers doing everything they can to protect your network and data? Anthony DeLorenzo, Director of Computer Services at the Chancery Office, is an invaluable resource and available to assist: adelor@dioceseoftrenton.org. ■

1 Cybersecurity Resource Center

"Phishers" of Men: Today's Biggest Threat to Data Security and How You Can Protect Yourself

Biblically, when we hear the phrase "fishers of men," we are reminded of Jesus calling his first Disciples (Matthew 4:18-20, Mark 1:16-18). These verses speak to the importance of spreading the message of Christianity through the Gospel. However, there's another type of phishing (pronounced *fishing*) of men, which has taken on a sinister connotation, and has become quite prevalent and dangerous in today's digital world. And it has the potential to negatively impact every one of us, if we're caught off guard.

Cybercriminals fully embrace the modern term "phishing," and its close cousin, "spear phishing." Phishing is a tactic used by hackers to obtain personal information from an end user via email. The risks of phishing on organizations implies a dire need for technology and skills to combat these attacks. As schemes grow in frequency – and complexity – it is more important than ever that organizations safeguard against future threats.

What is Spear Phishing?

The simplest definition of spear-phishing is an attempt to steal personal information from an individual or business and then use that information to access accounts or other digital assets from the individual and the organization. For instance, the hacker may email an employee to obtain their Social Security Number, birthday, driver's license number, or other data. They can then use that information to gain access to a bank account, PayPal account, or online data. Likewise, the hacker could also phish (that is, "hunt") for a company's information to hack into a network or infrastructure. How dangerous is spear phishing to both individuals and businesses? Spear phishing accounts for:

- 71% of targeted attacks involving email
- 66% of malware involving an attachment or file
- 93% of breaches involving social media
- 64% of attacks on all businesses in existence in the U.S.
- 21% of all malware attacks worldwide

Phishing Vs Spear-Phishing

When it comes to phishing and spear-phishing, the endgame is the same: acquiring private information. However, there is a subtle difference.

Phishing – When phishing, an attacker sends a malicious email to mass recipients – hundreds or thousands of potential victims. It becomes a numbers game. The more recipients who open the mail, the more victims the hacker can prey on. The hacker disguises himself or herself as a trusted source to fool the recipient. The sender attempts to lure the recipient into opening the email or attachment. Or they will persuade the person to click on a link to a dangerous website. From there the attacker will attempt to take over full control of the computer or network.

Spear-Phishing – During a spear-phishing attack, the hacker targets a demographic or profile. Rather than sending a mass email, the attacker sends a specific email to a smaller number of people based on certain criteria that include: social media profile, victim's online activity, work information, hobbies/interests, and friend/colleague information. Since attackers target their victims and customize their emails, they are far more successful at accessing private information than regular phishing. In addition, someone may use spear-phishing as a means to obtain information from a friend, colleague, or the person's company they are working for.

Protecting Yourself

Fortunately, however, spear-phishing attacks can be thwarted. Here are several tips:

- Be careful about what personal information you post online. Try to refrain from posting personal data on your social media pages or a website. When you create accounts, only provide the necessary information.
- Create smart passwords that have zero connection with anything in your life. Moreover, the passwords should make no sense at all. They should include at least eight characters made up of numbers, letters, and symbols.
- Perform software updates as the new software versions become available. Outdated software is more vulnerable to spear-phishing attacks.
- Refrain from clicking on any embedded links in an email linked to a website. You can also right click the link or scroll over the link to see the actual URL. If it does not match the website, then delete the email immediately. Also, never trust logos, letterhead, images, or anything else. Hackers are brilliant at making an email look legitimate.
- Delete any email that asks for personal information unless you are expecting the email and have confirmed the sender. Otherwise, there is no reason to hand out personal information via an email. ■

Article Submitted by Sentribit. Based in Mountainside, NJ, Sentribit is a Managed Security Solutions Provider specializing in Cybersecurity Monitoring, Detection, Response, Compliance, and Education.

Driving Safety

Driver and passenger safety is a serious concern of the Diocese of Trenton. Safe driving practices and properly-maintained vehicles are equally important. With 1 in 6 diocesan insured vehicles involved in an accident every year, safe operation and proper maintenance of the more than 600 insured vehicles is imperative.

The perils of winter driving are a long forgotten memory with the warm sunshine of August. It's important to prepare for the changing seasons and recognize the dangers of wet roadways covered in the leaves of fall, and the hazards of winter snow and ice that can make driving unsafe at almost any speed.

Vehicles need to be maintained year round but especially in the winter. Drivers must be ready to adapt to changing road conditions based on the weather. Extra caution is the key to safety when major weather threatens and visibility is impaired during the late fall and winter months.

Distracted driving is a component in more than 70% of motor vehicle accidents involving a diocesan insured vehicle. Focused attention to the operation of your vehicle is safe driving, and so is making sure that your vehicle is roadworthy; tires, battery, lights and fluids should be checked regularly. Always visually inspect your vehicle for fluid leaks or other potential problems.

If you are driving in areas experiencing heavy rain, snow, ice or windy conditions, adjust your driving to fit conditions and remember these driving tips: maintain a safe an reasonable speed, do not use cruise control, be alert for animals and downed trees, do not drive through water of an unknown depth, and remember that 4 wheel drive vehicles have better traction on snow and ice but don't stop any better than two wheel drive vehicles.

Every driver should have a "safety kit" in his or her vehicle for use in the event of an emergency. Include a flashlight, blanket, gloves, tools such as screwdrivers, pliars, duct tape, flares, first aid kit and other items that might be useful based upon driver experience.

Remember, preparedness is key to safety on the road. Share this article with your employees. ■

Hurricane Preparedness

Now Is the Time to Prepare — It Only Takes One

The Atlantic hurricane season officially begins on June 1 and runs through November 30 each year. Although the peak of the season is usually during August – October, preparation is strongly advised at all times no matter how many storms are forecast.

How to Prepare Your Church and School

At the start of every hurricane season, review any existing emergency response plans you have developed. These plans should generally include:

- Up-to-date contact information of employees, local emergency agencies, Diocesan Office of Risk Management and other Chancery contacts
- An emergency response team who will perform specific tasks in order to prepare for an event
- Communication procedures, cell phone numbers and e-mail address for all personnel critical to an emergency response
- A list of needed items and materials

In order to prepare a specific property or structure for a hurricane, keep in mind that buildings located next to open terrain where the wind can blow unobstructed — such as near fields, large bodies of water and parking lots — are likely to be damaged when the wind strikes with full force. Some tips for protecting your property in the case of a hurricane include the following:

Secure Your "Building Envelope"

The roof covering and building envelope are your first line of defense. Check the roof drains to ensure they are not clogged with debris and water can flow properly. The roof covering should be in good condition and free from blisters and other signs of physical damage. Also, the roof flashing should be tightly secured at the edge of the roof where the roof and building walls meet. Note: Unreinforced parapets (protective walls), decorative facades and unsecured mechanical equipment can blow over and damage the rooftop. Be sure to close and latch exterior doors and windows, and brace large doors.

Protect Against Wind-Borne Debris

Glass wall panels and plate glass windows are vulnerable to damage by wind-borne debris and the direct force of the wind. Before the storm, remove outdoor furniture, trash cans and other lightweight objects that could become wind-borne missiles. Indoors, relocate equipment away from windows or cover it with waterproof tarps.

In offices, remove items from windowsills and place papers and files in cabinets or other waterproof containers. Outside trailers should be tied down to the ground or building to prevent movement.

Prepare Equipment and Utilities

An orderly shutdown of equipment and utilities should be implemented. If deemed necessary, you may want to shut down critical utilities, such as natural gas and electrical systems, to prevent possible sources of ignition. Simply turning a piece of equipment to the off position may not be recommended until other steps are taken first.

Install flood panels and secure flood doors at least 24 hours before landfall is expected.

Back-up electrical equipment, such as uninterruptable power supplies (UPS systems) and generators, as well as sump pumps and other water removal systems, should be tested to ensure proper operation. Since it may be several days before the building can be occupied, make sure all fire protection equipment is in ready and working condition. Since electric power will probably not be available, ensure all fuel-fired equipment tanks are full.

Once the hurricane warning is issued, it's time to finalize all preparations as it may quickly become too dangerous to finish all the items you want to complete.

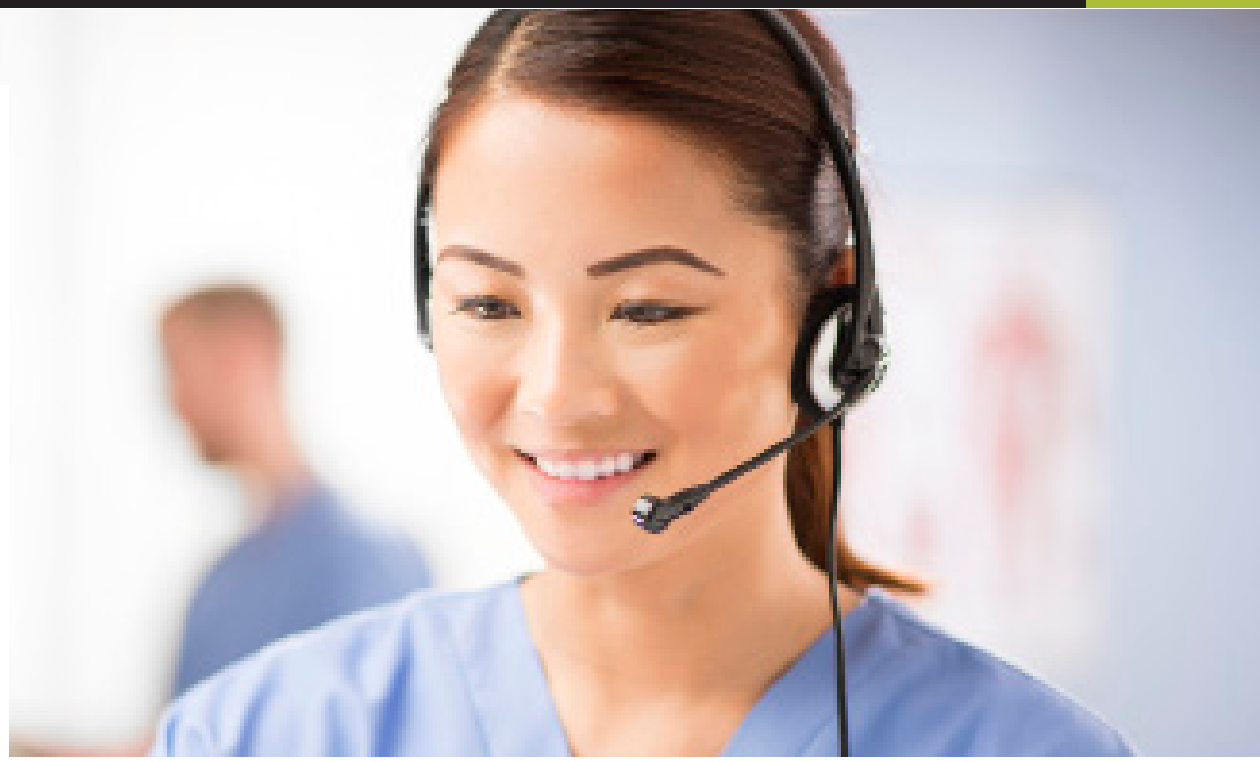
Post-Storm Assessment

Once the storm has passed, secure the facility and survey for damage, taking pictures or video. Review and document any damage to both the exterior and interior of buildings and their contents. Report all damage to the Diocesan Office of Risk Management. Contact Joe Cahill, 732-284-1600 (cell) or Joe Bianchi, 732-267-0381 (cell) for assistance.

Assume that all downed power lines are fully energized under all circumstances and avoid them. Before utilities are returned to service, check for gas leaks, look for electrical system damage, and check for sewage and water line damage.

Workers walking through areas covered with glass and other debris should wear proper personal protective equipment, such as steel-toed work boots, thick gloves, eye protection, dust masks and other safety equipment.

Should you need to shut down a fire sprinkler system during restoration, **follow the proper impairment procedures and notify the alarm company if alarm systems are placed in standby mode.** Follow proper permit procedure for any hot work that you may need to perform. Hot work includes the use of any flame or heat-producing device used for welding, brazing, grinding and soldering. ■



To access the PMA Care 24 Nurse Triage service:

When an employee is involved in a non-life threatening accident or injury, the employee should follow this procedure (If the manager or supervisor is available, he or she should also participate in the call):

1. Call the **CARE 24** Nurse Triage line at: **1-855-347-7334**. A triage nurse will review the situation and direct the employee to a participating provider who will best meet their medical needs. This service is available 24/7.
2. The incident should be reported by the supervisor/manager to Human Resources. The Diocese of Trenton Incident Report process is initiated with the call to **CARE 24**.
3. Employees should present the benefit card to the medical provider and/or pharmacy they are directed to for treatment. There are no out-of-pocket expenses for the employee related to any care provided when directed by the Triage Nurse.

This process will initiate a claim or notice of a claim with PMA, our Worker's Comp Claim's Administrator, and notification will be sent to Risk Management at the Diocese of Trenton confirming that the injury was reported.

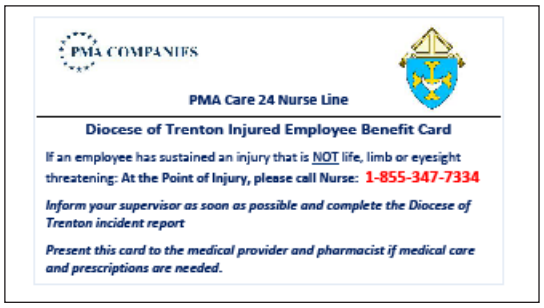
If an injury is not reported through CARE 24, it must be reported directly to PMA and a State of New Jersey First Incident of Injury Report must be completed and submitted.

Diocese of Trenton
Care 24
Workers' Compensation Benefit

In January 2017, a new workers' compensation benefit became available to all employees of the Diocese of Trenton specifically designed to provide the best medical care possible, as quickly as possible. The CARE 24 Nurse Triage Program, managed through our workers' compensation claims administrator, PMA, became available to all employees in the event they are injured on the job.

A licensed triage nurse is available by phone 24 hours a day, 7 days a week. The nurse provides triage and care coordination for the injured employee. The **CARE 24** Program has reduced time delays for treatment by avoiding emergency room visits for treatment that can be received at a local non-hospital emergency care facility. While this process will apply to most situations, any injury that threatens life, limb, or vision is immediately directed to the nearest hospital emergency room. **When in doubt, call 911.**

A webinar describing the program is available at: **http://www.dotinsurance.org/home/announcements/716-care-24-program** or by clicking on the **CARE 24** link on the Home Page of the Diocese of Trenton Insurance Website **www.dotinsurance.org**. A video has been posted for all employees explaining the reporting process and the benefits of the **CARE 24** Program. Every regular full-time


PMA COMPANIES

PMA Care 24 Nurse Line

Diocese of Trenton Injured Employee Benefit Card

If an employee has sustained an injury that is NOT life, limb or eyesight threatening: At the Point of Injury, please call Nurse: 1-855-347-7334

Inform your supervisor as soon as possible and complete the Diocese of Trenton incident report

Present this card to the medical provider and pharmacist if medical care and prescriptions are needed.

or part-time employee, including seasonal employees, should have a PMA **CARE 24** Card and know how to use it in the event of a workplace-related injury. An introduction to the PMA **CARE 24** process should be a part of every new employee training program. A PMA **CARE 24** posting should be placed with all employee notice postings required by law. If there are any questions concerning the program or benefit cards, contact Joe Cahill at 609-403-7189. To reorder cards, please send an e-mail to Joe Cahill requesting cards. ■

Cultivating Institutional Knowledge

Excerpt from **Don't be Dispassionate: "How to Use Emotional Impulses to Make Better Decisions"** *by Glenn Mott*

Understanding risk is an adaptive process—a continuing journey of best practices, best understood through a healthy alchemy of doubt, mission, and experience. NRMC's (Non-Profit Risk Management Center) risk management process consists of five steps:

1. **Consider the context:** In risk management, context refers to the environment in which an organization pursues its mission and delivers programs and services. Context is the backdrop for risk-taking and risk practice, making certain risks more or less likely to materialize. Risk context includes the setting, the surroundings, and the awareness of what is routine. In some instances, contextual issues or considerations may make risk management an urgent priority (such as post-scandal) or burdensome (such as during a period of high turnover). Contextual issues will affect implementation or adoption of risk management strategies.

2. **Appraise risks:** The process continues with identifying and discussing risks and exposures to events that potentially affect the objectives of the organization. Some nonprofit teams approach this part of the risk management process through informal brainstorming. Others use tools such as the Risk Bow Tie, root cause analysis, or the review of incident logs and claims files. Whether your team takes an informal approach or uses a framework to guide risk identification and appraisal, the key outcome is a deeper understanding and awareness of risks. After identifying risks, it's important to consider which issues warrant primary, versus secondary focus. This is the stage where some teams use a numeric scoring framework related to probability, potential impact, and in some cases, the organization's risk readiness. The NRMC team has found that spending an enormous amount of time on scoring can give the impression that the team's educated guesses are something more. An important reminder at this stage is to make sure the team identifying and appraising risks is diverse: include veterans as well as newer hires, those who are risk-takers and others who are risk averse.

3. **Decide what to do and communicate your decisions:** This step involves considering the possible options to address the likelihood or potential consequences of risk, or the organization's readiness to respond should the risk event occur. The team working on risk management evaluates alternative methods for addressing your exposures and selects the appropriate (practical, affordable, and effective) solution for each targeted exposure.

4. **Act on your decision(s):** Implementing strategies the risk management team has selected (such as a new screening process for volunteers), is often the most difficult part of the risk management process. This involves determining the necessary resources, including financial resources, human resources, and information technology required to bring new policies and practices to life.

5. **Follow up and adjust:** This step involves monitoring the results. How is the change in practice, policy, or training working for the organization? Has there been any pushback or suggestions to amend the approach? Strategies that are not working will almost certainly be felt on an emotional level, before they can be codified in a directive.

Risk is associated with almost every decision regarding the daily operations of a church and school. For the most part, risk exposure is well understood - best practices, in combination with experience, tend to keep the risk exposure low. It's the non-routine or one-time events that need careful evaluation of the potential to expose the institution to a situation that may result in an unexpected outcome, such as bodily injury or a liability lawsuit. Non-profits cannot protect themselves from exposure to a lawsuit by assuming that a claim of Charitable Immunity will provide adequate protection. If an institution operates outside of its normal (core) activities, many of the possible protections afforded to Charitable Institutions do not apply. Risks should be evaluated whenever a property is utilized by others or for purposes that are outside the bounds of normal religious or charitable services provided.

A few examples:

- School coaches use sports facilities to conduct sports camps not exclusively limited to parish school or religious education student participation.
- Parishioners utilize church property for fundraisers, parties, or social events that are not directly related to church ministries or for the 100% direct benefit of the church or school.
- Alumni events on school property regardless of the benefit to the school.
- Community or public events such as municipal, state, or federal voting, municipal "town hall" meetings, picnics, carnivals, fairs, flea markets, casino night, poker tournaments, blood drives, sporting events, etc.

The use of school or church property for political fundraising or rallies is not recommended even if the property is available to all candidates or political parties.

The proper "Use" agreements, permits, insurance, indemnifications and hold harmless agreements are essential to the protection of the parish, school, and diocese. The Diocesan Event Insurance Program may be utilized for eligible events, but additional insurance will be required in some circumstances. For more information, contact Joe Cahill at the Diocesan Risk Management Office, 608-403-7189

In all circumstances, the use of church property by any entity is governed by the requirement that the use of the licensed facility is in full compliance with the Child Protection Requirements of the Diocese of Trenton which includes a criminal background check prior to the start of the use of the facility when any activities involve minor children. In addition, the use of the facility must not in any manner be inconsistent with the teachings and practices of the Roman Catholic Church.

Items of Importance

Minimum Wage

The Minimum Wage in New Jersey increased to $10.00 per hour on July 1, 2019 and will increase again on January 1, 2020 to $11.00. Plan accordingly, especially if you employ seasonal workers paid at the minimum wage. Due to the size of the increase, there may be employees who were making more than the minimum wage prior to June 30, 2019, but are now earning less than $10.00 per hour. The minimum wage will increase every year on January 1st by $1.00 per hour until it reaches $15.00 per hour.

Property/Casualty Program

Property/Casualty invoices for the 2020 Fiscal Year were submitted to parishes, schools, and organizations in early July. Several parishes and schools have inquired about the percentage increases over last year. In the aggregate, the overall program premium increase was 12.4%. The new premium allocation model implemented almost three years ago has brought equality to the allocation of premiums to 90% of the program participants based upon standardized risk exposure metrics for workers' compensation, general liability, excess liability, and property at full replacement value.

Sixteen participant members experienced significant premium increases of 25% this year and there are a handful that will continue to receive large increases over the next few years until their allocation of premium costs is on an equal billing basis with all the other members of the plan.

The decreases/increases this year were as follows for participant members:

Premium Decrease	7%
0 – 4.99% Increase	16%
5 – 9.99% Increase	37%
10 – 14.99% Increase	9%
15 – 19.99% Increase	7%
20 – 24.99% Increase	10%
25 % Increase	14%
12.4% Increase	Program average

The premium allocation increase was primarily driven by the high (increased) cost of workers' compensation claims and property claims during the past year. The property program in particular incurred a doubling of property claims costs over the prior year due to a number of significant water damage/frozen pipe claims from this past winter, and several fires which until recently had been rare loss events.

Over time, we hope to see the water damage claims abate with the deployment of the HSB Sensor technology at all of our buildings. At present, 21 parish and ministry campuses have deployed the sensor technology, and more than 15 potentially significant loss incidents were avoided. This is a good start, but full deployment will be the key to reducing water damage claims in the future.

During the last two years, water damage claims totaled more than $1.8 million and have averaged more than $550,000 per year over the last 10 years. Workers' compensation claims continue to lead among all claims costs and accounts for more than 35% of our total claim reserves (incurred but not yet paid) across all line of coverages. Slip, trip and fall continue to dominate the number or frequency of claims. Many workers' compensation injuries occur when the requirements of the job are no longer within the capabilities of the individual to perform certain tasks. Always be attentive to the capabilities of all employees to perform tasks assigned in a safe manner.

As a primarily self-insured entity, the cost of program participation tracks to claims and the losses incurred. Lower premium allocations will be realized by all participants as the cost and frequency of property, workers' compensation, and automobile claims decline. Loss avoidance is the best way to reduce premium expense. The Department of Risk Management is always available to assist with loss control safety management.

Employment Law Posters

PosterGuard started shipping new Employment Poster updates on July 15th. If you haven't received your updated NJ posters, please contact Joe Cahill. jcahill@dioceseoftrenton.org, 609-403-7189.

HSB Environmental Sensor System

The deployment of the HSB Sensor System continues with installations completed at more than 20 parish and Catholic Charities campuses as of June 2019. There are more site surveys planned for this summer. As the program continues, the Hartford Steam Sensor Technology group continues to develop new algorithms that are predictive in nature. One that is ready for pilot testing identifies conditions under which mold can propagate based upon the data collected from temperature and humidity sensors.

Energy conservation reports for one of our parish participants (pilot testing) continues to identify opportunities for energy savings by monitoring temperature by time of day and analyzing space usage patterns, providing reports on a weekly basis. The loss prevention nature of the sensor technology is basic to our program, but there is so much more that can be achieved with this technology at no additional cost.

Thermographic Inspection – Electrical Systems

During the last three years, the electrical systems of all the building in the Diocese have been inspected using Infrared Thermographic Photography. A number of significant (severe) electrical problems were discovered and corrected. There were numerous advisory and corrective action recommendations made that prevented equipment failure and possible electrical fires.

The program has been a great success and regular inspections on a one- to five-year cycle will be scheduled based upon the building's electrical system age and severity of previously discovered issues. As in the past, inspection will be scheduled in geographic areas to minimize travel time and inspection costs. Schools and churches more than 70 years old are a priority for re-inspection. A minimum of 30 days advanced notice will be provided for inspections, which normally take place between May and September. ■

Safety First

The goal of the Department of Risk Management is to make sure all diocesan campuses are as safe as possible for its employees, as well as its visitors. The "Safety First" initiative has as its primary goal the protection of everyone working or visiting a diocesan property, with the potential for lower workers' compensation premiums. The Office of Risk Management sent letters to 100 parishes and schools requesting a hazard self-assessment of campus facilities in advance of an on-site meeting to discuss and plan for necessary corrective actions and safety improvements. In June of this year, information was sent to the same 100 parishes and schools in response to an incident at one of our campuses where someone was seriously injured while exiting a roof hatch. The information described how roof hatch protection is a necessity and must comply with OSHA Regulations.

The "Safety First" initiative at the Diocese of Trenton is focused on the proper use of Personal Protective Equipment, Fall Protection and Site Hazards. Every location will have unique issues and the Office of Risk Management is available to assist with the implementation of "Safety First" assessments and training. Contact Bill Wilson or Joe Cahill for more information or to discuss safety issue of concern at your parish, school, or cemetery. ■

Roman Catholic Diocese of Trenton
Department of Administrative Services
701 Lawrenceville Road
Trenton, NJ 08638

FIRST CLASS MAIL
US POSTAGE
PAID
MAILED FROM ZIP CODE 07006
PERMIT NO. 881

Summer Edition

Diocese of Trenton Risk Management Quarterly

Parishes, Schools, Cemeteries & Catholic Institutions

Inside this Issue:

Risk Management Key Contacts

Willis Towers Watson Team
Willis Insurance Services of Georgia, Inc.
Concourse Corp. Center 5, 18th Fl.
Atlanta, GA 30328

Jen Adams, Assistant VP
Tel: 404-302-3841
Jen.Adams@willistowerswatson.com

Mike Farrand, Sr. Principal
Tel: 610-715-1951
Mike.Farrand@willistowerswatson.com

Alex Lok, Sr. Client Specialist
Tel: 404-302-3824
Alex.Lok@willistowerswatson.com

Certificates of Insurance
For our online form, go to:
dotinsurance.org/forms/certs

Claim Reporting
PMA Management Corp.
PMA Corporate Processing Center
Tel: 800-482-9826; Fax: 856-727-3186

Auto Insurance Cards
Porter & Curtis, LLC
Tel: 484-445-7174
Email: trenton@aeti-inc.com

For our online form, go to:
dotinsurance.org/forms/auto-forms

Diocese of Trenton
Chancery
701 Lawrenceville Rd.
Trenton, NJ 08638
Main Tel: 609-406-7400

Joseph Bianchi, Chief Administrative Officer
Tel: 609-403-7208
Fax: 609-406-7413
jbianc@dioceseoftrenton.org

Joseph Cahill, Director of Risk Management
Tel: 609-403-7189
Fax: 609-403-7215
jcahill@dioceseoftrenton.org

Scot Pirozzi, Director, Department of Construction and Property
Tel: 609-403-7195
Fax: 609-406-7412
spiroz@dioceseofTrenton.org

www.dotinsurance.org

Insurance Hotline:
1-800-690-8709