September 2026

A quarterly newsletter of the Diocese of Trenton Risk Management Program

Diocese of Trenton
Risk Management Quarterly

Parishes, Schools, Cemeteries & Catholic Institutions



Fall Edition

Testimonial of Suitability for Priestly Ministry

Every employee as well as any volunteer who interacts with minors or vulnerable adults must be compliant with the criminal background check and monitoring, and the VIRTUS training and retraining requirements of the Diocese of Trenton Child Protection Program. But is there also a tool in place which applies to those non-diocesan members who seek to exercise priestly ministry within the Diocese of Trenton?

Permission from Bishop O'Connell is required before clergy, religious or lay ministers from outside the Diocese are invited to speak or exercise some ministry in the Diocese of Trenton. Requests for permission must be obtained from the Bishop's Office. In addition, invited priests or deacons must request that a letter or **Testimonial of Suitability** be sent from his diocese (or religious superior/provincial minister) to the Bishop of Trenton. The same applies to vowed religious brothers and sisters. These letters are managed by the Vicar for Clergy and Consecrated Life, Rev. Monsignor Thomas J. Mullelly.

Proof of Suitability to Minister

When a priest from outside our Diocese intends to perform priestly duties within our Diocese, Bishop O'Connell must receive a written certification from the bishop of that priest's home diocese stating the following:

- The priest is in good standing within his diocese or religious congregation.
- He has never been suspended or otherwise canonically disciplined.
- No criminal charges have ever been brought against him.
- He has never behaved in such a way as to indicate that he might engage in behavior inconsistent with priestly celibacy.
- He has never behaved in such a way as to indicate that he might deal with minors in an inappropriate manner.
- He has never behaved in a way to indicate that he might be suffering from alcoholism or other forms of substance misuse.
- He has no mental, moral, emotional or physical condition which might adversely affect his performance as a priest.
- He has never been involved in any known incident which might adversely affect his performance as a priest.

This **Testimonial of Suitability for Priestly Ministry** form must be on file before the priest engages in any priestly duty within the Diocese. This "screening" of priests from outside our Diocese ensures they will conduct themselves properly and with the safety and well-being of children, youth and vulnerable adults in mind.

Testimonial of Suitability Card

Likewise, all priests in good standing within the other four dioceses of NJ are issued a **Testimonial of Suitability Card**. This card identifies the priest by name and diocese and, along with government-issued identification, must be presented to the local pastor of the parish where the priest will minister. If the legitimacy of the card is challenged for date of expiration or other reasons, or if a priest from another diocese in NJ fails to present the card, permission for the exercise of the ministry will be denied. Ensuring the good standing of those priests from outside our diocese who wish to minister here and those who wish to minister away from their home Diocese of Trenton is yet another way to guarantee that those who come into contact with the most vulnerable among us have the support and trust of their Bishop. ■



Indoor Environments: Management of the Microbial Balance

The direction of healthier indoor air quality management has been shifting over the last 10 years. The definition of a healthy building is no longer driven by the oversimplified effort to eliminate all microbes to create a sterile environment. The approach has changed to achieve a reduction in the exposure to pathogens, mold growth, and contaminates that cause acute and chronic inflammation.

The shift away from treating buildings as a sterile enclosure to an indoor environment consisting of a healthy microbial world is driven by new research over the last ten years. Everyday life involves exposure to a diverse microbial world that can either help strengthen human immune development or, in an unhealthy environment, have the exact opposite effect.

The indoor environment is populated with microbes from a variety of sources, not just airborne bacteria, mold spores and particulate matter from outside. Other sources such as people, animals, water, indoor plants, dust and other materials in the building are contributing factors.

The indoor environment determines which organisms survive, grow, aerosolize or die off in a cycle driven by survival of the fittest. When diversified and balanced, a healthy microbiome can exist. When the environment favors the propagation of mold, pathogens, microbes and microbial fragments, conditions are ripe for allergic reactions, inflammation and toxin exposure.

Pathogens are dangerous. Mold growth in damp buildings, endotoxins, fungal particles and allergens may contribute to inflammation and respiratory symptoms. The goal is not to eliminate all microbes but to maintain a diverse and balanced environment while minimizing the exposure to organisms that have an adverse effect on health.

A balanced and diverse environment is influenced by the following:

Outside air introduced through fresh air intake (makeup air) in the HVAC system introduces diverse outdoor microbes while simultaneously diluting the buildup of indoor contaminates, including carbon dioxide.

Properly-configured air filtration in building air handling systems removes particulate matter such as pollen, air pollution and fungal spores from indoor air and outside makeup air.

Relative humidity, if too high, can promote mold growth and, if too low, can promote the transmission and dispersal of airborne particles of all kinds and impair the natural human respiratory defenses.

Thermal stress due to low or high temperatures can impact immune response in vulnerable populations, especially those with allergen sensitivity and respiratory and cardiovascular health conditions. High temperatures in combination with high humidity can promote mold and bacterial growth. The HSB Environmental Sensor system installed in most buildings in the diocese monitors temperature and humidity and will provide a mold alert to the location's contact, if the monitoring algorithm determines a temperature/humidity condition that would promote mold growth.

Strong chemical and antimicrobial cleaning chemicals can reduce pathogens on surfaces; however, there may be unintended results. Strong chemicals can irritate airways and may alter the microbial environment, allowing resistant organisms to predominate. Excessive disinfection, in low-risk environments, can diminish beneficial microbial diversity, allowing resistant organisms to propagate.

The proper management of ventilation, air filtration, temperature and humidity are key controllable factors in the process of maintaining a healthy building. Surface cleaning and disinfection are also critical. Unhealthy building conditions should be addressed by the appropriate professionals.

The services of an industrial hygienist may be needed to evaluate and test certain environmental conditions such as air quality, potential mold or other fungal/microbial contamination. Contact the Department of Risk Management for a referral to an Industrial Hygienist. Professional cleaning services should be hired to address all protocols documented by an Industrial Hygienist. Professional janitorial services for daily building cleaning should be considered if occupancy loads or square footage of the building are high or beyond the capabilities of custodial staff.

References

HPAC Engineering July/August 2026

National Academies of Sciences, Engineering and Medicine – A Research Agenda for Indoor Microbiology, Human Health, and Buildings. National Academies Press 2017.

This newsletter is provided for informational purposes only. The Diocese of Trenton assumes no liability arising out of the use or application of this information.

Disaster Preparation: Hurricanes

Peak season is here and now is the time to prepare — it only takes one.

The effects of a hurricane or tropical storm can be felt not just along the coast, but for hundreds of miles inland. Inland flooding is a major concern, even if you are not physically located in a flood zone. Tornadoes are frequently spawned from hurricanes and tropical storms making landfall, so precautions are needed to protect structures and personnel from these events as well.

When a tropical storm or hurricane watch is issued, local weather and news will provide guidance on the path of the storm and information about mandatory evacuation orders from public emergency management authorities.

2026 landfall forecasts

This summer, NOAA's National Hurricane Center (NHC) implemented an improved version of its tropical cyclone forecast cone graphic, which includes tropical storm and hurricane watches and warnings for inland areas that will incorporate direction of movement and timing. NOAA's new technology provides high resolution Flood Inundation Mapping with visualization of streets and neighborhoods likely to go underwater.

How to prepare your church/school

Every hurricane season, review any existing emergency response plans you have. These plans should generally include:

- Up-to-date contact information for employees, local emergency agencies, Diocesan offices
- Emergency response team who will perform specific tasks before, during and after the event
- Communication procedures and cell phone numbers and email addresses for all personnel critical to an emergency response
- A list of items and materials needed

Keep in mind that buildings located next to open terrain where the wind can blow unobstructed — such as nearby fields, large bodies of water and parking lots — are likely to be damaged when the wind strikes with full force. 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 roof drains to ensure they are not clogged with debris and water can flow. The roof covering should be in good condition and free from blisters and other signs of physical damage. The roof flashing should be tightly secured at the edge of the roof where the roof and building walls meet. Unreinforced parapets (protective walls), decorative facades and unsecured mechanical equipment can blow over and damage the rooftop. 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
Implement an orderly shutdown of equipment and utilities. 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 off 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, 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. 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.

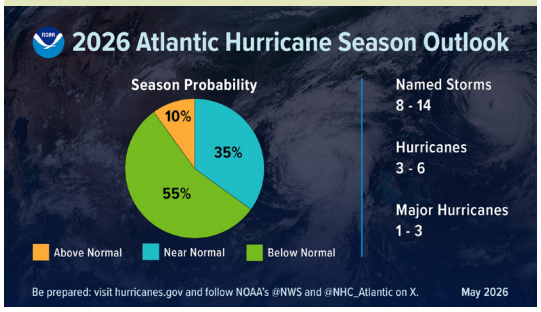
Understanding Hurricane Terminology

Hurricane: A tropical storm that reaches wind speed of 74 miles per hour or greater.

Major hurricane: A hurricane which reaches a sustained low-level wind of at least 111 mph (96 knots) at some point in its occurrence. This equates to a Category 3 or higher on the Saffir-Simpson Hurricane Wind Scale.

Hurricane watch: Hurricane conditions are possible within the specified area. (Because hurricane preparedness activities become difficult once winds reach tropical storm force, the hurricane watch is issued 48 hours in advance of the anticipated onset of tropical storm-force winds.)

Hurricane warning: Hurricane conditions (sustained winds of 74 mph or higher) are expected somewhere within the specified area. (Because hurricane preparedness activities become difficult once winds reach tropical storm force, the hurricane warning is issued 36 hours in advance of the anticipated onset of tropical storm-force winds.)



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 thick sole 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. ■



Are You Covered? The Value of COIs

Are your parish/school-owned properties covered when used by others for events or the performance of services?

A Certificate of Insurance (COI) is needed when an outside party (a Lessee, Licensee, Vendor, Contractor or Service Provider) **uses** parish/school-owned property or **performs a service** on the property. The COI accompanies a **contractual agreement** signed by both parties. The outside party must name the Parish/School and Diocese of Trenton as an additional insured on their commercial general liability policy in accordance with the required limits of coverage for the following lines: liability; property damage; medical coverage; completed works; sexual abuse and molestation; other coverage deemed appropriate. Proof of insurance coverage for workers' compensation and auto liability for owned and non-owned vehicles is also required.

Typically, the named additional insured would be the Pastor, Parish, Diocese and Bishop. It may also be appropriate to name the school/principal, cemetery, director or social service agency, and executive director. Additional insured coverage must be primary and noncontributory with a waiver of subrogation to the benefit of the Parish/Diocese. Most insurance companies require a contract for additional insured status; otherwise the COI, no matter the language, will just be a confirmation (proof) of insurance coverage.

Many COIs with additional insured language will clearly state that the status is dependent upon a contractual obligation, but not always. **Always have a COI reviewed by the Department of Risk Management.** Keep it on file for a minimum of six years.

The use of church property by an outside party typically falls into two categories:

Leases are required for the use of a building for an extended period of time on an exclusive basis and on occasion with negotiated, limited use by the landlord. Leases have a long duration with renewal options and are not easily terminated. A lease grants the tenant exclusive possession and a legal interest in the property for a set term. The Construction & Real Estate and Finance departments must review all leases, and the signature of the Bishop is required. The Diocesan Land Use Attorney should prepare all leases in coordination with Construction & Real Estate.

License agreements are usually written for the use of space, with or without a fee, in a building for a limited number of hours or days for a very specific purpose such as the parish hall for a party, a meeting room for a self-help group or a basketball court for practice. Licenses provide no rights to the Licensee other than the use of the property subject to the conditions of the agreement which can be easily terminated with written notice by either party. License agreements are between the parish and the Licensee and do not require the signature of the Bishop. License "USE" agreements are issued by the Department of Risk Management, which must review and approve the COI. The Licensee may opt to waive the COI requirement by paying a fee to the parish, which the parish will use to purchase Special Events (TULIP) coverage, but only if the event is an **approved use** in the special events program policy – sports activities and other activities specifically prohibited in the Special Events policy are not eligible events.

License agreements are required for all third-party use of parish properties even if no fee is charged for the use of the property. Examples: NA, AA, SVDP Food Pantry, Knights of Columbus, Scouts, American Heritage Girls. License agreements spanning a full year can contain language that allows for perpetual renewal, as long as the COI is valid and compliant. Perpetual license agreements can be terminated by either party with 10-day-written notice, and also with a change in pastor. Leases and Licenses include conditions such as insurance, compliance with the Child Protection policies of the Diocese, and other conditions appropriately documented, including that the use of the property cannot be contrary to Catholic teachings.

Contractors and Vendors

All parishes, schools and cemeteries must obtain up-to-date insurance COIs for both Workers' Compensation (WC) and General Liability (GL) and Property Damage from vendors and subcontractors that perform work on church or school property, owned or leased. The Parish, Pastor, Diocese and Bishop must be named as additional insured and there must be a contractual obligation to provide additional insured status in the contract between the vendor and the parish. Typically, the need for obtaining evidence of GL coverage is straightforward. Any damage or injuries to others caused by the vendors or subcontractors should be their responsibility and requiring them to have GL coverage will help ensure these damages are covered.

It is critical that all contractors, vendors and service providers do business with the parish under a contract that stipulates that the parish and diocese are additional insureds on their commercial package insurance policy with the coverages and limits required. If the contract doesn't include language related to the provision of the insurance and indemnification of the parish and diocese, it shouldn't be signed. The signed acceptance of a proposal is not necessarily a contract and will not likely have the insurance and indemnification language required. If the vendor cannot or will not include the necessary language, the Risk Management Department can provide an addendum to attach to the contract/proposal that must be signed by both parties. Payment to a contractor/service provider should only be made if a proper COI and W9 have been provided.

In a similar manner, required WC coverage to statutory limits in NJ ensures the vendors' and subcontractors' employees are covered if one of their workers is injured while providing services on church, school or cemetery property. However, "small" contractors consisting of a one-person (owner and sole proprietor) company are not required by NJ law to carry WC coverage. **These small contractors, if injured during the performance of their work, could and likely would make a claim against the diocesan WC program or GL policy.**

Uninsured contractors should never be hired; however, an occasional situation may arise where the needed services are unavailable elsewhere. If this occurs, a Hold Harmless Agreement, provided by or approved by the Diocesan Department of Risk Management, specific to the individual and services provided should be obtained prior to the performance of any contracted work.

continued on page 5

Certificates of Insurance (COI), *continued from page 4*

All work conducted on parish, school or cemetery property must have a contract that includes a named additional insured obligation. All contracts must include language that prohibits subcontracting of work to others without specific "written" contractual permission from the parish, assuming that all insurance requirements can be met.

The **"best practice"** is to use only fully insured contractors who can provide COIs indicating both GL and WC coverage.

Most lease and license agreement documents prepared by the Diocese will require owned and non-owned automobile liability coverage. In a commercial auto insurance package, **auto liability coverage for owned vehicles** protects the business from third-party claims (bodily injury or property damage) when company-owned cars are used in operations. **For non-owned vehicles**, the need for additional coverage comes from a common gap in standard policies:

- **Personal auto policies** often exclude business use, especially for deliveries, client meetings, or errands, and may have lower limits.
- **Commercial auto policies** typically only cover vehicles the business owns, leases, hires, or borrows (hired auto coverage) unless the policy includes a hired/non-owned auto (HNOA) endorsement.
- If an employee drives their personal car for work, the business can still be held liable for damages or injuries, even though the vehicle isn't company-owned.
- **Non-owned auto coverage** protects the business when employees, partners, or others use their personal vehicles for business purposes. This can fill the gap left by personal auto policies and ensure the business meets its liability limits.

Including auto liability coverage for both owned and non-owned vehicles in a commercial policy ensures the business is protected from liability in all relevant vehicle use scenarios. Without HNOA, businesses risk paying claims out of pocket or facing lawsuits when employee or company use of vehicles is not covered under the standard policy. ■

Boiler & Machinery Insurance

Boiler & Machinery coverage renewed for all locations on August 1, 2026. Invoices were distributed from JM Glover, our Broker of Record, for HSB Boiler & Machinery before September 1, 2026. Please pay by the due date.

HSB Common Boiler Inspection Failure within the Diocese

Condition

Jurisdictional requirements specify that the makeup water pipe must be provided with a check valve near the boiler. Many boiler systems, existing and newly installed, have a back flow preventer installed in lieu of a check valve. Although this is an approved American Society of Mechanical Engineers (ASME) equivalent for the check valve, the State of NJ does not accept the backflow preventer valve as an acceptable check valve equivalent.

Code Recommendation

For code compliance, HSB recommends installing a check valve and stop valve in the makeup water line as close to the boiler as possible. A stop valve is required between the check valve and the boiler. Please note that all other devices (backflow preventer, feeder valve, pressure reducer, etc.) and bypass lines must be located upstream of the required check and stop valves. If the check valve is installed in a vertical section of pipe, it must be of the spring-loaded type. ■

Items of Importance

Labor Law Posting Requirement

The NJ Family Leave Act (NJFLA) posting has been updated with a mandatory change to show eligibility changes that took effect on July 17. Employers with 15 or more employees worldwide or government entities must generally provide NJFLA leave. Employees who have worked for an employer for at least three months and who have worked at least 250 hours in the past 12 months may take leave for a covered event. As a subscriber to the J J Keller Update Service, you will receive a new poster when **New Jersey** releases the final wording.

VIRTUS

Multiple updates to the VIRTUS Online platform have been issued recently. A webinar is available on the VIRTUS website for viewing – the passcode is 0T$rRaB5. Contact Janet Boris, Associate Director, Child Protection, for assistance. Updates include local administrator rights template, option to add dropdown lists for titles/ministries, and much more.

New Jersey Department of Environmental Protection

Includes boilers with fuel input of 1 million BTU to 50 million BTU as Minor Source

The Division of Air Quality, Bureau of Stationary Sources (BoSS) announced a revision to the Air Permit Application Checklist and a new requirement that the checklist be submitted as a **mandatory** attachment with all future air permit applications. The revised checklist is now divided into two documents: (1) *Air Permit Application Checklist for Minor Source Facilities* and (2) *Air Permit Application Checklist for Title V Major Source Facilities*. Each checklist is designed as a fillable PDF form that will display relevant questions for the application selected by the user.

Questions are asked as "Yes" or "No" questions and designed for a "Yes" response to indicate the user has completed the necessary task. As such, any "No" responses will require an explanation at the end of the form with a reference to the specific question. If a required item is not included and no explanation is provided, the application may be found administratively and/or technically deficient.

The intent of this checklist is to more clearly define required elements of air permit applications to minimize the number of deficiencies and reduce permit application review times. The checklist does not introduce any new requirements.

The revised checklists are now available on the BoSS webpage at **https://dep.nj.gov/boss/applications-and-forms/** webpage under **Other Applications and Forms**.

continued on page 7



Cyber Risk:
What Parishes Need To Do

Reprinted in part from the National Catholic Report with the permission of The National Catholic Risk Retention Group

Catholic parishes increasingly rely on digital tools to support their mission. Online giving, parish databases, email communications, livestreamed liturgies, and accounting software have become essential to daily operations. Unfortunately, this reliance also makes parishes attractive targets for cybercrime. Attackers often assume parishes lack technical resources, making prevention especially important.

Why Parishes Are at Risk

Parishes handle sensitive information (in a digital format), including donor records, financial accounts, employee data, and sometimes sacramental or pastoral records. Common cyber threats include fraudulent emails requesting wire transfers or gift cards, hacked email accounts impersonating clergy, ransomware that locks parish files, and theft of online donation funds. Even a single incident can disrupt ministry, harm trust, and divert funds away from pastoral work.

Cybersecurity as an Ongoing Program

Cybersecurity should not be treated as a one-time project or a checklist that is completed and forgotten. Instead, parishes should view cybersecurity as an ongoing program that supports good stewardship and responsible governance. Technology, threats, staff, and volunteers change over time, and parish protections must adapt accordingly. A small number of consistent practices, reviewed regularly, are far more effective than a long list of controls that are never revisited. At a minimum, parish leadership should review cybersecurity practices **annually**, ideally as part of financial or operational reviews. Initial steps to this review can be simple: confirming that passwords are updated, staff and volunteers have received refresher guidance, backups are functioning and contact information for support and the diocese is current. For a more detailed review, consultation with a cybersecurity specialist is recommended. While no solutions are foolproof, failure to act can be highly detrimental.

Practical Protections for Parishes

One of the most effective safeguards is **staff and volunteer awareness training**. Many cyber incidents begin with a deceptive email that appears to come from the pastor, bookkeeper, or diocese. Training parish staff and key volunteers to pause, verify unusual requests, and be cautious with links and attachments can prevent costly mistakes.

Clear financial procedures are essential. Parishes should require verbal or in-person confirmation for requests involving money, changes to bank information, or gift card purchases. These simple controls may stop many common scams.

Using **strong passwords and multifactor authentication** may protect email, accounting systems, and online giving platforms. **Regular software updates** and **secure data backups**, disconnected and stored separately from parish computers, help ensure continuity if systems are compromised. Trusted **endpoint protection** and **antivirus software** provide ongoing protection with minimal effort.

Every parish should also maintain a **basic incident response plan**, reviewed annually, so staff know who to contact and what steps to take if a problem arises.

Costs Versus Stewardship

Basic cybersecurity measures typically cost a few thousand dollars per year. By comparison, the financial, operational, and pastoral impact of a cyber incident can be far greater, in some cases over $200,000. Treating cybersecurity as a routine, essential parish risk mitigation program is an act of faithful stewardship that protects parish resources so the mission of the Church can continue without disruption.

Getting Assistance

If you have questions or need assistance implementing these cybersecurity practices, your parish is not alone. Your Diocese, parish IT support providers, Office of Risk Management, and professional advisors are available to guide you, answer questions, and help tailor policies and protections to your parish's size and resources.

Reaching out for help is a smart step in safeguarding parish operations, finances, and the trust of your community. No matter the size of the parish or school, you are a target for cyber criminals. Awareness training can have a major impact. Don't be the next victim.

Suspicious Email – Stop, Read Carefully, Think. Don't be fooled.

- **Don't reply to the email, even if it comes from someone you know.** If you do reply, the person who replies to you probably won't be who you expect if the account has been compromised. You could be communicating with a cybercriminal.
- **Do not forward the email.** The best practice is to never click a link or open an attachment that you were not expecting. If you are fooled by a phishing email and open an attachment, the file may actually open an installation window or redirect you to a fake login page. Never forward an unusual or suspicious email to others. Delete the email.
- **Don't mark suspicious email as spam.** Spam emails are typically unwanted advertisements. While spam emails are annoying, they are usually harmless. A phishing attack is a malicious email designed to look like a legitimate message. **Phishing emails typically include a call to action: click a link – open an attachment – provide credentials – transfer money.** If you mark a suspicious email as spam, it will be moved to a folder along with other emails from the sender and remain hidden until you delete or empty the spam folder, leaving the problem unresolved.
- **Utilize the phishing button** in your Outlook tool bar to report the email to the IT Team at the Diocese or your remote Endpoint Solution Management provider to assess and mitigate the threat. Follow the cybersecurity protocols that have been put in place to keep everyone's information safe. ■

Crime & Fraud Prevention

Many nonprofit organizations are especially vulnerable to crime and fraud due to limited resources, reliance on volunteers with minimal oversight, and the failure to strictly adhere to established internal financial controls. Fraud not only results in financial losses — it also erodes public trust, leading to long-term reputational damage.

Fraud Risk Can Be Minimized

1. Follow Internal Financial Controls. Conduct internal reviews of policies, practices and procedures at least annually. Only about 4% of fraud cases are discovered through external audits, which are primarily designed to validate financial statements, not uncover fraud. There is a genuine benefit and stewardship need for the periodic spot-checking of payroll details, vendor payments, and credit card charges matched to receipts and invoices.

2. Segregation of Duties. One of the most important controls is the proper segregation of duties. This principle ensures that no single person is responsible for completing all aspects of a financial transaction — processing, approving, and reconciling. Without this segregation, it becomes much easier for an individual to commit fraud unnoticed.

3. Conduct Fraud Awareness Training. Everyone in the organization should be on the lookout for fraud. Employees should be educated about the behavioral red flags of fraud and how to report concerns. Fraudsters usually display at least one of these behavioral signs — refusing to share responsibilities; exhibiting sudden wealth; isolating themselves from the oversight.

4. Conduct Thorough Background Checks. Diocesan policy requires that every employee receive a fingerprint-based criminal background check and, if handling money, a credit check. Verification of employment history and prior job responsibilities is essential. Be diligent in the verification of employment history and references. Individuals who defraud an organization will likely have committed similar offenses at a previous job.

5. Encourage and Facilitate Whistleblowing. An effective whistleblowing system is essential for fraud detection. Train staff on how to report fraud.

6. Enforce Policies Consistently. Having a set of strong policies in place is only useful if those policies are consistently enforced.

7. Signature Authority. Signature authority should align with Diocesan policy. No exceptions.

8. Financial Expertise on the Finance Council. Having at least one member of the Finance Council with financial or accounting expertise is invaluable.

Supplemental Questions

As we approach the renewal of our Crime and Fiduciary insurance policies, the carriers have presented several supplemental questions which should be considered by every parish and school as critical to compliance with the Diocesan Internal Financial Controls Policy.

1. How many individuals are authorized to approve or execute funds transfers?
2. Is multi-factor authentication (MFA) required by policy for independent contractors who are remotely accessing the corporate network, cloud-based email, CRM or any services where banking or payment systems may be accessed? (Multi-factor authentication means authentication which uses at least two different types of the possible authentication factors to confirm identity.)
3. Other than employees, who has access to accounting and banking data (outside accountants, consultants, outside IT administrators)?
4. How frequently are access reviews conducted for users of banking, payment or funds transfer systems (have ex-employees been immediately removed from authorization lists upon termination)? Does access review of these platforms include:
   - Who has access to the platform?
   - Types of transactions permitted?
   - Value of transactions authorized?
   - Validation of segregation of duty of authorized personnel?
5. What is the dollar threshold for funds transfer transactions requiring dual authorization?
6. Are there automated alerts triggered by high-value transaction and high-volume transactions in a short period of time? (Does the bank have a policy to call an authorized signer for any check above a specified amount?)
7. With respect to funds transfer requests made by an employee or executive, do policies and procedures require:
   - The employee who received the request to verify the identity of the requesting employee and his/her authority to request such transfer, payment or delivery of funds (through a call-back to a telephone number on record)?
   - The employee receiving the request to obtain two approval signatures for such transfer, payment or delivery of funds?
8. With respect to funds transfer requests from a vendor, do policies and procedures require:
   - Confirmation that the vendor is in fact owed such requested amounts?
   - An employee to perform a call-back to a telephone number on file with an authorized vendor contact in advance of any change to that vendors account information (including payment information)?
   - The employee receiving the request to obtain two approval signatures for such transfer, payment or delivery of funds?
9. Are employees who are authorized to approve or execute funds transfer requests required to attest that they have read and understand the policies and procedures described in questions 7 and 8 above?
10. Is fraud awareness, detection and prevention training required for all employees at least annually? (Does your banking partner offer training and share policy information?) ■

Items of Importance, *continued from page 5*

BoSS will be hosting a webinar for the Air Permit Application Checklist on September 16, 2026 from 10:30 AM to 12:00 PM to introduce the new Air Permit Application Checklists and provide step-by-step guidance on how to complete them. To participate in the webinar, please provide your registration information (name, affiliation, and email) by September 11, 2026. Webinar participation instructions will be provided to all registered attendees prior to the event. This webinar is planned to be recorded.

Air Permit Application Checklists will become mandatory for all air permit applications submitted starting **October 16, 2026**. Any applications submitted after the Checklist becomes mandatory will be returned as deficient with no action taken. It is highly encouraged to begin using the Air Permit Application Checklists before they become mandatory. ■

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

2026 Fall Edition

Diocese of Trenton Risk Management Quarterly

Parishes, Schools, Cemeteries & Catholic Institutions

Inside this Issue:

Testimonial of Suitability for Priestly Ministry 1
Indoor Environments: Management of the Microbial Balance 2
Disaster Preparation: Hurricanes..... 3
Are You Covered? The Value of COIs..... 4
Boiler & Machinery Insurance..... 5
Items of Importance..... 5
Cyber Risk: What Parishes Need To Do..... 6
Crime & Fraud Prevention 7

Risk Management Key Contacts



Felix Tartaglia
Client Advocate



Mike Farrand
Sr. Principal

WTW Team
WTW
200 N. Warner Road, Suite 300
King of Prussia, PA 19406

Felix Tartaglia, Client Advocate
Tel: 610-254-7484
felix.tartaglia@wtwco.com

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

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

Claim Reporting
Lodestar
Tel: 800-482-9826; Fax: 856-727-3186

PMA Workers Comp Nurse Triage
CARE 24 Tel: 855-347-7334

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

Online Form: dotinsurance.org/forms/auto-forms

www.dotinsurance.org

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, Dept. of Construction & Property
Tel: 609-403-7195; Fax: 609-406-7412
spiroz@dioceseoftrenton.org