BPIC
A Member-Owned Insurance Company

Bishops' Plan Insurance Company
Safety and Loss Control News

Prepared by Gallagher Bassett | Risk Control Services *Early Spring 2026*

Inside this issue:

About BPIC

Bishops' Plan Insurance Company (BPIC) is a Vermont-domiciled, nonprofit captive and collaborative pooling effort among dioceses and archdioceses in the Kenedy Directory, established in 2003 to serve their risk financing and risk management needs. We are at 33 members spread across the country. BPIC offers a customizable structure and benefit offerings that allows each diocese to work with its broker and BPIC's underwriting team in designing its own program structure, using the unique all-lines capabilities of the program. BPIC is governed by its Board of Directors along with the spiritual guidance of its Episcopal Moderator and several third party partners service providers. BPIC offers a members' only website (password-protected) comprised of company financial information and risk management resources. Contact information is provided below, should you seek more information about BPIC or our website.

Phone:
Toll-Free: 877.325.BPIC (2742)

Email:
info@bpicmembers.org

Website:
www.bpicmembers.org

Preparing Facilities for Spring: A Post-Winter Checklist

As the winter frost begins to thaw and the promise of spring emerges, facilities must prepare for the seasonal transition. Winter weather can take a toll on buildings, grounds, and equipment, and addressing these issues early ensures that facilities remain safe, functional, and welcoming for parishioners and staff. Proper preparation also helps prevent costly repairs and ensures that the facilities are ready for the busy spring season, which often includes Easter celebrations, outdoor events, and community gatherings.

Here's a comprehensive guide to help dioceses prepare their facilities for spring following the winter season:

1. Inspect and Repair Building Exteriors

Winter weather can cause significant wear and tear on a facility's exterior. Start with a thorough inspection:

- **Roof**: Check for missing, damaged, or loose shingles, as well as signs of leaks or water damage. Address any issues promptly to prevent further damage during spring rains.
- **Gutters and Downspouts**: Clear out debris such as leaves, ice, and dirt to ensure proper drainage. Verify that downspouts direct water away from the building's foundation.
- **Siding and Walls**: Look for cracks, peeling paint, or other damage caused by freezing temperatures or moisture.
- **Windows and Doors**: Inspect seals and weatherstripping to ensure they remain intact and energy-efficient.

2. Assess and Maintain Landscaping

Winter can leave outdoor spaces looking neglected. Prepare the grounds for spring by:

- **Clearing Debris**: Remove fallen branches, leaves, and other debris from lawns, gardens, and walkways.
- **Pruning and Trimming**: Cut back dead or damaged branches from trees and shrubs to promote healthy growth and prevent hazards.
- **Lawn Care**: Aerate and fertilize the lawn to encourage new growth. Reseed any bare patches caused by snow or ice.
- **Irrigation Systems**: Test sprinkler systems to ensure they are functioning properly and repair any leaks or damage caused by freezing temperatures.

3. Inspect Parking Lots and Walkways

Snow, ice, and salt can cause cracks and potholes in paved surfaces. Address these issues to ensure safety and accessibility:

- **Repair Potholes**: Fill in potholes and cracks in parking lots and driveways to prevent further deterioration.
- **Clean Walkways**: Power wash sidewalks and entryways to remove salt residue and grime.
- **Repaint Markings**: Refresh faded parking lot lines, handicap spaces, and directional arrows.

(Continued on page 2)

Preparing Facilities for Spring: A Post-Winter Checklist

(Continued from page 1)

4. Service HVAC Systems

As temperatures rise, it's essential to ensure that heating, ventilation, and air conditioning (HVAC) systems are ready for the warmer months:

- **Switch to Cooling Mode**: Test air conditioning units to ensure they are functioning properly.
- **Replace Filters**: Clean or replace HVAC filters to improve air quality and system efficiency.
- **Schedule Maintenance**: Have a professional inspect and service the HVAC system to address any issues before peak usage.

5. Check Plumbing Systems

Freezing temperatures can cause pipes to crack or burst. Inspect plumbing systems for any signs of damage:

- **Inspect Pipes**: Look for leaks, cracks, or corrosion in exposed pipes.
- **Test Outdoor Faucets**: Turn on outdoor spigots to ensure water flows freely and check for leaks.
- **Check Water Heaters**: Ensure water heaters are functioning properly and adjust the temperature if necessary for warmer weather.

6. Deep Clean Interior Spaces

Spring is the perfect time for a thorough cleaning of the facility's interior:

- **Sanitize Common Areas**: Clean and disinfect high-touch surfaces, such as door handles, light switches, and pews.
- **Wash Windows**: Remove dirt and grime from windows to let in more natural light.
- **Clean Carpets and Floors**: Deep clean carpets and polish hard floors to remove winter dirt and salt residue.
- **Declutter Storage Areas**: Organize and clean storage spaces to prepare for upcoming events and activities.

7. Test Safety and Security Systems

Ensure that all safety and security measures are in place and functioning:

- **Fire Safety**: Test smoke detectors, fire alarms, and sprinkler systems. Replace batteries and schedule inspections if needed.
- **Emergency Exits**: Verify that all emergency exits are clear and properly marked.
- **Security Systems**: Test security cameras, alarms, and access control systems to ensure they are operational.

8. Plan for Spring Events

Spring is a busy time for diocesan organizations, with events such as Easter services, outdoor gatherings, and community outreach programs. Prepare by:

- **Scheduling Maintenance**: Complete all necessary repairs and cleaning before major events.
- **Setting Up Outdoor Spaces**: Arrange seating, tents, and decorations for outdoor services or activities.
- **Stocking Supplies**: Ensure that cleaning supplies, hand sanitizers, and other essentials are well-stocked.

9. Communicate with Staff and Volunteers

Engage staff and volunteers in the preparation process:

- **Assign Tasks**: Create a checklist of tasks and delegate responsibilities to ensure everything is completed on time.
- **Provide Training**: Offer guidance on proper cleaning, maintenance, and safety procedures.
- **Encourage Feedback**: Ask for input from staff and volunteers on areas that may need attention.

10. Budget for Repairs and Upgrades

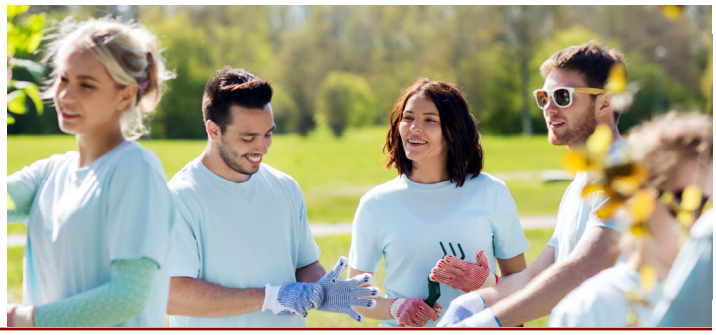
Spring maintenance is an opportunity to address not only immediate repairs but also long-term improvements:

- **Evaluate Needs**: Assess the condition of the facility and prioritize projects based on urgency and budget.
- **Plan for Upgrades**: Consider energy-efficient upgrades, such as LED lighting or solar panels, to reduce utility costs and environmental impact.

Conclusion

Preparing diocesan facilities for spring is an essential part of stewardship, ensuring that buildings and grounds remain safe, welcoming, and functional for the community. By addressing winter-related damage, performing routine maintenance, and planning for upcoming events, dioceses can create a vibrant and inviting environment for parishioners and visitors alike. With a little effort and organization, your facilities will be ready to embrace the beauty and renewal of the spring season.

Return to "Inside This Issue" index.



Training Staff on Cybersecurity

Training staff on cybersecurity is one of the most effective ways to protect your organization from cyber threats. By equipping employees and volunteers with the knowledge and skills to recognize and respond to potential risks, you can create a strong first line of defense. Consider the following practical actions to train staff on cybersecurity.

Conduct Regular Cybersecurity Awareness Training

- **Frequency**: Schedule training sessions at least twice a year or whenever there are significant updates to cybersecurity protocols.
- **Content**: Cover topics such as recognizing phishing emails, creating strong passwords, safe internet browsing, and handling sensitive data.
- **Interactive Learning**: Use quizzes, role-playing scenarios, and real-life examples to make the training engaging and memorable.

Teach Staff to Recognize Common Cyber Threats

- **Phishing Emails**: Show examples of fake emails and teach staff how to spot red flags like misspellings, suspicious links, or urgent requests for personal information.
- **Social Engineering**: Explain how attackers may use manipulation tactics to gain access to sensitive information.
- **Malware and Ransomware**: Educate staff on how malicious software can infect systems and how to avoid downloading suspicious files or clicking on unknown links.

Implement Simulated Cybersecurity Drills

- Conduct mock phishing campaigns to test staff's ability to identify and report suspicious emails.
- Use these drills as learning opportunities to reinforce best practices and address any gaps in knowledge.

Provide Clear Policies and Guidelines

- Develop and distribute a cybersecurity policy that outlines acceptable use of technology, password requirements, and procedures for reporting incidents.

Conduct mock phishing campaigns to test staff's ability to identify and report suspicious emails.

- Ensure staff understand the importance of adhering to these policies and the consequences of non-compliance.

Promote the Use of Strong Passwords and Multi-Factor Authentication (MFA)

- Teach staff how to create strong, unique passwords using a mix of letters, numbers, and symbols.
- Encourage the use of password managers to securely store and manage passwords.
- Train staff on how to set up and use MFA for an added layer of security.

Highlight the Importance of Data Protection

- Explain the significance of safeguarding sensitive information, such as parishioner records, financial data, and internal communications.
- Train staff on secure file-sharing practices and the importance of encrypting sensitive data.

Provide Ongoing Resources and Updates

- Share cybersecurity tips and updates through newsletters, emails, or bulletin boards.
- Offer access to online courses, webinars, or workshops on cybersecurity topics.

(Continued on page 4)

Training Staff on Cybersecurity

(Continued from page 3)

- Keep staff informed about emerging threats and how to respond to them.

Appoint a Cybersecurity Champion

- Designate a staff member or team to serve as the go-to resource for cybersecurity questions and concerns.
- This person can also monitor compliance, provide additional training, and stay updated on the latest cybersecurity trends.

Encourage a "Report It" Culture

- Train staff to report suspicious emails, links, or activities immediately, without fear of blame.
- Create a simple and clear process for reporting potential cybersecurity incidents.

Partner with Cybersecurity Experts

- Bring in external cybersecurity professionals to conduct workshops or provide specialized training.
- Consider partnering with organizations that offer cybersecurity training tailored to faith-based or nonprofit organizations.

Evaluate and Improve Training Programs

- Collect feedback from staff after each training session to identify areas for improvement.
- Regularly assess the effectiveness of your training program through surveys, tests, or simulated attacks.

Lead by Example

- Leadership should model good cybersecurity practices, such as using strong passwords, reporting suspicious activity, and following organizational policies.
- When staff see leaders prioritizing cybersecurity, they are more likely to take it seriously.

Conclusion

Training staff on cybersecurity is an ongoing process that requires commitment and consistency. By investing in education and fostering a culture of vigilance, your diocesan organization can significantly reduce the risk of cyberattacks. Remember, cybersecurity is a shared responsibility, and every staff member plays a vital role in protecting the organization and its community. Together, we can build a safer digital environment for all.

Return to "Inside This Issue" index.

Common Cyber Threats

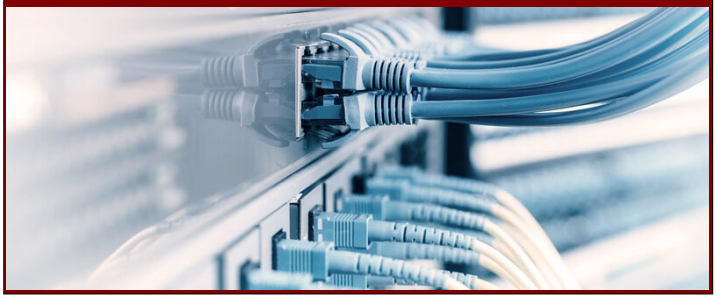
Phishing Attacks
Fraudulent emails or messages designed to trick individuals into revealing sensitive information, such as passwords or financial details.

Ransomware
Malicious software that locks access to systems or data until a ransom is paid.

Data Breaches
Unauthorized access to sensitive information, often resulting in the exposure of personal or financial data.

Social Engineering
Manipulative tactics used by cybercriminals to deceive individuals into divulging confidential information.

Weak Passwords
Easily guessed or reused passwords that make it simple for hackers to gain access to systems.



BPIC
A Member-Owned Insurance Company

39009