

# the Municipal RISK MANAGER

SUMMER 2021

A PUBLICATION OF THE MAINE MUNICIPAL ASSOCIATION

## Ransomware Alert: You must protect yourself

Ransomware is a form of malware designed to encrypt files on your computers, rendering any files and the systems that rely on them, unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among the state, local government entities, and critical infrastructure organizations. Ransomware incidents can severely impact an organizations leaving them without the data they need to operate and deliver critical services. The monetary value of ransom demands has also increased, with some demands exceeding \$1 million. Ransomware incidents have become more destructive and impactful in nature and scope. The key is to be prepared.

### Ransomware Prevention Best Practices

- 1) Ensure antivirus and anti-malware software and signatures are up to date.
- 2) Implement a cybersecurity user awareness and training program that includes guidance on how to identify and report suspicious activity (e.g., phishing) or incidents.
- 3) Conduct organization-wide phishing tests to gauge user awareness and reinforce the importance of identifying potentially malicious emails.
- 4) Train staff to question the validity of all emails and to verify emails that they find are questionable.
- 5) Use strong passwords and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts. Password managers can help you develop and manage secure passwords.
- 6) It is critical to maintain offline, encrypted backups of data, and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups are maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.
- 7) Retain backup hardware to rebuild systems in the event rebuilding the primary system is not preferred. Hardware that is newer or older than the primary system can present installation or compatibility hurdles when rebuilding from images.
- 8) Be Prepared



For further assistance and access to governmental resources, please contact the Cybersecurity & Infrastructure Security Agency at <https://www.cisa.gov/cybersecurity> 

### InforME (Information Resource of Maine)

The Internet gateway to interact with government electronically

Through InforME, all municipalities have access to a free subscriber account that allows municipal staff to interact with state government. With a subscriber account, municipal staff can search vehicle information including driver, registration and title records, corporate information including corporate records search, and, in some cases, no cost Public Criminal Records. You can take comfort in knowing that the NIC Maine staff is a phone call or email away if you have questions about any of these services. MMA Risk Management services encourages you to use this service when obtaining annual MVR checks and/or background checks for new hires.

To learn more about NIC Maine, InforME, and the services available to your municipality, please visit [www.maine.gov/informe](http://www.maine.gov/informe) or contact [municipalservices@informe.org](mailto:municipalservices@informe.org). 

# MMA RISK MANAGEMENT SERVICES

## Announces new *grant opportunities* exclusive to Property & Casualty Pool Members

### RISK REDUCTION GRANT PROGRAM



Risk Management Service is pleased to announce the new Risk Reduction Grant Program (RRGP) for members of the Property & Casualty Pool. The RRGF is crafted to assist members in the reduction of liability and property exposures and to aid members in their efforts of applying effective risk management and loss control techniques.

- Members are eligible for 100% reimbursement, up to \$3,000.
- Grants must be submitted by September 15<sup>th</sup> (only one grant submission per year).
- Submissions must demonstrate a proactive approach to mitigate property & liability losses.

#### Eligible Grant Purchase Suggestions

- Plow Wing Lasers
- Water Alarms
- Backup Cameras
- Lightning Protection
- Generators
- Financial Controls Training
- Human Resources Training
- Sewer Line Inspection Tools
- Computer Surge Protections
- Security and Emergency Lighting
- Automatic Water Shut Offs
- Side View Cameras
- Protective Barriers
- Backing Proximity Alarms

### MAINE LAW ENFORCEMENT ACCREDITATION GRANT PROGRAM



The Maine Law Enforcement Accreditation Grant Program is designed to encourage and support MMA Property & Casualty Pool Member Law Enforcement Agencies to improve policy management and officer training with the potential of achieving certification in the Maine Law Enforcement Accreditation Program (MLEAP).

The grant will reimburse up to \$5,000 (\$2,500 allowed upon award and proof of contract with outside agency, and \$2,500 at end of award period with requirements met).

- Member's with Law Enforcement Agencies must be a current Member of the Pool on or after July 1, 2021.
- Grant requests must be submitted no later than September 1, 2021.
- Up to 10 Law Enforcement Agencies will receive this award.



*\*The MMA Property & Casualty Pool is also offering Agencies that are MLEAP certified up to 15% credit on the annual Police Professional Liability contribution.*

For more information contact MMA Risk Management Services:

Email: [safetygrants@memun.org](mailto:safetygrants@memun.org) | Phone: (800) 590-5583 | Web: [www.memun.org](http://www.memun.org)

# RMS Online University & Safety Management System

## Achieving Your Goals Together

MMA Risk Management Services is committed to providing members of our Workers' Compensation Fund and Property & Casualty Pool with the highest quality educational resources. The Online University & Safety Management System is provided as a value added service at no cost to you.

The Online University is an educational portal which grants your staff access to more than 225 health, safety, and liability prevention courses at your fingertips.

Did you also know that the Online University & Safety Management System grants your entity the ability to:

- Organize training by departments
- Assign courses with due dates via an email format
- Upload 90 uniquely named Operating Procedures (policies) with an automatic acknowledgment statement
- Upload up to 6 entity wide Personnel Policies
- Assign Policies and Standard Operating Procedures just like the training modules.
- Retain documentation, training, Policies, and acknowledgments all in one place.

City of Augusta Police Chief Jared Mills shared the following about the Online University & Safety Management System:

“MMA has been instrumental with enabling our department to achieve the MLEAP. The software, provided free of charge by MMA, allows us to store our policies and track our changes while allowing us to upload trainings for all employees to take online. The services is convenient and has made us much more efficient as an agency in the realm of policies, procedure, and training.”

We are pleased to offer members of our Workers' Compensation Fund and Property & Casualty Pool with this powerful safety and administrative tool. If you would like more information or to setup and explore the Online University & Safety Management System, please contact us by email at [rmslosscontrol@memun.org](mailto:rmslosscontrol@memun.org) or by phone at 1-800-590-5583. 🏠

## Benefits of Financial Controls

Unfortunately, embezzlements occur in communities and districts of all sizes. As a result, it is of great importance to protect your entity, community, and staff from such events by establishing a positive work environment and by instituting sound internal controls.

One of the primary goals of internal controls is to create a separation of accountability and custodianship; i.e. to assure that municipal officials or employees who have responsibility for keeping records of municipal finances are not also the same individuals who have custody of its assets. In the accounting world, the principle of separation of accountability and custodianship dictates that a person who handles bank deposits or keeps cash books, should not also receive bank statements or make bank reconciliations.

Internal control is a process is designed to provide reasonable assurance that the following objectives are performed:

- Effectiveness and efficiency of operations
- Protect the entity and staff
- Reliability of financial reporting
- Compliance with applicable guidelines and standards.

Generally internal controls are achieved through education and the institution of written policies:

- a. Education.** Financial policies help educate those municipal officials who may not have a background in government financial management. Written financial policies can help inform officials of good financial practices, making it more likely that these good practices will be implemented and followed.
- b. Prevention and Resolution of Conflicts.** Financial policies may help prevent and resolve conflicts in local government. The key to effectively navigating this complexity is effective communication and cooperation among local officials, management, and staff. Financial policies can clarify both the responsibilities of local officials and lines of authority. The process of adopting written financial policies can also afford local officials the opportunity to engage in communication and develop common financial goals for their municipalities. Active participation in the process makes it more likely that all the parties involved in financial decision-

making will abide by a common set of rules.

- c. Continuity and Efficiency.** Financial policies can aid in the continuity and efficiency in the municipality's financial operations. Elected officials may serve relatively short terms and new officials may not be experienced with financial issues. Instituted financial policies can eliminate the need to reinvent responses to recurring situations, thereby increasing efficiency, by standardizing operations and retaining institutional knowledge built up over the years.
- d. Transparency and Confidence.** The adoption of financial policies can foster confidence in local government by increasing transparency, accountability, and consistency in municipal decision-making. The policies can help local officials make more informed decisions about providing services, acquiring and managing capital assets, safeguarding a municipality's resources, and promoting financial stewardship, all of which helps to support your entity and community. 🏠

# The Compensation Corner

## The Importance of the Selection Process

Controlling workers' compensation costs actually starts before the hiring begins. By developing and utilizing sound hiring and training methodologies, you can create a positive selection process that is designed to foster a safe and healthy work environment. Well written job descriptions are an essential tool in the employee selection process. Not only will a good job description help you recruit the right employees, a job description can prevent injuries by ensuring that an applicant is qualified and capable to perform the job, while preventing misunderstandings about performance expectations. It is recommended that you detail the physical requirements and working conditions within the job description.

## Orientation and Training

Whether lifting files, exiting a vehicles, general housekeeping, collecting trash, firefighting or pursuing a fleeing suspect, everyone needs training and to be reminded of their own safety and the safety of others. Such safety awareness begins with a culture of safety in the workplace. It is critically important for management to be a positive example of the safety culture and to encourage employee safety. Provide trainings, safety resources, and positive reinforcement through visual and verbal reminders. The goal is to develop a safety culture.

The Workers' Compensation Fund (WC Fund) provide resources to help members address potential loss exposures of local governmental entities. This includes on-site visits by experienced Loss Control staff that can provided hazard identification, training, and education. The Fund also offers Best Practices, Grant Programs, Safety Shorts, an Online University, and more all located at:

<https://www.memun.org/Insurance-Services/Risk-Management-Services>

Please take advantage of these free services to improve your own programs and foster a safe workplace. 🏠



## The Municipal Risk Manager

The Municipal Risk Manager is published seasonally to inform you of developments in municipal risk management which may be of interest to you in your daily business activities. The information in these articles is general in nature and should not be considered advice for any specific risk management or legal question; you should consult with legal counsel or other qualified professional of your own choice.

**Publisher:** Risk Management Services

**Editor:** Marcus Ballou

**Layout Designer:** Sue Bourdon

P.O. Box 9109, Augusta, ME 04332 • 1-800-590-5583 or (207) 626-5583

## FREQUENTLY ASKED QUESTIONS

### What are the Top 4 Cyber-Attacks Now?

Cyber-attacks are on the rise and understanding how they work and educating yourself and your staff is a key in prevention.

**MALWARE** - It is any malicious form of software designed to harm, monitor, or control a computer system

- Malware performs a malicious function such as stealing, deleting, or encrypting data, monitoring a computer users' activity or hijacks core computing functions.
- Common malware includes worms, viruses, Trojan horses, and spyware.
- Malware is commonly distributed through physical hard drives, USB external drives, or internet downloads.

**PHISHING** - Phishing is when a hacker uses a false identity/email to trick someone into: providing sensitive information, clicking on a link to downloading malware, or visiting a site containing malware.

- The most common phishing attack targets people through email. An attacker creates an email looking like it comes from a trusted source, like your local bank or the IRS, and the email asks you to visit a website or click a link, which in turn, unknowingly infects your computer.

**RANSOMWARE** - Ransomware is a form of malware designed to encrypt files on a system or device, rendering them unusable. Hackers demand ransom in exchange for decryption.

- This type of malware can be spread through phishing emails or visiting an unknowingly infected website.
- Ransomware can be devastating if proper data backups are not in place and tested often.
- BEWARE: Not all hackers will release/return/unlock data files and systems once the ransom is paid!

**SOCIAL ENGINEERING ATTACKS** - Attacks use human interaction (social skills) to obtain or compromise information about an organization or its computer systems.

- One of the most common tactics is trick someone into thinking they are helping someone in need.
- A hacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity.
- The hacker may also ask questions to piece together enough information to infiltrate an organization's network. 🏠

MMA Risk Management Services welcomes its newest member to the **PROPERTY & CASUALTY POOL**

## Town of New Sharon

*We thank our dedicated members for their partnership.*