MCIT BULLETIN

A PUBLICATION OF MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST

MCIT MISSION:

Providing Minnesota counties and associated members cost-effective coverage with comprehensive and quality risk management services.

VOL. 39, No. 3 | May/June 2026

More Flexibility Brings New Challenges for Remote Board Meetings

In 2025, the Minnesota Open Meeting Law was updated to allow a board member regularly to attend and participate in board meetings from a remote location that is not open to the public.

Although public bodies must still provide notice of the remote meeting, the meeting notice no longer must include details about remote locations.

Instead, the notice must only provide notice of the regular meeting location and state that members may be participating in the meeting by interactive technology.

These changes have raised some interesting questions related to posting and public access to remote meetings.

Posting the Remote Participation Notice

Other than the contents of the notice, the revised Section 13D.02, subd. 4 on remote meetings is vague on how the notice of remote participation should be given.

From a risk management standpoint, the prudent course of action is to continue posting the notice about remote participation using the special meeting notice time frames and the method. A special meeting notice generally requires posting a written notice on the entity's principal bulletin board or usual meeting room door three days before the meeting.

This is based on the premise that the place of the regular meeting is different when a board member attends remotely. Under the Open Meeting Law, when a public body decides to hold a regular meeting at a time or place different from the time or place stated in its schedule of regular meetings, it must give the same notice of the meeting as for a special meeting.

To make this process easier for staff, the Minnesota Department of Administration's Data Practices Office (DPO), which is tasked with providing guidance about the Open Meeting Law, suggests that boards establish a procedure that requires board members to notify the chair or applicable county staff at least three days in advance of a meeting about whether they will attend remotely.

Providing the Public Remote Access

Whenever interactive technology is used to conduct a meeting, a public body must allow the public to monitor the meeting electronically from a remote location to the extent it is practical.

Does the entity still need to provide the public the ability to monitor the meeting remotely if the board member who intended to be remote shows up at the regular meeting location instead?

When posed this question, the DPO noted that in general, there is no requirement under the Open Meeting Law to provide the public with remote access

continued on page 7

COMING EVENTS

May 8
MCIT BUILDING, ST. PAUL
9 A.M.: Board of Directors meeting
1 P.M.: Claims Committee meeting

May 27-28
ST. CLOUD AREA
9:30 A.M.: How to Conduct an Employee Investigation Seminar

June 12
MCIT BUILDING, ST. PAUL
9 A.M.: Board of Directors meeting
1 P.M.: Claims Committee meeting

June 25
ST. CLOUD
9 A.M.: Practical Leadership Seminar

In-person Training for Managers

Register early at *MCIT.org*. Limited to first 45 people!

When people leaders understand the expectations of their role, they are able to supervise in a way that fosters healthy working relationships with each employee that reports to them. This, in turn, builds positive organizational culture and avoids destructive behaviors in the workplace. Unskilled supervision, on the other hand, can create organizational cultures that are ineffective at best and cause harm at worst.

"Practical Leadership: Cultivating Thriving Supervisory Relationships" June 25 at Holiday Inn, St. Cloud is a highly interactive in-person training that provides participants with immediately implementable tools and strategies.

What Participants Learn

By the end of the training, attendees will:

- Better understand the competencies and required skills of the supervisor role and have improved confidence in implementing the role
- Be aware of the challenges to collaborative leadership with the vertical power dynamic created by hierarchical structures, and will connect this to specific strategies learned in the training
- Cultivate self-awareness and accountability for fostering positive organizational culture and avoiding destructive behaviors in the workplace
- Have increased comfort to hold a range of conversations, including corrective and developmental feedback about both work and behavioral performance
- Learn strategies for helping employees solve their own challenges
- Understand the fundamental components of coaching and participate in experiential learning exercises to practice listening and inquiry
- Know the supervisor continuum and the critical skills of supervision (structuring, selecting, onboarding, goal setting, guiding and supporting), including how to set expectations, give recognition and hold performance conversations

Who Should Attend?

This seminar is for those who are in an employee management role, such as a manager or supervisor. The training is designed for both those who are new to formal supervision and for more seasoned leaders. Space is limited to 45 attendees.

Presented by Lisa Negstad, Consultant

Lisa Negstad (Negstad Consulting) is a trainer, consultant, coach and facilitator, specializing in leadership, organizational culture and networks. Negstad helps managers become better in their roles and assists groups to collaborate and improve their shared leadership skills. Prior to starting Negstad Consulting, Negstad held senior leadership positions in several nonprofit organizations. She has a master's degree in business administration from Yale University and holds a bachelor of arts in psychology.

Register at *MCIT.org*

- Complete the registration form on the Practical Leadership page at *MCIT.org/Events*. Payment for the registration fee is required by credit card at the time of registration.
- $90 per person for MCIT member organizations.*

More information is available at *MCIT.org/Events*.

*Cancelation policy: Seminar cancellations received by June 10, 2026, will receive a full refund. No refund will be issued for cancellations received after that date.

In-person Training for Human Resources

Register early at *MCIT.org*. Limited to first 34 people!

Allegations of employee misconduct can run the gamut from an inappropriate comment to the exceptionally serious and require the employer to respond appropriately. The investigation must be fair, thorough and comply with the law. This fast-paced, two-day seminar helps members meet these requirements.

The training is designed for human resources professionals who want to conduct their own investigations.

What Participants Learn

Attendees learn strategies for approaching topical areas, such as allegations of harassment, workplace bullying, computer misuse and theft; the impact various laws have on an investigation; and techniques to manage media and public scrutiny of an investigation.

Learn More

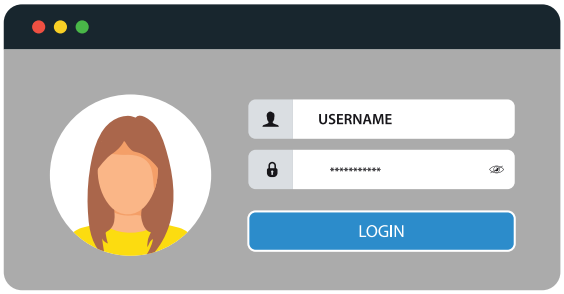
More information is available at *MCIT.org/events*. Members who have questions about this event should contact MCIT Communications Manager Heather Larson-Blakestad at *hblakestad@mcit.org* or **866.547.6516**.

*MCIT cancelation policy: Seminar cancellations received by May 12, 2026, will receive a full refund. No refund will be issued for cancellations received after this deadline.

CYBERSECURITY TIP

Deactivate Unnecessary Credentials to Shut Down Security Vulnerability

One of the fundamentals of securing an organization's systems and facilities is following the principle of least privilege. This means limiting an individual's access to the organization's devices, programs, information and facilities to the minimum they need to carry out their job duties. Adhering to this is easy if employees never leave the organization nor change roles.



Obviously, the reality is that employees do leave employers, change roles and take extended leave. Keeping the list of active employees and the systems to which they have access up to date requires attention and redundancies. If unnecessary credentials are left active, the system is vulnerable to malicious access from former employees and threat actors.

This circumstance has unfortunately been used to gain access to an MCIT member's network. It resulted in MCIT's largest cyber claim to date in terms of dollars: $1.3 million in total, $430,000 of which was covered by MCIT, leaving the county responsible for $850,000.

Steps to Keep Access Current

When permissions are set up, they should be time bound where appropriate with automatic expiration dates, especially for temporary roles, contractors/vendors or elevated permissions. Managers should maintain a list of permissions for each of their team members. And managers should regularly review access rights for their direct reports and make appropriate adjustments as necessary.

As part of the organization's off-boarding process, Human Resources or the individual's manager should be required to alert IT to deactivate the individual's access to programs, systems and devices. The manager's lists of permissions should make this easy.

For employees who are on extended leave (not just a few weeks of vacation or medical leave), an employer may want to deactivate credentials to limit the threat landscape. The accounts can be re-established when the employee returns to active employment.

When an individual moves to a different position within the organization, the manager should identify which devices, programs and systems the employee needs and ask IT to activate new accounts and deactivate those that are no longer pertinent for the individual.

Third-party contractors should be subject to the same access controls with clearly defined start and end dates. An organization should assign an individual regularly to review contractors' permissions.

continued on page 7

Stay Vigilant for Phishing Attacks, Educate Staff

Phishing is one of the most significant contributing factors of cyber claims for MCIT members. In 2025, 26 percent of all cyber claim expenses came from those involving phishing. The most common vector for the attacks was through email, but members have had claims via phone calls. Text messages are also used to deploy phishing attacks.

Phishing scams aim to steal sensitive information, deploy malware or commit financial fraud (misdirected payment fraud).

The messages typically mimic known vendors, business partners or employees, making it easy to fall victim. However a few safeguards and keeping a vigilant eye for fraud can help prevent loss. MCIT members are encouraged to remind employees regularly about how to identify phishing and steps they can take to reduce the likelihood of attack.

Spotting and Avoiding a Scam

These best practices can help members spot fraudulent requests before releasing funds, sharing log in credentials or providing sensitive information.

Verify that the request is coming from the purported contact. Employees should ask themselves:

- Is the email account name correct? Does it match what is known to be legitimate?
- Is the email address correct? Is the @ symbol in the correct place? Is the domain name or extension correct (e.g., ".gov" instead of ".com")?

Be wary of requests for quick response or actions. Often threat actors use urgency to get people to act without thinking. Remind employees that it is always better to take a few minutes to verify that the request is coming from a verified partner and makes sense. Most requests from legitimate local government partners do not require immediate action.

Scrutinize messages that are "click bait" (those that entice curiosity) or are too good/bad to be true. This is a classic trick of phishing scams to get people to open messages and click on links. As such, it is best that employees assume that these messages are scams.

Before clicking on links in messages, especially those that are unexpected or unsolicited, employees should **determine if the actual URL is legitimate.** Staff should hover the mouse over the link without clicking to see where the link actually would take them. If it is not where it is claiming to go, they should not click it.

Look for signs a video, image or audio clip is a deep fake, such as inconsistent shadows, unnatural speech patterns, overly smooth skin on face, etc. Generative artificial intelligence makes it easy for threat actors to create social engineering attacks that are hard to detect. These attacks are significantly more personalized, have fewer errors and may employ convincing deep fake images, audio clips and videos.

Tips specifically to reduce the chances of falling victim to misdirected payment fraud scams include:

- Require that staff **verify payment changes before authorizing a change.** Best practice would be to call the vendor or payee using a known, previously verified phone number. Another option is personally to visit the payee.
- **Verification using email is not advised**, but if used, start a new message to the vendor or payee and, again, use a known, previously verified email address for the vendor or payee. This should prevent the message from delivering to the perpetrators of the theft attempt.

REDUCE THREAT LANDSCAPE: TREAT EMAIL AS PASS THROUGH, NOT STORAGE SYSTEM

When email, which is a vulnerable system regardless of technical security tools, is used for long-term storage, threat actors potentially have access to years of data that can be mined for sensitive and private information they can exploit for various nefarious purposes.

To reduce the amount of information that is vulnerable to threat actors through email, employees should update their practices to save necessary messages, information or attachments in secure locations outside of the email system. Secure locations could be a document management service, customer relationship management service or private network drives.

Once securely saved outside of the email system, employees should be instructed to remove the original message from the email account to avoid unnecessary duplication. This includes all duplicates such as those saved in the inbox, sent, deleted or other folders within the email system.

- Request that the **member's bank** call a specific contact at the member to **verify a transfer of funds outside of the United States** before processing the release of funds. Most local governments do not send money internationally, but misdirected payment fraud is often perpetrated by those outside of the U.S.
- **Red flag Green Dot Bank in email systems.** This online bank is frequently used in misdirected payment fraud scams.
- **Require the vendor or payee to complete and sign a new direct deposit or ACH form** to provide documentation if an issue arises.
- **Limit** the number of **individuals who can make changes** to a vendor or payee's direct deposit or ACH information and train them on policies and procedures.
- **Investigate unusual requests**, ask questions and verify the authenticity of the request.

Build Employee Awareness

MCIT offers members four email security awareness digital images to help build understanding among employees about how to spot scams delivered through email. Members can download these at *MCIT.org/resources*.

The digital images can be used anywhere a jpeg can be placed. Ideas for use:

- Paste images into emails sent to staff
- Post to intranet landing page
- Print and hang as small posters throughout the facility
- Publish in the employee newsletter
- Display on screen/monitor to kick off a staff or team meeting
- Set as the lock screen image for workstation computers

Quick Takes on Data Security are mini training scripts for supervisors to use with their teams to remind employees about how they can strengthen the organization's data security through their own simple actions. Scripts and handouts are available at no cost at *MCIT.org/resources* and cover:

- Phishing and social engineering
- Business email compromise and misdirected payment fraud
- Data storage and destruction
- Password security
- Mobile device security
- Safe internet browsing

MCIT risk management consultant Richard Miehe can assist members with their cybersecurity risk management efforts. He has a special focus in this area. Reach Miehe at **866.547.6516** or *rmiehe@mcit.org*.

Report Known or Suspected Incidents Immediately

Members should report a known or suspected cyberincident to MCIT immediately. The sooner MCIT can begin investigating the situation, the more it can be minimized. Members should submit claims through the online member portal at *MCIT.org*.

Drive Wisely

Minnesota's Basic Speed Law

With road construction season upon us, it is worthwhile to review fundamentals of safe driving. The Minnesota Basic Speed Law is one such fundamental.

Per Minnesota State Statute Section 169.14, drivers must not drive faster than what is "reasonable and prudent under the conditions."

Road conditions and/or other circumstances may supersede speed limits; therefore, a driver could receive a citation for driving the posted speed limit in the following types of situations.

- **Weather:** There is snow, ice, sleet or heavy rain
- **Visibility:** There is dense fog or smoke
- **Hazards:** When approaching a hill crest, curve or narrow bridge
- **Pedestrians:** In areas with high foot traffic or children

Construction zones also require careful assessment of conditions and often necessitate alterations of speed. If construction workers are present and a lane is closed, the speed limit on roads posted at 50 mph or higher are automatically reduced to 45 mph (speeding in a work zone carries a minimum fine of $300).

Following signs, traffic control devices/flaggers or other notifications is vital, but the Basic Speed Law remains relevant and may require driving even slower than posted in construction zones.

Although it is tempting to speed, it is always important to remember the increased risks that are inherent with speeding and that driving within the conditions is ultimately the first and most basic law regarding speed.

SPEED LIMITS WHEN SIGNS ARE NOT PRESENT

Although the Basic Speed Law still applies, Minnesota law assumes the following speed limits per road type if signs are not present and/or visible.

- Alleys, manufactured home parks: 10 mph
- Urban districts (city streets): 30 mph
- Residential roadways (specific zones): 25 mph
- Rural interstate highways: 70 mph
- Urban interstate highways: 65 mph
- Other roads (default/unmarked): 55 mph

Prevent E. Coli, Food-borne, Other Illnesses at County Fairs

Two of the more popular pastimes at the county fair are eating fair food and seeing the animals. These and other activities do not come without risks. Outbreaks of various illnesses serve as a reminder that attendees may get more than they bargained for at the county fair.

- At least 11 people were infected with E. coli at the Minnesota State Fair after contact with animals while visiting the Miracle of Birth exhibit in 2019. Six people were hospitalized.
- Romaine lettuce was the likely cause of a nationwide E. coli outbreak in 2018 when 210 Americans were sickened and five deaths were reported as a result, including two in Minnesota.
- 157 cases of E. coli were linked to a Minnesota traveling petting zoo in 2014.

Take Illnesses Seriously

E. coli is a common type of bacteria that can spread relatively easily. Illness can occur after consuming contaminated food, including unpasteurized milk and apple cider, water that has not been disinfected, undercooked meats, and contaminated fruits and vegetables.

E. coli can also spread by contact with animals or animal environments. Although the major source of human illness is cattle, other sources include sheep, goats, birds, deer and pigs. In addition, the illness can occur after eating food prepared by people who did not wash their hands after using the toilet or coming into contact with bacteria from other sources.

Numerous other sources of food-borne illnesses, such as cryptosporidiosis and salmonellosis are common in the United States and can also be an area of concern for county fairs. In some states salmonellosis is the most commonly reported form of intestinal disease and is one of the most commonly reported bacterial food-borne illnesses.

Coverage and Outbreaks

It is important that MCIT members understand that MCIT liability coverage may not apply to claims related to contraction of E. coli and other communicable diseases. Claims arising from disease are excluded under the fungus, communicable disease and/or pollution exclusions to liability coverage in the MCIT Coverage Document.

Members may consider seeking special event coverage from the private insurance market that addresses these risks. MCIT risk management consultants can provide more information about this to members individually. They can be reached at **866.547.6516**.

Prevent Spread of Disease

To protect fairgoers and member entities, MCIT members should take measures to prevent the spread of these illnesses and establish guidelines and procedures for food vendors, corn-filled play areas for children, petting zoos and other sources of animal contact at the fair.

Risk management recommendations, including key suggestions from the National Association of State Public Health Veterinarians' report, "Compendium of Measures to Prevent Disease Associated with Animals in Public Settings," include:

- Establish protective guidelines and procedures for vendors and fairgoers for handling food and contact with animals.
- Ensure contractors and vendors agree to protect, defend and hold the member organization, as appropriate, harmless from any and all claims or liability arising out of their operations.
- Require food vendors to provide a certificate of liability coverage that includes product liability coverage (for products consumed both on and off premises) with recommended limits of $500,000 per claimant and $1.5 million per occurrence. This coverage should include an additional insured endorsement, naming the member entity, as appropriate, as an additional insured.
- Post signs warning visitors that they are entering animal areas.
- Educate visitors not to eat, drink, smoke, use bottles or pacifiers, or put hands in mouths when in animal areas or corn-filled play features.
- Establish transition spaces at animal area exits with adequate hand washing facilities for all, and follow Americans with Disabilities Act guidelines for accessibility.
- Post signs or otherwise instruct visitors to wash hands when exiting animal areas or corn-filled play features.

Helpful Resources

The "Agricultural Society Loss Prevention Best Practices Guide" provides risk management recommendations for animal-borne and food-borne illnesses at county fairs in addition to many other concerns. This publication is available at *MCIT.org/resources* for no cost.

The Minnesota Department of Health provides posters and other resources to help reduce the spread of illness at fairs and at petting zoos through its website at *Health.state.mn.us*.

For more information, members should contact their MCIT loss control consultant or risk management consultant toll-free at **866.547.6516**.

The MCIT Board of Directors approved Martin County Historical Society for MCIT membership during its April 10 meeting. Martin County sponsored MCHS for membership.

The historical society preserves local history such as artifacts, documents, newspapers, oral and video histories, and more. Located in Fairmont, MCHS has been in operation since 1954.

More Flexibility Brings New Challenges for Remote Board Meetings ... continued from page 1

to the meeting when all board members are in attendance at the regular meeting location. As such, it may not be a violation not to livestream and provide remote access in this circumstance.

The bigger challenge may be criticism and concern from the public that the board is not being transparent when it does not provide remote access after giving notice that it would do so. One way to counter this expectation may be to inform the public of where they can find the link on the day of the meeting, and offer a reason the link is not there (i.e., no remote board member attendance).

However, DPO noted that it may be a better practice for entities to continue to offer the public a remote viewing option once the board has posted that it will have members participating remotely.

This practice may be even more important for boards that routinely post before every meeting that members may be participating by interactive technology. Some entities have adopted this approach so as to provide board members with maximum flexibility for situations such as sudden illness or inclement weather where a three-day notice would be impossible.

DPO takes the position that boards should be offering maximum transparency if its members want the maximum flexibility for how to attend the meeting. In other words, if meetings are consistently noticed so that members have the ability to attend remotely, the board should always be offering a remote viewing option so there is no confusion for the public about how they can observe the board's work.

DPO noted that although it may not be a violation of the Open Meeting Law to cancel a remote viewing option, any time a public body deviates from what it says it will do, there may be questions from the public about whether the body is being truly transparent.

DPO also noted that when considering compliance with the Open Meeting Law, it is good to keep in mind that the Minnesota Supreme Court has indicated that the law should be interpreted in favor of transparency.

Also, it may be unreasonable for the public not to know whether remote access will be available up until the meeting starts based on board member in-person attendance.

Further Guidance

Members are encouraged to review Minnesota Statutes Section 13D.02 of the Open Meeting Law to confirm that their remote meeting attendance practices remain consistent with the law. Although some areas of the law changed in 2025, others remained the same, such as including the names of members and reasons for attending remotely in the meeting minutes.

Members with questions regarding their approach to remote meeting attendance are encouraged to consult with their legal counsel.

The Data Practices Office also responds to Open Meeting Law questions on an informal basis via telephone or email. More information about the Data Practices Office can be found on its website at *MN.gov/admin/data-practices*.

Deactivate Unnecessary Credentials to Shut Down Security Vulnerability ... continued from page 3

The organization should also have a process for circumstances that require immediate security concerns and deactivating access.

Besides deactivating credentials, the employer should develop a process to allow for proper archiving of information such as emails or work product before accounts can simply be deleted.

Technical tools can be part of the solution to ensure that the active directory (those accounts that have current access to devices, systems and programs) is kept current. These tools have the ability to track logins and access attempts; generate reports for audits or compliance; and identify suspicious behavior, such as login attempts at odd hours, multiple failed login attempts and login attempts from unfamiliar devices or locations.

Conducting an audit of the active directory regularly (e.g., every three to six months) can help catch accounts that were not reported to IT to deactivate or were accidentally overlooked.

Technical tools are perhaps best used as a backup for solid communication and planning among leadership, Human Resources and IT.

Document Changes

Changes to account access should be documented for many reasons. Most notably, threat actors may attempt to make changes, so documenting changes allows an organization to know which modifications were made, when and why.

Additionally, documentation may help speed up troubleshooting. If an update or change presents any issues, the organization can easily determine the changes that were made and when in the event it needs to revert back to previous settings or configurations.

Lastly and perhaps most importantly, documenting changes provides a level of accountability so that they can be tracked back to an individual who can and should indicate reasons for any adjustments and when they took effect.