Risk Management Fund

COVID-19:
Best Practices Guide

March 2020

Table of Contents

General Overview

For Texas Water Conservation Association Risk Management Fund (TWCARMF) Members

01. Establish A Team

Establish a team from different departments to assess your organization's coronavirus needs and risks. Determine the team's command and decision-making structure. Choose one person to be the spokesperson for the public entity.

02. Create A Communications and Contingency Plan

It's important to agree internally about what will be communicated before any announcements are made to assure that messaging will be consistent across different audiences. Should an outbreak occur near your offices, what should happen first, second and third? Who is authorized to make prompt decisions? Who should be informed? By what communication methods? What messages should they hear? What are the protocols for providing updates?

03. Create A Human Resources Plan

Explore what the rules will be if your employees need to work from home. Regarding travel, see the World Health Organization's (WHO) written travel guidelines for COVID-19. Will employees' compensation continue as normal? What about non-salaried employees? What does your government require? Review telecommuting policies and accountability. Beware of bias, discrimination and exclusion at your organization, and always be protective of employee personal privacy and confidentiality as required by law. Follow up on reports of discrimination and respond to concerns.

04. Communicate With Your Staff

Communicate with your staff on a regular basis to prevent fear-based rumors. Prepare statements/intranet news and continue to educate the employees and regularly pass on information to them including what the district is doing to handle COVID-19.

05. Establish A Cleanliness Protocol

Do a SWOT (Strengths, Weaknesses, Opportunities, Threat) Analysis specifically related to COVID-19 or infectious disease. What protocols for cleanliness does your organization have or need? Is your custodial staff increasing its cleaning and disinfection of touch surfaces (restrooms, doorknobs, kitchen and dining areas)? Do they have the correct personal protective equipment?

General Overview *continued...*

They should avoid cleaning methods that might aerosolize pathogens (pressure washing, steam cleaning). What emergencies should you plan for?

06. Monitor The CDC Website For Updates

Develop a protocol system for monitoring daily, hourly and emergency information. Your organization should seek advice from scientific and medical officials with experience in epidemiology, such as those in the WHO, the U.S. CDC, or similar national government health organizations in other countries.

07. Communicate With Your Public

Maintaining their trust and confidence during a potential coronavirus-related disruption is critical (identify concerns, steps taken to protect public from exposure to the virus, provide resources, update frequently).

08. Prepare For Media Inquiries

It is recommended that organizations only discuss their policies relating to the outbreak, their advice to employees on staying healthy, and their plans to keep meeting customer/public needs.

09. Plan For The Future

Evaluate your practices and plan to sustain them in the event the virus grows stronger or comes back. Monitor the effectiveness of communication to different audiences. Immediately address fear and prejudice against different groups of people directly and with science-based facts.

Hygiene and General Precautions

01. Wash your hands often with soap and water for at least 20 seconds.
02. If soap and water aren't available, use hand sanitizer that contains at least 70% alcohol.
03. Avoid touching your eyes, nose and mouth with unwashed hands.
04. Continue to use personal protective equipment such as safety glasses, face shield, gloves, and respirators required by your job.
05. Avoid close contact with people who are sick.
06. Stay home when you are sick and do not return to work or school until you have been fever-free without the use of fever reducing medication for at least 24 hours.
07. Avoid large crowds. Put distance between yourself and other people whether or not you believe COVID-19 is spreading in your community.
08. Keep your exercise regimen, if you feel well.
09. Get plenty of sleep. A good night's sleep boosts your immune system.

Your Staff

01. Instead of meeting face-to-face, consider any form of telephonic/video chat apps/websites.

02. Allow staff to work from home, where possible. The fewer people in contact with each other, the better we can contain this virus.

03. Sick employees should be sent home immediately.

04. If employees feel sick before coming to work, require them to stay home until they are without a fever for 24 hours or more.

05. Require handwashing for at least 20 seconds for all staff and members of the public (where applicable).

06. Discourage gatherings of people in small areas (meeting rooms, kitchens, etc.).

07. Prohibit gatherings/events by large groups of people (more than 10, though that number can be much lower, if needed).

Social Distancing

District management, in consultation with local public health officials, should consider taking any or all actions below to reduce opportunities for coronavirus transmission and increase social distancing:

01. Restrict building access with locked doors or a secured indoor lobby. Designate most areas of the building for only currently on-duty personnel.

02. Cancel all tours.

03. Postpone non-essential in-person continuing education of all types - lecture, hands-on and high-fidelity simulation.

04. Deliver district training, virtually with a conference call or web meeting.

05. If a group of personnel must gather in a meeting room, ensure that chairs, tables and all training equipment are disinfected before and after the meeting.

06. Require any face-to-face meeting attendees to spread out so they are at least six feet apart. Do not serve drinks, snacks, or lunches.

07. Postpone any group meetings with contractors regarding RFP's, facility tours for them, or any in person meetings that could be conducted with teleconferencing.

08. Postpone non-essential visits for equipment demonstrations or checks. Ask the vendor to provide demonstrations by live or recorded web video.

Travel

The U.S. government has taken unprecedented steps with respect to travel in response to the growing public health threat posed by this new coronavirus:

01. Foreign nationals who have been in China, Iran, Italy, or Europe within the past 14 days cannot enter the United States.

02. U.S. citizens, residents, and their immediate family members who have been outside the United States within the past 14 days can enter the United States, but they are subject to health monitoring and possible quarantine for up to 14 days.

03. On March 8, CDC recommended that people at higher risk of serious COVID-19 illness avoid cruise travel and non-essential air travel.

04. On March 26, Texas Governor Abbott orders mandatory quarantine for people traveling from New York area, New Orleans, and other COVID-19 hot spots. Travelers from these areas and other hot spots must register with the Texas Department of Public Safety and immediately quarantine themselves at home or in a hotel for 14 days or until they leave the state, whichever occurs first.

05. For additional travel information visit:

www.cdc.gov/coronavirus/2019-ncov/travelers/map-and-travel-notices.html

Information Technology – Cyber Security Recommendations

Here are some helpful tips on IT and Cyber Security during COVID-19:

01. Be very cautious with real interactive dashboards of Coronavirus infections and death rates. They are being used in malicious websites and emails to spread password-stealing malware.

(For Example: Cyber - Criminals have started disseminating real-time, accurate information about global infection rates to the pandemic in a bid to infect computers with malicious software.)

02. Cyber - Criminals have also started selling digital Coronavirus infection kits that use the interactive maps as part of Java-based malware deployment schemes.

(For Example: They offer $200 kit costs if the buyer has a Java code signing certificate and $700 if the buyer wants to use the seller's certificate.)

03. Cyber - Criminals have started sending email scams that prey on a person's desire to help during the Coronavirus crisis. These malicious emails inform the recipient to open an attached document that includes information about safety measures which then directs users to a page that asks for their email address and password. Please do not provide email address, passwords or personal information.

It is important you are cautious on attachments in emails. Sometimes these malicious attachments will be PDFs, MP4s and Docx files indicating they are coming from the US Centers for Disease Control and Prevention (CDC). Any grammatical errors in the address or message may be indicative of a potential cyber-attack.

04. Ensure backups are adequately being completed and test restoring data from the backups. There should be one backup disconnected from the network in case of a ransomware attack.

05. Update Virtual Private Networks (VPNs), network infrastructure devices, wireless devices, and devices being used to remote into work environments with the latest operating systems, software patches and security configurations.

06. Ensure IT personnel are prepared to ramp up remote access log review, attack detection, and incident response/recovery.

Information Technology – Cyber Security Recommendations *continued...*

07. Implement multifactor authentication on all VPN connections. If it's not implemented, require remote workers to use very strong passwords.

08. Ensure there's a telephone system or mobile business phone for the remote workers along with the monitors, laptops, and printers. Document any changes in personnel phone numbers for emergencies.

09. Create a Telework policy that outlines expectations, hours, duration, equipment, software, monitoring, confidentiality, removable media, security, reviews, travel expenses, performance standards, communication, accessibility, and emergency operations including dependent care and other non- employment responsibilities.

10. Having a security awareness training program implemented is very important. When discussing your security awareness training program, we encourage to steer away from in-person (large group) training due to the current COVID-19 virus threat.

Working From Home – Cyber Security Recommendations

01. Ensure Virtual Private Networks (VPN) and other remote access systems are fully updated with the latest operating systems, patches, and security configurations. Unpatched network infrastructure equipment, servers and end user equipment continue to be an attractive target for malicious actors.

02. If a VPN is not implemented, require all users, especially remote, to use very strong passwords. A minimum length of 16 characters containing numbers, symbols, upper/lower case letters, and spaces is recommended. Attackers can steal a weak password using dictionary attacks and automated tools.

03. Avoid using Remote Desktop Protocol (RDP), if possible. This protocol connects a user to another computer remotely over a network connection. This leaves RDP client ports open to the Internet, leaving vulnerability to attackers that scan blocks of IP addresses for open RDP ports.

04. Enhance system monitoring to receive early detection and alerts on abnormal activity. Ramp up remote access log review and attack detection.

05. Implement multi-factor authentication protection methods to reduce the potential for malicious activity.

06. Ensure all machines and wireless devices have properly configured network firewalls as well as anti-malware and intrusion prevention software installed. Most operating systems include a built-in firewall feature to enable for added protection.

07. Test the remote access solutions capacity and increase capacity, if needed.

08. Ensure disaster recovery, continuity of operations plans, or business continuity plans are up to date. Update incident response plans to consider workforce changes in a distributed environment.

09. Ensure backups are adequately being completed and test restoring data from the backups. There should be one backup disconnected from the network in case of a ransomware attack.

10. Ensure there's a telephone system or mobile business phone for the remote workforce along with the monitors, laptops, and printers. Document any changes in personnel numbers for emergencies.

Working From Home – Cyber Security Recommendations *continued...*

11. Create a Telework policy that outlines expectations, hours, duration, equipment, software, monitoring, confidentiality, removable media, security, reviews, travel expenses, performance standards, communication, accessibility, and emergency operations including dependent care and other non-employment responsibilities.

12. Increase awareness of information technology support mechanisms and support phone numbers for employees who work remotely.

13. Having a security awareness training program implemented is very important. When discussing your security awareness training program, we encourage to steer away from in-person (large group) training due to the current COVID-19 virus threat.

14. Be aware of an increase in phishing attacks that use a combination of email and fake websites to trick users into revealing sensitive information.

15. Be very suspicious of interactive dashboards COVID-19 infections and death rates being used in malicious websites and emails to spread password-stealing malware. Criminals have also started selling COVID-19 infection kits for deployment of malware.

    (For Example: Cyber - Criminals have started disseminating real-time, accurate information about global infection rates to the pandemic in a bid to infect computers with malicious software. Also, offering $200 kit costs if the buyer has a Java code signing certificate and $700 if the buyer wants to use the seller's certificate.)

16. Be cautious of disinformation campaigns that spread discord, manipulate public conversation, influence policy development, and disrupt markets.

17. Use extreme caution. Avoid clicking on links in unsolicited emails and be wary of email attachments.

18. Never reveal personal information or financial information in emails and do not respond to email solicitations requesting this information.

Working From Home – Cyber Security Recommendations *continued...*

19. Use only trusted national online medical resource websites for up-to-date and fact-based information about COVID-19 at: www.cdc.gov/ and https://www.who.int/

20. Verify a charity's authenticity before making donations. Review the Federal Trade Commission's blogs for current information on avoiding COVID-19 related scams at: www.consumer.ftc.gov/blog/2020/02/coronavirus-scammers-follow-headlines

21. Visit only official state agency websites and social media accounts such as: Public Health, Governor's Office, Homeland Security and Emergency Management, Attorney General, and Department on Aging.

22. Volunteer your due diligence by helping to report scams and identity theft and other cyber-related crimes.

Families First Coronavirus Response Act

Employers need to be aware of the changes to federal employment law effective April 2, 2020 concerning new paid sick leave requirements and expansion of the Family and Medical Leave Act (FMLA). This Act, the Families First Coronavirus Response Act affects all employers with fewer than 500 employees (FFCRA) and most public employees.

Employer Eligibility

At present, the FFCRA applies to private employers with fewer than 500 employees, and most public employers.

For many smaller employers, the FFCRA could introduce FMLA coverage into your workplace for the first time. Prior to this law, FMLA only applied to employers with more than 50 employees. FFCRA does not limit its coverage to employers with more than 50 employees so all employees may be subject to FMLA through the new FFCRA. The FFCRA allows the U.S. Department of Labor to issue regulations to exclude emergency responders and/or businesses with less than 50 employees where the requirements "would jeopardize the viability of the business as a going concern." However, at this time, The U.S. Department of Labor has not issued any exclusions. We will continue to update any changes to employer eligibility under the FFCRA.

Two Main Provisions Under the FFCRA: Child Care/FMLA and Emergency Leave

Employers are required to give employees two types of paid leave when employees must miss work because of the COVID-19 outbreak: (1) FMLA related to an employee's care of a child, and (2) emergency sick leave for employees who cannot work because the employee meets one of the six separate categories described below.

Emergency Family and Medical Leave Expansion

- **Employee Eligibility:** The Act will apply to any employee who has worked for the employer for at least 30 days prior to the designated leave.

- **Reasons for Emergency Leave:** Any individual employed by the employer for at least 30 days may take up to 12 weeks of job-protected leave to allow an employee, who is unable to work or telework, to care for the employee's child (under 18 years of age) if the child's school or place of care is closed or the childcare provider is unavailable due to a public health emergency.

Families First Coronavirus Response Act *continued…*

- **Paid Leave:** The first ten days of such leave are unpaid under the Act, though an employee may elect to use existing accrued paid leave (like vacation or sick leave) to cover some or all of the 10-day unpaid period. After the 10-day period, the employer generally must pay full-time employees at two-thirds the employee's regular rate for the number of hours the employee would otherwise be normally scheduled.

  The FFCRA does not require employers to exceed a rate of pay equal to $200 per day and $10,000 in the aggregate per employee. Nothing in the FFCRA prohibits employers from going beyond these limits in compensating their employees, but the employer may not be eligible for tax deductions under the FFCRA beyond the limits.

- **Calculating Pay for Non-Full Time Employees:** Employees who work a part-time or irregular schedule are entitled to be paid based on the average number of hours the employee worked for the six months prior to taking Emergency FMLA. Employees who have worked for less than six months prior to leave are entitled to the employee's reasonable expectation at hiring of the average number of hours the employee would normally be scheduled to work.

- **Job Restoration:** Employers with 25 or more employees will have the obligation to return any employee who has taken Emergency FMLA to the same or equivalent position upon the return to work. However, employers with fewer than 25 employees are generally excluded from this requirement if the employee's position no longer exists following the Emergency FMLA leave, due to an economic downturn or other circumstances caused by a public health emergency during the period of Emergency FMLA.

Emergency Paid Sick Leave Act

An employer must allow an eligible employee to take paid sick leave when the employee is:

1. subject to a Federal, State or local quarantine or isolation order related to COVID-19;
2. advised by a health care provider to self-quarantine due to COVID-19 concerns;
3. experiencing COVID-19 symptoms and is seeking medical diagnosis;
4. caring for an individual subject to a Federal, State or local quarantine or isolation order or advised by a health care provider to self-quarantine due to COVID-19 concerns;
5. caring for the employee's child if the child's school or place of care is closed or the child's care provider is unavailable due to COVID-19 precautions; or

Families First Coronavirus Response Act *continued…*

6. experiencing any other substantially similar condition specified by the Secretary of Health and Human Services in consultation with the Secretary of the Treasury and the Secretary of Labor.

- **Employee Eligibility:** This provision requires employers to provide full-time employees (regardless of the employee's duration of employment prior to leave) with 80 hours of paid sick leave at the employee's regular rate when the employee is subject to any of the qualifying reasons contained in 1, 2 or 3 above (i.e., the employee is the individual subject to quarantine or isolation). The employer is required to provide 80 hours of sick leave at two-thirds the employee's regular rate to care for others as set forth in qualifying reasons 4, 5, or 6 listed above.

- **Cap on Paid Sick Leave Wages:** Another significant change in this Act is that employers are only required to pay an employee $511 per day, up to $5,110 total per employee when the employee is the affected individual, and $200 per day up, to $2,000 total to care for others and if they are experiencing any other substantially similar condition. Nothing prohibits an employer from paying an employee at a higher rate for paid sick leave, but the FFCRA does not require employers to pay higher rates and there could be a limit on the tax deduction available under the FFCRA.

- **Notice Requirements:** We expect that the Department of Labor will shortly issue notices for the new Act which will have to be posted in your workplace and distributed to employees. We will provide updates on these developments, as well.

Important Compliance Guidelines

This is a federal law and it will also be important for employers to monitor whether state or local governments issue new workplace laws/regulations.

Likewise, in this rapidly changing environment, employers ought to pay close attention to, and follow, any new directives or mandatory instructions from Federal, State or local authorities related to COVID-19.

Additional Information and Resources

FEMA's Public Assistance Program

FEMA's Public Assistance Program provides supplemental grants to state, tribal, territorial, and local governments, and certain types of private non-profits so that communities can quickly respond to and recover from major disasters or emergencies. FEMA also encourages protection of these damaged facilities from future events by aiding for hazard mitigation measures during the recovery process.

More detailed information can be in the **FEMA Public Assistance Program and Policy Guide.**

Click Here for FEMA Public Assistance Program and Policy Guide (Pg: 71-74)

www.fema.gov/public-assistance-local-state-tribal-and-non-profit

Resources and Links:

Coronavirus Plan and Prepare Now - Situation Summary: **www.icma.org/coronavirus-resources-plan-and-prepare-now-it-hits-your-community**

Mass Gatherings or Large Community Events: **www.cdc.gov/coronavirus/2019-ncov/community/large-events/mass-gatherings-ready-for-covid-19.html**

Managing Anxiety and Stress - Responders: **www.emergency.cdc.gov/coping/responders.asp**

State Fiscal Responses to COVID-19: **www.ncsl.org/research/fiscal-policy/state-fiscal-responses-to-covid-19.aspx**

Legislative Sessions and the Coronavirus: **www.ncsl.org/research/about-state-legislatures/legislative-sessions-and-the-coronavirus.aspx**