

COVID-19 RE-OPENING THE ECONOMY

MAY 2020

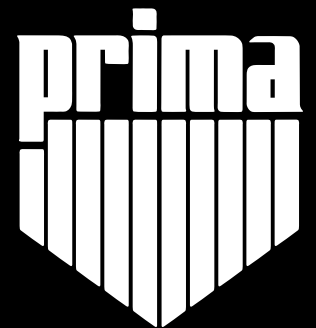


TABLE OF CONTENTS

| | |
|-------------------------------------|----|
| COVID-19 RE-OPENING TASK FORCE..... | 2 |
| EXECUTIVE SUMMARY..... | 3 |
| TRAINING & COMMUNICATION | 5 |
| INTERNAL & EXTERNAL CUSTOMERS..... | 13 |
| LEGAL CONSIDERATIONS | 18 |
| CYBERSECURITY | 21 |

PRIMA'S COVID-19 RE-OPENING TASK FORCE

James Curbeam, Chair

Risk Manager
Las Vegas Valley Water District
Las Vegas, NV

Jean Heald

Employee Safety/Loss Control Manager
County of Palm Beach
West Palm Beach, FL

Amy Larson

Risk and Litigation Manager
City of Bloomington
Bloomington, MN

Michael Payne (Board Liaison)

Risk Manager
City of Fresno
Fresno, CA

Aaron Ambrose

Director of Risk Management
Midwest Public Risk
Independence, MO

Patrick Hughes

Risk Manager
City of Portland
Portland, OR

Timothy Mulligan

Safety and Loss Coordinator
City of Show Low
Showlow, AZ

Jennifer Ackerman (Staff Liaison)

CEO
Public Risk Management Association
Alexandria, VA

Robin Flint

Senior Risk Management Advisor
ACWA JPIA
Roseville, CA

Daniel Hurley

Risk Manager
City of Chesapeake
Chesapeake, VA

Margaret Penado

Risk Manager
County of Coconino
Flagstaff, AZ

Shaunda Ragland (Staff Liaison)

Director, Education & Training
Public Risk Management Association
Alexandria, VA

Marco Guardi

Regional Risk Control Leader
Arthur J. Gallagher and Co.
Irvine, CA

Alonzo Johnson

Risk Management & Liability Manager
City of North Las Vegas
North Las Vegas, NV

John Whalen

Operations Director & Risk Manager
First Tennessee Human
Resource Agency
Johnson City, TN

EXECUTIVE SUMMARY



In response to significant number of requests for information related to COVID-19 activities being performed by its members, including steps being taken to re-open member workplaces, PRIMA established the COVID-19 Re-Opening Task Force comprised of PRIMA members from different public entities and service vendors. The following white paper is produced with the intent to provide ideas and information to PRIMA members that they may use to consider and identify issues specifically related to the re-opening of their facilities to both their employees and customers. This document is intended to be a fluid document that will change as we learn more about the COVID-19 virus and as future treatment and mitigation options are developed.

The material contained in this white paper is not intended to be construed as legal advice about the content, interpretation or application of any law, regulation, or regulatory guideline. Members are encouraged to consult with their entity's legal counsel to understand the applicability of any law or regulation related to COVID-19.

The Centers for Disease Control and Prevention provides guidance regarding reintegrating your workforce. While Re-Opening your entity, everyone should continue to practice social distancing and personal hygiene measures as recommended by the [CDC](#). Reducing the risk of exposure to COVID-19 by [cleaning and disinfecting](#) is an important part of Re-Opening public spaces.

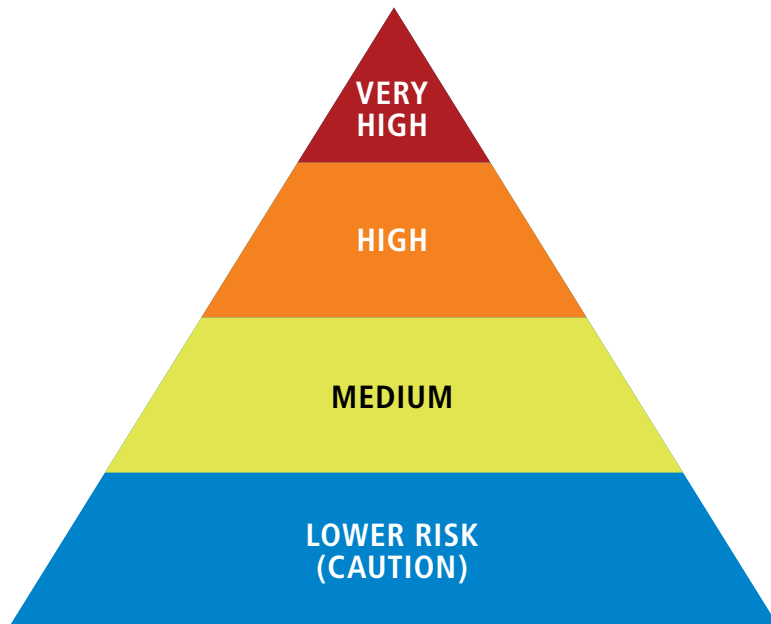
As entities navigate through this unprecedented time, it is important to develop a Reintegration Plan, implement the phases of your plan as applicable, and regularly review and update your plan. Although not an exhaustive list, this paper will provide readers with topics to consider from the following categories:

- Training & Communication
- Internal & External Customers
- Legal
- Cyber security

This document will provide ideas and information related to the Re-Opening phase of your plan specific to COVID-19 with important elements from the following:

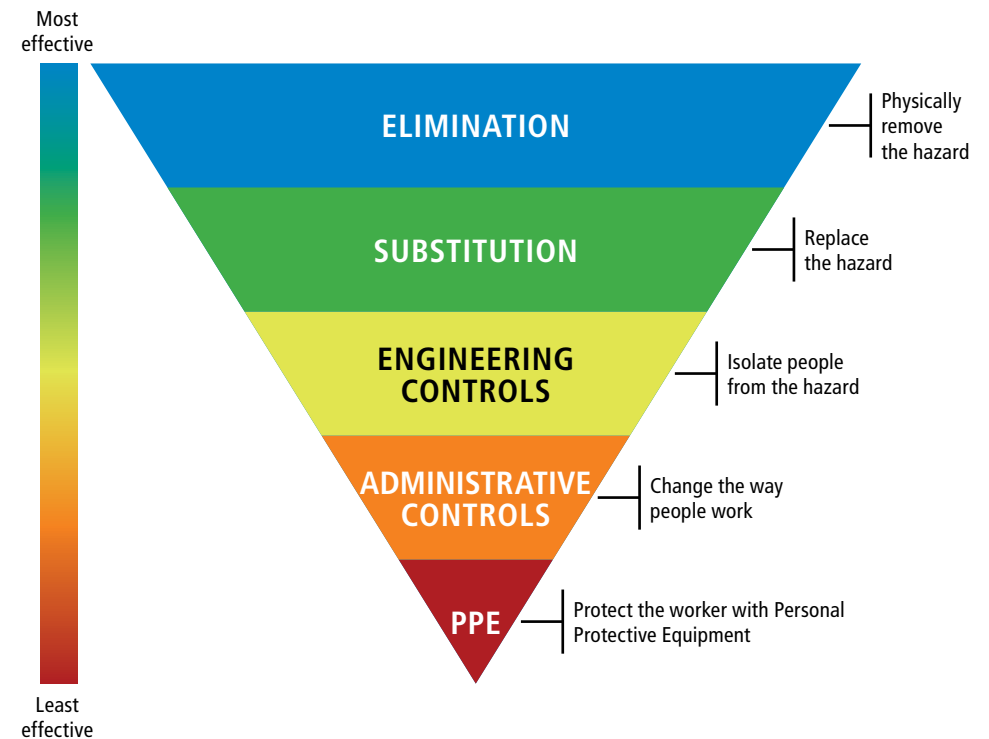
- Reviewing the potential operational and policy considerations related to resuming operations during the COVID-19 pandemic.
- Developing a checklist of important issues that need to be considered when developing a reintegration plan related to operations during the COVID-19 pandemic.
- Providing a centralized location for PRIMA members to share ideas, questions and resources for re-opening their entities.

WORKER EXPOSURE RISK TO COVID-19



HIERARCHY OF CONTROLS

Controlling exposures to occupational hazards is the fundamental method of protecting workers. Traditionally, a hierarchy of controls has been used as a means of determining how to implement feasible and effective control solutions.



PANDEMIC PREPAREDNESS RESOURCE

TRAINING & COMMUNICATION

EMPLOYEE TO CUSTOMER INFECTIOUS DISEASE RISK MITIGATION



WHO ARE THESE GUIDELINES FOR?

These guidelines are suggested for any employees who interact with customers on a face to face basis as part of their job duties. This includes employees greeting customers at counters, windows, outside of a facility, during meetings, etc.

WHAT ARE THE GUIDELINES?

These guidelines are methods and procedures designed to decrease the risk of contracting an infectious airborne disease during interactions between employees and customers. Following them will not guarantee immunity from such an infectious disease, but will increase the odds that the employee will not become infected and remain healthy.

GENERAL HYGIENE

- Wash hands often with soap and water for at least 20 seconds, especially after going to the bathroom, before eating, and after blowing your nose, coughing, or sneezing.
- Use sanitizing solution to clean hands and work surfaces frequently throughout the day.
- Using hand sanitizer that contains at least 60% alcohol if soap and water are not available.
- Avoiding touching eyes, nose, and mouth with unwashed hands.
- Cover coughs and sneezes with a tissue, then throw the tissue in the trash.

- Disinfect and sanitize high-touch areas that customers may use while conducting business.
- Stay home if you are experiencing COVID-19 symptoms and report this via telephone to your supervisor and human resources.
- Staff has the right to use masks that are not OSHA-regulated without being added to the city's respiratory protection program.
- Employees may use unregulated cloth or surgical masks without any restrictions or controls.
- Employees may use gloves while working without regulation or restrictions.

INTERACTING WITH CUSTOMERS

- Use social distancing to maintain at least six feet between individuals in all areas of the work environment, including customers.
- Set up six foot queue markers to help customers waiting in line maintain safe social distancing.
- Unruly customers:
 - » Alert your supervisor or others who can assist.
 - » Ask customer to please leave building.
 - » Contact 911 or local law enforcement.
- Use barriers whenever possible to maintain safe separation between you and the customer.
- Postpone events where social distancing or other mitigating measures cannot be maintained.
- Use telephone contact to conduct business whenever possible.
- Use tele-meeting applications to conduct business meetings as the preferred method of contact.
- Schedule the minimum amount of people needed for any in-person meetings.
- Limit the number of registrants and participants in special events to maintain social distancing.
- Customers will have their temperature taken if they wish to enter a facility. Otherwise if conditions are safe, business may be conducted outside.

- Communicate policies in advance to your customers using Employee to Vendor Guidelines.
- Post signage that encourages social distancing and effective hygiene in areas where customers frequent.

WHERE ARE THESE GUIDELINES NECESSARY?

These guidelines are necessary in any customer setting. A customer interaction setting could be at a customer counter, on a job site, in a meeting or anywhere else where you are interacting with someone in person.

WHY MUST WE FOLLOW THESE GUIDELINES?

Employers are responsible to ensure that employees are provided a work environment that is healthful and safe. Employees are encouraged to follow these guidelines in order to maintain their health while at their place of employment. Following the guidelines will also help to maintain our customer's health and well-being.

HOW SHOULD I USE THESE GUIDELINES?

Risk managers are encouraged to use these guidelines and apply them to employees that work face to face with the entity's customers in environments such as the entity's buildings, special events, outdoor settings, and other gatherings involving customers.

EMPLOYEE TO EMPLOYEE INFECTIOUS DISEASE RISK MITIGATION



WHO ARE THESE GUIDELINES FOR?

These guidelines are suggested for any employees who interact with other employees on a face to face basis as part of their job duties. This includes employees working in offices, cubicles, departments, during meetings, or in breakrooms, water fountains, restrooms, or other work spaces.

WHAT ARE THE GUIDELINES?

These guidelines are methods and procedures designed to decrease the risk of contracting an infectious airborne disease during interactions between employees. Following them will not guarantee immunity from such an infectious disease, but will increase the odds that the employee will not become infected and remain healthy.

GENERAL HYGIENE

- Wash hands often with soap and water for at least 20 seconds, especially after going to the bathroom, before eating, and after blowing your nose, coughing, or sneezing.
- Use sanitizing solution to clean hands and work surfaces frequently throughout the day.
- Use hand sanitizer that contains at least 60% alcohol if soap and water are not available.
- Avoiding touching eyes, nose, and mouth with unwashed hands.
- Cover coughs and sneezes with a tissue, then throwing the tissue in the trash.
 - » If not tissue is not available, cough or sneeze into your elbow – not your hands.

- Disinfect and sanitize high-touch areas that customers may use while conducting business.
- Create emails, task reminders, or other prompts for staff to sanitize frequently touched areas.
 - » Entry/Exit door handles, timeclocks, light switches, faucets, microwave panels, etc.
- Stay home if you are experiencing COVID-19 symptoms and report this via telephone to your supervisor and human resources.
- Staff has the right to use masks that are not OSHA-regulated without being added to the city's respiratory protection program. Check with your supervisor for clarification and local, state, or other guidance given at this time.
- Employees may use unregulated cloth or surgical masks without any restrictions or controls. Check with your supervisor for clarification and local, state, or other guidance given at this time.
- Employees may use gloves while working without regulation or restrictions. Check with your supervisor for clarification and local, state, or other guidance given at this time.

INTERACTING WITH EMPLOYEES

- Consider having employee schedules staggered so they are not coming in and going out all at the same time.
- Use social distancing to maintain at least six feet between individuals in all areas of the work environment.
- Set up six foot queue markers to help employees waiting in line to clock in/out, at office doorways, vending machines, or other frequented spaces to maintain safe social distancing.
- Engineer your facilities so employee foot traffic can flow without having to pass through restrictive spaces placing employees within an acceptable six-foot distance.
- Use barriers whenever possible to maintain safe separation between you and others.
- Postpone proceedings where social distancing or other mitigating measures cannot be maintained.
- Use telephone contact to conduct business whenever possible.

- Use tele-meeting applications to conduct business meetings as the preferred method of contact.
- Schedule the minimum amount of people needed for any in-person meetings.
- Limit the number of registrants and participants in special events to maintain social distancing.
- Employees may have their temperature taken upon entering a facility. Otherwise if conditions are safe, business may be conducted outside. Check with your supervisor for clarification and local, state, or other guidance given at this time.
- Communicate policies in advance to your Employees using Guidelines.
- Post signage that encourages social distancing and effective hygiene in areas where employees frequent.
- Employees that do not practice safe guidelines:
 - » Ask employee to please step back or take it upon yourself to move away to a safe distance.
 - » Alert your supervisor or others who can assist.
 - » Contact human resources if a solution for the issue is not readily available.

WHERE ARE THESE GUIDELINES NECESSARY?

These guidelines are necessary in any workplace setting. Interaction settings could be at a counter, on a job site, in a meeting space, at a watercooler, or anywhere else where you are interacting with a fellow employee in person.

WHY MUST WE FOLLOW THESE GUIDELINES?

Employers are responsible to ensure that employees are provided a work environment that is healthful and safe. Employees are encouraged to follow these guidelines in order to maintain their health while at their place of employment. Following these guidelines will also help to maintain our fellow employee's health and well-being.

HOW SHOULD I USE THESE GUIDELINES?

Risk managers are encouraged to use these guidelines and apply them to employees that work face to face with other employees in workplace environments such as the entity's buildings, offices, vehicles, warehouses, special events, and other gatherings places.

COMMUNICATION

- Communicate policies in advance to your employees using Employee to Employee Guidelines.
- When a new employee is hired, provide training and expectations concerning to Infectious Disease Guidelines. Discusses safety precautions and policies in advance of job placement.
- Require employees to acknowledge Infectious Disease Guidelines and Safety Policies on acceptance forms if possible.
- Explain any PPE requirements especially if confined spaces are required for work with fellow employees.
- Post signage that encourages social distancing and effective hygiene in areas where employees frequent.
- Place statements concerning your guidelines to employees on their pay checks and/or envelopes.
- Communicate that violations of the safety guidelines may subject the individuals involved to disciplinary action(s).

EMPLOYEE TO VENDOR INFECTIOUS DISEASE RISK MITIGATION



WHO ARE THESE GUIDELINES FOR?

These guidelines are suggested for any employees who interact with vendors on a face to face basis as part of their job duties. This includes employees working on delivery/receiving docks or facilities, purchasing departments, inside/outside of a facility, during meetings, etc.

WHAT ARE THE GUIDELINES?

These guidelines are methods and procedures designed to decrease the risk of contracting an infectious airborne disease during interactions between employee and vendor. Following them will not guarantee immunity from an infectious disease, but will increase the odds that the employee will not become infected and remain healthy.

GENERAL HYGIENE

- Wash hands often with soap and water for at least 20 seconds, especially after going to the bathroom, before eating, and after blowing your nose, coughing, or sneezing.
- Use sanitizing / disinfecting solution to clean hands and work surfaces frequently throughout the day.
- Using hand sanitizer that contains at least 60% alcohol if soap and water are not available.
- Avoiding touching eyes, nose, and mouth with unwashed hands.
- Cover coughs and sneezes with a tissue, then throwing the tissue in the trash. If not tissue is not available, cough or sneeze into your elbow – not your hands.

- Disinfect and sanitize high-touch areas that vendors and staff members may use while conducting business.
- Stay home if you are feeling sick. Report illness via telephone to your supervisor and human resources.
- Staff has the right to use masks that are not OSHA-regulated without being added to the city's respiratory protection program. Check with your supervisor for clarification and local, state, or other guidance given at this time.
- Employees may use unregulated cloth or surgical masks without any restrictions or controls. Check with your supervisor for clarification and local, state, or other guidance given at this time.
- Employees may use gloves while working without regulation or restrictions. Check with your supervisor for clarification and local, state, or other guidance given at this time.

INTERACTING WITH VENDORS

- Use social distancing to maintain at least six feet between individuals in all areas of the work environment, including vendors.
- Set up six foot queue markers to help vendors waiting in line maintain safe social distancing.
- Unruly vendors:
 - » Alert your supervisor or others who can assist.
 - » Ask vendor to please leave building.
 - » Contact 911 or local law enforcement if necessary.
- Use barriers whenever possible to maintain safe separation between you and the vendor.
- Postpone proceedings where social distancing or other mitigating measures cannot be maintained.
- Use telephone contact to conduct business whenever possible.
- Use tele-meeting applications to conduct business meetings as the preferred method of contact.
- Schedule the minimum amount of people needed for any in-person meetings.
- Limit the number of registrants and participants in special events to maintain social distancing.

- Vendors may have their temperature taken upon entering a facility. Otherwise if conditions are safe, business may be conducted outside. Check with your supervisor for clarification and local, state, or other guidance given at this time.
- Communicate policies in advance to your vendors using Employee to Vendor Guidelines.
- Post signage that encourages social distancing and effective hygiene in areas where vendors frequent.
- Engineer your facilities so vendor foot traffic can flow without having to pass through restrictive spaces placing employees and vendors within an acceptable six-foot distance.
- Consider having vendors call and wait in their delivery vehicles prior to entering your facility. Once you are prepared to bring in the next vendor, call them in for delivery or pickup.
- For multiple semi-truck deliveries, specify a lane or parking area for them to stage their vehicles while they wait.

WHERE ARE THESE GUIDELINES NECESSARY?

These guidelines are necessary in any vendor setting. Interaction settings could be at a counter, on a job site, in a meeting space, on a dock, or anywhere else where you are interacting with a vendor in person.

WHY MUST WE FOLLOW THESE GUIDELINES?

Employers are responsible to ensure that employees are provided a work environment that is healthful and safe. Employees are encouraged to follow these guidelines in order to maintain their health while at their place of employment. Following these guidelines will also help to maintain our vendor's health and well-being.

HOW SHOULD I USE THESE GUIDELINES?

Risk managers are encouraged to use these guidelines and apply them to employees that work face to face with the entity's vendors in environments such as the entity's buildings, warehouses, special events, outdoor settings, and other gatherings involving vendors.

COMMUNICATION

- Communicate policies in advance to your vendors using Employee to Vendor Guidelines.
- When a new vendor is accepted, provide a pre-delivery document or meeting that discusses safety precautions and policies in advance.
- Require vendors to acknowledge your safety policies on vendor acceptance forms if possible.
- Post signage that encourages social distancing and effective hygiene in areas where vendors frequent.
- Place statements concerning your guidelines to vendors on accounts payable checks and/or envelopes.
- Set up staging areas that are well signed for shipping and receiving of goods and products.
- Communicate that violations of the safety guidelines may subject the individuals and/or contractors involved to dismissal from the site.
- Explain any PPE requirements especially if confined spaces are required for work with vendors.

INTERNAL & EXTERNAL CUSTOMERS



WHO ARE THESE GUIDELINES FOR?

The principles and approaches of our “new working relationships” with internal & external customers we work with and serve are outlined in this section.

Internal functions include but are not limited to: Facilities Preparation; Pre-Operational Preparation; and the Resumption of Operations.

External functions include but are not limited to: Facility Preparation including customer and vendor access points; Supply Chain; and Community Partners.

FIRST STEPS

Review CDC, state OSHA guidance, and OSHA federal guidance. Implement appropriate procedures to safeguard employees and customers.

- ☐ [CDC Interim Guidance for Businesses](#)
- ☐ [OSHA Workplace Guidance COVID-19](#)
- ☐ [OSHA Protecting Workers during Pandemic Factsheet](#)
- ☐ [State OSHA](#) Pandemic Guidance
- ☐ [CDC Coronavirus webpage](#)
- ☐ State Department of Health resources
 - » To find your state or territorial health department view this [CDC webpage](#)

Associated resources:

- ☐ [Ready.gov, Pandemic and Coronavirus](#)
- ☐ [FEMA Continuity Planning Factsheet for Pandemics](#)

INTERNAL CUSTOMERS

FACILITIES PREPARATION

Assess Workplace using Hierarchy of Controls

Engineering Controls

- ☐ Develop a social distancing plan
 - ☐ Consider physical workspace modifications
 - ☐ Barriers
 - ☐ Six foot queue markers to outline social distancing space
 - ☐ Workstation distancing

- ☐ Provide guidance on employees entering common areas
- ☐ Consider the use of portable shade structures to create outdoor break rooms

Administrative Controls

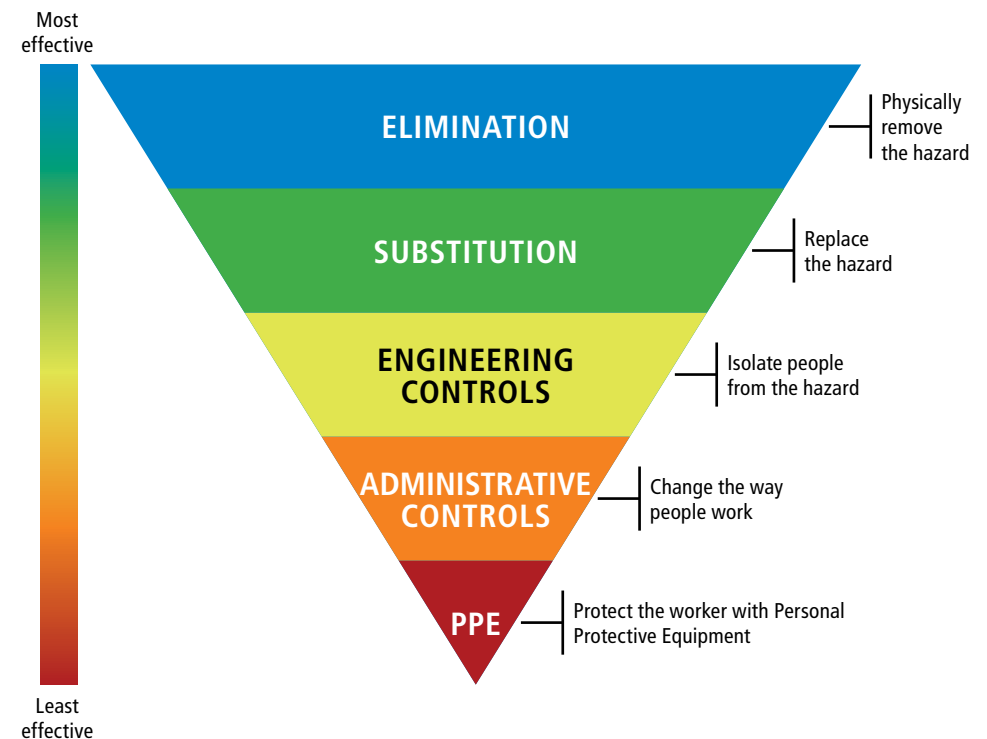
- ☐ Define the new “normal” for workplaces
 - ☐ Encourage virtual meetings
 - ☐ Continue remote working

Encourage the use of PPEs when engineering and administrative controls are not feasible or when encouraged by public health.

Additional resource:

- ☐ Review OSHA's [Guidance on Preparing Workplaces for COVID-19](#)

Hierarchy of Controls



Housekeeping and Workplace Sanitation

The CDC highlights that reducing the risk of exposure to COVID-19 by cleaning and disinfection is an important part of Re-Opening and maintaining public spaces.

- ☐ Maintenance staff responsibility—increase cleaning on frequently touched surfaces
- ☐ Individual employee responsibility —maintaining own workspace
- ☐ Discourage employees from using other employees' telephones, desks, offices, or other work tools and equipment, when possible. If there is a need to share workstations or equipment ensure these items are disinfected between usage.
- ☐ Cleaning and disinfecting SOPs use of proper PPE as identified on the MSDS/SDS sheet(s).

Additional resources:

- ☐ [CDC Re-Opening Guidance for Cleaning and Disinfecting Public Spaces, Workplaces, Business, Schools and Homes](#)
- ☐ [CDC Cleaning and Disinfecting Your Facility](#)
- ☐ [CDC Cleaning and Disinfecting Community Facilities](#)

Facility/Building Water Systems

- ☐ If any of your facilities have been shut down for a prolonged period of time, review the [CDC Guidance for Building Water Systems](#).

PRE-OPERATIONAL

Employees

- ☐ Establish an employee screening policy. The policy may include the screening measures outlined below, how confidentiality will be maintained and actions taken to address at risk employees with reference to your public entity's leave policy.
- ☐ Consider displaying markings or signs reminding customers to maintain social distancing in areas where people congregate; to avoid touching surfaces unnecessarily; to wash your hands properly and regularly; to wear a face covering where social distancing is not feasible.
- ☐ Evaluate if public restrooms allow for social distancing and implement a regular sanitation schedule.
- ☐ Communications and training for managers and workers necessary to implement the plan.
 - ☐ HR Considerations/Review Policies and Procedures
 - ☐ WC
 - ☐ Leave—FMLA/COVID-19 sick leave/individual employee leave
 - ☐ Not allowing sick people to come to work
 - ☐ Training Considerations
 - ☐ Proper PPE, types and usage
 - ☐ Cleaning procedures
 - ☐ Social distancing guidelines

- ☐ Infection prevention measures
 - ☐ Virtual meetings
 - ☐ Working remote
 - ☐ Split shifts
 - ☐ Assess, budget and manage use of PPE and sanitizers

- ☐ Prompt identification and isolation of sick persons
 - ☐ Consider developing screening protocols
 - ☐ Temperature checks
 - ☐ Frequency
 - ☐ Voluntary/mandatory
 - ☐ On-site, or have employee(s) fill out the form?
 - ☐ Expectations regarding sick people in the workplace
 - ☐ Sending them home
 - ☐ How to “recover” if an ill person comes to work

RESUMPTION OF OPERATIONS

Management

- ☐ Management and supervisory support necessary to ensure effective ongoing implementation of the plan
 - ☐ Reporting issues
- ☐ Daily/Weekly updates from management re: return to work, surges, etc.
- ☐ Social media:
 - ☐ Internal monitor social media outlets
 - ☐ External notification regarding public entity services

EXTERNAL CUSTOMERS

FACILITIES PREPARATION: PUBLIC, CUSTOMER AND VENDOR ACCESS POINTS

- ☐ Develop and communicate a social distancing plan.
 - ☐ Consider displaying markings or signs reminding customers to maintain social distancing in areas where people congregate; to avoid touching surfaces unnecessarily; to wash your hands properly and regularly; to wear a face covering where social distancing is not feasible.
- ☐ Evaluate if public restrooms allow for social distancing and implement a regular sanitation schedule.
- ☐ Update visitor and contractor sign in logs to include health screenings results if done for COVID-19 symptoms.
- ☐ For billing or payments consider having financial transactions online, touchless payment options including drop boxes.
- ☐ Practice “contactless” receipt of deliveries whenever possible. Contactless deliveries allows a vendor or service provider to leave a delivery at a doorstep, box, container, etc. When a delivery requires a receipt make attempts to confirm electronically (e.g., in an app or over a phone). Avoid sharing scanners, pens, or other tools with a vendor or service provider.
- ☐ Maintain a distance six feet or greater from vendors or service providers you might meet or need to speak with during a delivery.
- ☐ Limit contact with frequently touched surfaces during receipt of deliveries, such as doorbells or door handles. Use a foot, shoulder, elbow, hip, or forearm when opening doors, instead of hands, if possible.
- ☐ Contractors and repair service personnel will provide a written copy of their Coronavirus pandemic response plan.

SUPPLY CHAIN

Assess Third Party Services, Contractors and Vendors

- ☐ Managing vendors and contractors (quantities, redundancies, performance and contractual obligations)
- ☐ Estimate stock quantities needed and improvement projects planned for upcoming quarter. Notify primary vendors/contractors of modifications or deviations from previously agreed upon commitments.

- ☐ Examine vendor/contractor agreements for:
 - ☐ Performance obligations and variations on insurance requirements like changes in limits and coverage
 - ☐ Modify if necessary
- ☐ Audit vendors/contractors to assess upstream exposures
- ☐ Establish redundancy vendor/contractor agreements
- ☐ Vendor and contractor management to mitigate exposure potential
 - ☐ Review vendor/contractor access to facilities and interaction with employees
 - ☐ Implement exposure control measures as necessary

Community Partners

- ☐ Review and modify mutual aid and shared services agreements, if necessary
- ☐ Explore additional mutual aid opportunities

RESOURCES SPECIFIC TO PUBLIC SECTOR

- ☐ Schools & Colleges
 - ☐ Public education institutions should consult with their state and local offices of education on continuity of operations. Discussion and plans should be developed for student testing, accreditation, staffing, virtual learning, enrollment and more.
 - ☐ Sample Panflu plan (Gallagher)
- ☐ Cities
 - ☐ [National League of Cities](#)
- ☐ Counties
 - ☐ [National Association of Counties](#)
- ☐ Water & Wastewater Public Water Systems
 - ☐ Communicate with neighboring public water systems about resource sharing and mutual aid, particularly if a small PWS with few operators or use contract operators, and consider registering with [WARN](#).
 - ☐ Review and update any operations plans and provide instruction and training to operators to help improve redundancy.

- ☐ Ensure that any necessary chemicals or equipment are readily available and stockpile any extra materials as needed. Contact normal suppliers to verify that supply chains are still intact and their staff and operations are equally aware and prepared Encourage their likewise preparedness.
- ☐ Make sure important records are available to staff and consider storing those documents electronically and in a place that can be accessed outside of the workplace.
- ☐ Resources:
 - ☐ [American Water Works Association Coronavirus Resources](#)
 - ☐ [EPA Water Utility Resources for COVID-19 Pandemic](#)
 - ☐ [EPA Pandemic Incident Action Checklist for Water Utilities](#)
 - ☐ [OSHA Solid Waste and Wastewater Management Workers and Employers COVID-19](#)
 - ☐ [Water Environment Federation, Water Professional's Guide to COVID-19](#)
 - ☐ [US Department of Homeland Security Critical Infrastructure Water & Wastewater Sector](#)
- ☐ Public Works
 - ☐ [American Association of Public Works](#)
- ☐ Public Utilities
 - ☐ [American Public Power Association](#)
- ☐ Parks and Recreation
 - ☐ [National Parks and Recreation Association COVID-19 webpage](#)

LEGAL CONSIDERATIONS



There are legal implications to re-opening entities in the time of COVID-19. Things to consider when you are sending employees back to work are outlined below. Members are encouraged to consult with their entity's legal counsel to understand the applicability of any law or regulation related to COVID-19.

1. Establish a human resources and Legal Task Force in each organization
 - ☐ Designate human resources team members
 - ☐ Assigned City Attorney staff
 - ☐ Assign additional designated staff
2. Risk Assessments for specific jobs (Ex. Code inspections in homes)
 - ☐ Initiate assessment of critical positions
 - ☐ Initiate assessment other positions based on priority (customer contact, work crews)
3. PPE Requirements (Example N95 respirator policy)
 - ☐ Re-evaluation of public safety PPE needs
 - ☐ Evaluate basic customer contact PPE needs
 - ☐ Evaluate employee to employee based on contact - proximity
4. Work isolation policies if possible (challenge – work crews in field)
 - ☐ Provide acceptable spacing guidelines for interior staff
 - ☐ PPE requirements for staff in shared vehicles
 - ☐ Recommend social distancing for field crews which may include PPE

5. Promotion of personal hygiene and cleaning
 - ☐ Provide posted instructional guidance on hygiene methods and requirements
 - ☐ Provide hand sanitizers for field crews and vehicle wipes
 - ☐ Post reminder instructions in rest rooms
6. Social distancing policies – Travel/Training/Schedules
 - ☐ Update travel restrictions or requirements for approved travel
 - ☐ Determine training needs for webinars through WebEx, Zoom etc.
 - ☐ Determine methods for in-service certifications requirements (Police)
7. Employment Policy: sick leave, FMLA, Paid Time Off
 - ☐ Keep up to date on changing Federal or State leave requirements
 - ☐ Post leave policies on Human Resources website
 - ☐ Update employee handbook
8. COVID Specific Laws Compliance – Families First COVID-19 Virus Act
 - ☐ Check for daily updates for leave requirements
 - ☐ Post and provide an interpretive explanation for staff
9. COVID-19 Policy Resources and Guidance in Employee Handbook
 - ☐ Update handbook with COVID-19 policies
 - ☐ Post COVID-19, consider a generic communicable disease policy
10. Leave Request & Tracking Program
 - ☐ Establish an event specific leave tracking program inclusive of requests
 - ☐ Publish weekly management reports that includes leave use and staffing information
11. Employee Testing and Monitoring within EEOC guidance (confidentiality, fit for duty requests, body temperature – consistency, non-discriminatory, self-reporting, refusal issues)
 - ☐ Determine current employee health monitoring procedures based on CDC & EEOC guidelines
 - ☐ Encourage staff to self-report illness along with available leave options
 - ☐ Determine legal requirements with counsel when to order a Fit for Duty Assessment
 - ☐ Establish confidential record keeping and communication processes
12. Employee Health Screening Requirements – electronic tele-med certificates, questionnaires,
 - ☐ Establish acceptable medical certificates that will include tele med evaluations
 - ☐ Establish confidential record keeping and communication to employee's supervisor
13. Effective Communications – Health & Safety, complaint response
 - ☐ Provide an employee hotline for information and assistance
 - ☐ Provide a complaint resource with reasonable follow up
14. Remote Work Policies – consistent application
 - ☐ Establish a remote work policy that provides determination of eligibility
 - ☐ Require work production logs approved by the supervisor
 - ☐ Establish appeal procedures
15. Vulnerable population - pregnant employees, immunosuppressed, high risk (age, COPD)
 - ☐ Recognize special ADA considerations for those with compromised health
 - ☐ Special procedures in place for those high risk who may not come to work indefinitely
 - ☐ Determine medical validation requirements
16. Workers' Compensation – Health care workers, Public Safety
 - ☐ Determine what constitutes a work related transmission
 - ☐ Require public safety to maintain contact logs
 - ☐ Establish a claim review process between the TPA and public entity coordinator
17. General Citizens – right to access public building: ability to perform health screen, first amendment issues
 - ☐ Monitor State guidelines for restricting City access
 - ☐ Determine through task force any PPE requirements, social distancing or screening requirements obviously with legal consultation
 - ☐ Understand limitations based on First Amendment rights as they relate to the health crisis

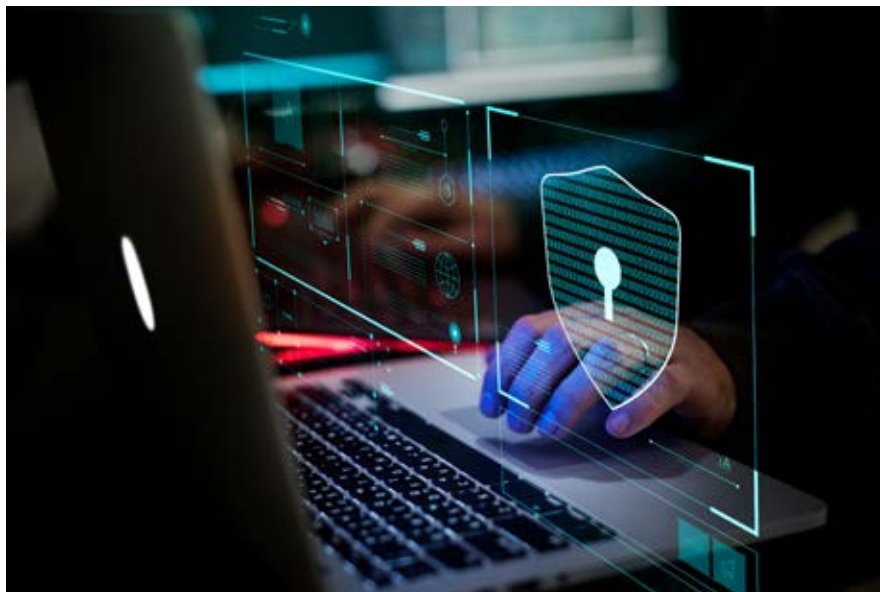
18. Tenants: requirements for those leasing City spaces and when City services are tenants, requirements for landlord and fellow tenants
 - ☐ Establish requirements for tenants renting City spaces during the health crisis
 - ☐ Determine what landlord requirements are for City leased space in private structures
19. Notices and Signage – post restricted access, mask requirements etc.
 - ☐ Ensure that adequate notices and signs to communicate access and PPE requirements to access City buildings
20. Jail – prisoners: adequate medical care, isolation
 - ☐ Determine jail medical plans for treating increased patient load
 - ☐ Determine isolation options for large volume of inmates with security issues
 - ☐ Determine legal early released options for non-violent prisoners who will require a place to stay as a condition for release
 - ☐ Expect requests for additional release through personal attorneys, State, Federal and the ACLU
21. Contracts and vendors – force majeure, safety program requirements, contract deadlines effected
 - ☐ Understand force majeure may provide allowable disruption of supply and construction contracts
 - ☐ Stipulated supply or completion dates with penalties may be amended
 - ☐ Establish alternative supply chain and/or service vendors
 - ☐ Purchasing will establish emergency contract guidelines
22. CARES Act 457 plans individuals taking loans and time frame to pay back
 - ☐ Update information on 457 plans and communicate to employees
 - ☐ Establish an information resource for employees to understand benefits and liabilities of the CARE Act
23. City or County services shutdown for economic reasons furlough
 - ☐ Establish an advanced furlough plan inclusive of critical retentions
 - ☐ Determine post furlough benefits such as paid leave, sick and/or sustaining health insurance
 - ☐ Include a re-entry program based on priority of need that is defensible

OUTSIDE CONSIDERATIONS:

1. Public parks
 - ☐ Develop a park closure plan based on State or local requirements
 - ☐ Communicate restrictions to the public through appropriate media
2. Festivals
 - ☐ Communicate restrictions for festival and establish early cancellation dates
3. Social distancing
 - ☐ Communicate social distancing requirements typically based on State requirements
 - ☐ Establish guidelines on how police will address non-compliant gatherings
4. State compliance
 - ☐ Monitor State requirements or guidelines with effective communication to the public
 - ☐ Publish local updates on the COVID-19 or other applicable communicable diseases
5. Business restrictions
 - ☐ Determine enforceable business closure requirements during the pandemic
 - ☐ Determine gradual re-opening plans for specified businesses based on governor's decree or guidelines

CYBERSECURITY

CYBER EVENT RESPONSE CHECKLIST



With many more employees working remotely during COVID-19, there are myriad cybersecurity threats to public entities that may have not previously been an issue. This section outlines some of the cyberthreats and response best practices.

IT BEST PRACTICES FOR CYBER SECURITY

- ☐ Have IT schedule and track all patch updates to software to reduce risk.
- ☐ Install anti-virus software on all end points to ensure up to date.
- ☐ Install fire walls to enable containment of a cyber attack.
- ☐ Encrypt all data at rest or in communication flow including cloud services.
- ☐ Set up Multi Factor Authentication for employees to access intranet using remotely located devices other than their desk workstation. (smart phone, iPad, laptop, home computer).
- ☐ Classify data and systems, and define user roles with least privilege model.
- ☐ Inventory all devices connected to entity intranet and software.
- ☐ Monitor privileged user account activity for inappropriate behavior.

EMPLOYEE BEST PRACTICES FOR CYBER SECURITY

- ☐ Define user security policy and educate employees.
- ☐ Train employees on cyber security, privacy and awareness to protect the entity network and data.
- ☐ Implement strong user password policy and require password change every 30 to 60 days.

- ❑ Scan employee external devices for malware before remote access if given to the network.
- ❑ Test security of employee laptops, iPads, smartphones, home telecommuting desktops, zip drives, external storage, and other external devices before allowing connectivity to the network.
- ❑ Add multifactor authentication (MFA) for employee remote access to the network.
- ❑ Install emergency shut down application on smart devices and laptops to deactivate if reported stolen or lost.

VENDOR AND GUEST BEST PRACTICES FOR CYBER SECURITY

- ❑ Scan guest flash drives, and laptops for malware before access if given to the network.
- ❑ Test security of third party devices used in your business.
- ❑ Test and request proof of cloud and other service provider security measures to protect your entity data.
- ❑ Use contractual language to hold third parties accountable for cyber event losses they cause to your entity.
- ❑ View and approve third party cyber security policies before engaging in a contract.
 - ❑ Scan vendor software before implementing on a network to ensure adequate review of vendor needs and monitoring prior to giving vendor network access to install the software.
 - ❑ Change default passwords on vendor products prior to connecting them to the network.
 - ❑ Within vendor contracts include language on vendor responsibility for confidentiality of personal identity information (PII) and personal health information (PHI), cyber liability insurance requirements for the vendor, and language for indemnification from the vendor should they cause a cyber security or privacy breach of your data.

More on the [Risks of Using Third Party Vendors](#)

DEFINING A CYBER EVENT

A Cyber event may include any of the following:

- Virus intrusion which damages data or makes data inaccessible
- Ransomware that restricts access to data and promises release if ransom paid
- Stolen passwords or unauthorized access to private identity information (PII) of third parties
- Unauthorized access to medical HIPAA protected data on third parties
- Unauthorized access to credit card information, or bank account information
- Social engineering leads to funds from a target entity being redirected to a false or unauthorized account.
- Distributed Denial of Service (DDOS) attack that makes site access unavailable on the internet
- Website defacement
- Server hijacking for cryptocurrency mining which slows down computer server

QUICK RESPONSE TO A CYBER EVENT

- ❑ Secure evidence and document all decision and actions.
- ❑ Disconnect the affected computer(s) if ransomware or virus is suspected.
- ❑ Have IT change user password for affected employees as soon as possible to block hacker use of stolen email to infect others or access to emails (current and historical), and cloud data files.
- ❑ Convene Cyber Incident Response Team to review event and determine next steps.
- ❑ Report cyber event to insurer.
- ❑ Contact cyber attorney as approved by insurer.
- ❑ Inform senior leadership and message employees as needed to inform and warn.
- ❑ Inform law enforcement of the attack.
- ❑ Draft a preliminary statement for public information officer to use if needed.
- ❑ Define cyber claim coverage, self-insured retention, and track expenses of response.

- ❑ Hire a cyber attorney approved by your insurer, and review current requirements for affected persons/businesses notification, State and Federal notification, credit card industry notification, and credit bureau notification. (Likely step #2 after notifying the insurance carrier as step #1)
- ❑ Tip: funnel all written communication on the event through your privacy attorney to invoke the attorney/client privacy privilege.
- ❑ Set a notification timeline as suggested by cyber privacy attorney.
- ❑ Conduct forensic investigation – through your cyber attorney (privileged and confidential protections will apply if done correctly) - to identify unauthorized user and ensure unauthorized access has ceased. Your insurer may suggest a forensics firm for hire.

The following steps should be coordinated with your cyber attorney and insurance carrier:

- ❑ Use forensic investigation to create a listing of any third parties affected by the security/privacy breach, and what information may have been compromised.
- ❑ Based upon the number of affected persons/businesses, decide whether to use a communications firm approved by insurer to send notifications and manage a call center or have the entity itself send notifications and take inquiry calls. Have all calls directed to the same responder.
- ❑ Hire an identity theft protection firm approved by your insurer to offer this service to affected person(s) in notification.
- ❑ Draft affected person(s)/business notification letter and offer of identity theft protective service to send out by certified mail within timeline required by State and Federal law following discovery of a cyber privacy/security event which may have compromised personal/business data.
- ❑ If required by your State, inform the three major credit rating bureaus of the cyber event which may have compromised the data of specific affected person(s) within the time period required by your State, and other applicable regulatory bodies.
- ❑ Keep documentation of affected persons/business reached by certified mail and of other notifications made to meet legal requirements.

- ❑ If the required threshold of verified communication to affected parties cannot be achieved within the required timelines as applicable under State, Federal, or other regulatory body guidelines, create and release a public notice and post this on the entity website as required by State and/or Federal law.
- ❑ Consider providing a press release when a public notice is posted to your website on the cyber event. (Note, middle of the week may be best for release).
- ❑ Update the statement for public information officer to use if needed.
- ❑ Maintain documentation on the cyber event for response to third party claims should these be received.

RISK MANAGER PREPARATION

- ❑ Create a Cyber Incident Response Team. Positions to consider for inclusion are IT Director, HR Director, Risk Manager, Chief Attorney, Public Information Officer.
- ❑ Conduct an annual risk assessment to inform of areas to improve upon. A third party vendor may be used for assessment.
- ❑ Assign follow up and track steps taken toward remediation of identified areas for improvement.
- ❑ Familiarize yourself with your cyber insurance policy and its coverages, event notification requirements, limits, any special coverages, any special tools provided to you as an insured.
- ❑ Identify vendors acceptable to your insurer for; cyber attorney, forensics, cyber privacy/security event notifications and call center, identity theft protection services for affected person(s), public relations firm. Create a quick contact list for these.
- ❑ Conduct table top exercises at least annually with the Cyber Incident Response Team.

ADDITIONAL STEPS TO TAKE TO ENSURE CYBERSECURITY

- Corporate equipment preferred [Remote Access Methods Pros and Cons](#)
- Secure corporate equipment to [disable remotely if lost or stolen](#)
- Train employees to notify IT immediately if their work smartphone, laptop or workstation is lost, stolen or compromised. (Link to example form)
- Encrypt data at rest and in-transit [Best Practices for Data Encryption](#)
- Join [Multi State Information sharing and Analysis Center](#) for updates on cyber threats
- Communicate cyber security updates to employees when increased vigilance is needed
- Strengthen login password requirements [Password Strength Defined](#)
- Use [multi-factor authentication \(MFA\)](#) for increased security at login
- Regularly update software, and monitor the releases of [software updates and patches](#)
- Increase [cyber security training for employees](#)
- Update cyber incident response plan to address increased remote working link to cyber incident at PRIMA document
- Review and update a telework security policy that defines [telework, remote access, and bring your own device \(BYOD\) requirements](#) and [NIST Cybersecurity Framework](#)
- Review Cyber insurance policy to understand coverage and conditions [How Does Cyber Insurance Work? by Travelers](#)
- Secure conference calls [Secure conference call privacy](#)
- Examine increased data storage which may be needed to record online meetings
- Research requirements that inform when you need to record and save online meetings
- Personal equipment concerns to address
 - » Public Records Request
 - » Legal Hold / eDiscovery
 - » Data Retention Policies (conference call recordings)
 - » Confirming current antivirus software
 - » Does employee have broadband internet
 - » What are you going to do about employee expenses
 - » Session and screen lock timeouts must be according to best practices
 - » Is the personal computer shared with others in the household
 - » Ethernet installation
 - » Password secured wifi
 - » Cyber insurance policy ramifications
 - » Potential fines and penalties from data privacy or security breach
 - » Outlook 365 no phishing alert option

