IUPAT & Affiliated Funds

INFECTIOUS DISEASE PREPAREDNESS & RESPONSE PLAN

JUNE 9, 2020
DISCLAIMER - LEGAL STATEMENT

Please be advised that some or all of the information contained in this document may not be applicable to affiliates or other places of work.

We strongly recommend that before implementing any of the ideas contained herein you carefully evaluate, and consult with outside legal counsel as appropriate, the legality, applicability and potential efficacy of this information in your place of business.

Please also note that this is a “living” document that may be updated at any time given the fluidity of this situation.

IUPAT and Affiliated Funds bear no responsibility for any circumstances arising out of or related to the adoption, or decision not to adopt, any of the practices or procedures contained herein.

Infectious Disease Preparedness and Response Plan

During these unprecedented times COVID-19 is having a major impact around the world and in our communities. We are facing a threat not only to our livelihood, but our safety and health, even our very lives. As the construction industry experiences an unprecedented crisis, our goal is to protect the safety of our staff, students and members as well as others that may be exposed to this health threat.

While we learn something new each day about this COVID-19 threat, there are some common sense guidelines that we can all take to reduce our risk and protect the lives of workers on the job, both during and after this crisis. OSHA also recommends employers prepare an Infectious Disease Preparedness and Response Plan to help guide protective actions against COVID-19.

In response, the IUPAT, working in conjunction with the Finishing Trades Institute, Pension, the Labor Management Partnership and industry experts, has developed employee, and student guidelines. This plan has been created specifically for the purpose of establishing guidelines for all employees, members, students and instructors that come to our facilities during the COVID-19 pandemic. We are taking immediate actions to reduce the possibility of contamination or spread of the virus. To reduce the impact of COVID-19 outbreak conditions, it is of utmost importance that all staff adhere to this plan.

These guidelines have been established to do our best prevent infection and transmission of this virus to staff through contact with other staff, family members, contractors, vendors, and other members of the public. Other risk factors may include individuals 50 or older, or those who have chronic health conditions such as diabetes, lung disease, cancer, heart disease, kidney disease, and severe obesity. We will do our best to adhere to all recommendations and guidelines that are disseminated from the Center for Disease Control (CDC), World Health
Organization (WHO), Maryland State Department of Health, OSHA and guidance from other city, state or federal authorities. Given the rapidly changing conditions and environment of this crisis, this plan may be updated as guidelines change. As an organization, we will utilize our Communications, Compliance and Training teams, management and supervisory staff, to obtain and distribute timely information to all staff.

Policy Statement

It is the duty of IUPAT and Affiliated Funds to present a workplace free of recognized health and safety hazards as mandated under the preamble of the OSH Act of 1970 under Section 5(a)(1,2) as stated: “Each employer shall furnish to each of its employees, employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to its employees; shall comply with occupational safety and health standards promulgated under this Act.” As Coronavirus is a known hazard and the disease it causes could have significant health effects, including death, and could potentially be present on any worksite; its risk to workers will be assessed and controls shall be implemented and reviewed on an on-going basis. All trades and workers shall be governed under this Plan while working at this site.

Introduction

It is now well understood that transmission of the COVID-19 virus can occur easily though contact with infected persons expelled droplets (from breathing, talking, coughing or sneezing) in air which then create airborne aerosols traveling distances of 27 feet or more and through cross contamination of surfaces. Therefore, it is important to evaluate a workplaces risk factors which contribute to transmission of COVID-19 between workers (and the general public including workers family members) and then develop and implement control methods to reduce those risks. Certain factors will increase a person’s risk to infection, while other factors will decrease the risk. The main risk factor of infection is whether or not a person is around those who are sick. People who are working during the COVID-19 pandemic are at increased risk if they frequently interact with potentially infected or infected individuals and/or work in areas where surface contamination may be present. Furthermore, risk will be increased for those spending a significant time indoors, and in groups. These risk factors enhance or deteriorate by the quality (or lack thereof) of your ventilation systems. Unfortunately, it is possible for a COVID-19 infected person to not show symptoms or only have mild symptoms and still infect
others. This Plan will therefore implement a combination of different controls in an attempt to reduce the risk of COVID-19 transmission to as low as possible.

Five controls exists and three of them are currently available to us:

**Elimination**: physically removing the hazard. For COVID-19 we may consider a vaccine as the only way to eliminate the hazard. At the time of the development of this plan no vaccine is available.

**Substitution**: replacing the hazard – Not an option for COVID-19.

**Engineering controls**: isolate people from the hazard - barriers, ventilation, contagion zones, etc.

**Administrative controls**: change the way people work to reduce exposure – policies, work practices, social distancing, individual behavior, etc.

**Personal Protective Equipment (PPE)**: protect the worker with PPE, respirators, masks, face shields etc.

**Scope**

This plan will make every effort to utilize *engineering* and *administrative controls* as well as *PPE* to protect our greatest assets. All on-site personnel, students, instructors, members, including visitors, are required to comply with this Plan. Due to the high transmission potential of the COVID-19 virus, and it’s potential to effect multiple workers, disciplinary and or termination procedures shall be implemented for site personnel violating the policies and procedures of this Plan. Students, instructors, members, and visitors, who do not comply risk temporary or permanent expulsion from the campus. This Plan pertains to all areas of the workplace (active work areas, staging areas, break areas, changing areas, gyms, cafeterias,
bathrooms, etc.) as the potential for COVID-19 transmission is possible anywhere employees, students, instructors, members and visitors are physically located.

**Organization, Authority and Responsibility**

In order to develop, implement and maintain the effectiveness of this Plan, it is important for all stakeholders to clearly understand the responsibilities inherent in their job duties. Below are the minimum requirements necessary to remain compliant with this COVID-19 Plan.

**Workplace/Campus Management Plan: Responsibilities**

**Employer**

- Develop, implement and maintain a IUPAT and Affiliated Funds COVID-19 Workplace/Campus Management Plan
- Designate a worksite COVID-19 Officer: **Erica, DeStefano**, MBA, HR/Compliance
- Develop, deliver and maintain a training course as outlined in the Plan for all on-site personnel, students, instructors, members, and visitors
- Fund to the level appropriate to ensure compliance with this Plan and the applicable OSHA Standards, CDC guidance and applicable State and Local government rules;
this includes funds for purchasing of vital equipment, disinfectants and cleaners and additional workers where necessary as well as funding of all related procedures

- Ensure to the best of our ability that all known and current aspects of COVID-19 transmission risk reduction are captured in this Plan and that those aspects are effectively transferred through training sessions to all site personnel and visitors

**COVID-19 Officer (CO)**

- Communicate to IUPAT and Affiliated Funds the level of resources required to ensure compliance with this Plan (PPE, cleaning products, work staff, work schedules, etc.)

- Conduct Workplace Hazard Analysis (JHA)/Workplace Safety Analysis (JSA) for COVID-19 exposure and implement controls where necessary to reduce transmission risk.

- Develop and implement a procedure to conduct daily symptom screenings for employees, students, members and visitors

- Establish a “return to work” policy based on current CDC guidance

- Provide the appropriate amount of time for training and other Plan elements to supervisors, workers, and visitors to ensure compliance with this Plan

- Work with Supervisors, and Workers to ensure Plan compliance and effectiveness

- Review and revise the Plan as Federal standards or guidance changes as well as new information for the implementation of best practices

**Supervisor**

- Ensure that workers receive training on this Plan

- Assure that personal protective equipment required for compliance with this plan are accessible to all site personnel and visitors

- Ensure site-wide compliance with this Plan

- Identify and document Plan deficiencies followed by communication of deficiencies to the Covid-19 Officer in a timely manner

- Provide authority to affected workers to “stop work” when their health and safety is at risk due to Plan deficiencies.
Investigate, document and control Plan deficiencies which may increase transmission spread and seek worker input for improvement

**Employees, Students, Instructors and Members**

- Will adhere to and fulfill all Plan related requirements (e.g. reading the Plan, training, accessing PPE, following the requirements, etc.) during work time
- Read and understand the Plan and sign/date that they have done so
- Comply with this Plan and its procedures to help reduce the spread of COVID-19
- Consult with a supervisor or Covid-19 Officer whenever there are any questions regarding implementation of COVID-19 transmission risk reduction procedures
- Report any concerning deficiencies in the Plan to the Supervisor or Covid-19 Officer
- Follow appropriate safe work practices including use of engineering, administrative and personal protective equipment (PPE) controls
- Report all hazards, incidents and accidents to supervisors as soon as it is safe to do so
- Exercise “stop work” when Plan deficiencies are assumed or identified; record the deficient situation and immediately communicate “stop work” reasoning to Supervisor

**Visitors and Instructors**

- Visitors shall read, understand, receive training and follow this Plan
- Visitors will adhere to and follow applicable worker requirements as listed above
- Visitors shall not modify Plan procedures
Basic Infection Prevention Measures

Employer’s Commitment

- **IUPAT and Affiliated Funds** will ensure that the facility is clean and disinfected prior to any students or trainers permitted onsite per CDC guidelines.

- **IUPAT and Affiliated Funds** will disinfect all equipment, gauges and common areas used specifically for training and general office use on a daily basis or more frequently as needed.

- **IUPAT and Affiliated Funds** will ensure that there is a screening process in place to take the temperature of all employees, students, members, instructors, visitors and contractors. Anyone presenting with a temperature of 100.4 and above will be denied entry.

- **IUPAT and Affiliated Funds** will have all students and instructors fill out a Covid-19 questionnaire and assessment prior to being allowed into the training facility and will be provided the same guidance that must be agreed to prior to arrival.

- **IUPAT and Affiliated Funds** will provide training to visitors, instructors, and students. We will also require them to complete training prior to them being permitted onsite.

- **IUPAT and Affiliated Funds** will help avoid exposure to the virus by limiting contact with others and maintaining a social distance of six feet or more away from others during work activities, training sessions and meetings.

- **IUPAT and Affiliated Funds** will support respiratory etiquette and hand hygiene for students, instructors, and staff:
  - Provide soap and water in the facility. If soap and water are not readily available, alcohol-based hand sanitizer that is at least 60% alcohol must be. If hands are visibly dirty, soap and water should be chosen over hand sanitizer. Ensure that adequate supplies are maintained.
  - Place hand sanitizers in multiple locations Time to encourage hand hygiene.
  - Hang posters or signs that encourage hand hygiene and help stop the spread, at the entrance to your facility and in other areas where they are likely to be seen.
  - Encourage individuals in the building and at times insist that masks be worn at appropriate times.
  - Discourage handshaking – encourage the use of other noncontact methods of greeting.

- **IUPAT and Affiliated Funds** will evaluate, improve and remedy the engineering controls such as the HVAC system and clean water opportunities within acceptable constraints.
Basic Infection Prevention Measures (continued)

Employees, Students, Members, Visitors, and Contractors

- Mouth and nose coverings are required upon arrival to the building. These face coverings must be worn upon entering the building, while moving about the building (breaks, file rooms and using copy machines etc.) and when leaving the building. When seated at your desk you can use your own judgement with regard to wearing a mouth and nose covering.
- Wash their hands often with soap and water, especially after going to the bathroom, before eating and after coughing, sneezing, or blowing your nose.
- Practice social distancing — keep at least 6 feet of distance between yourself and others and avoid crowds.
- Wash your hands when they are visibly soiled and after removing any PPE.
- Cover mouth and nose with a tissue or cloth garment while sneezing or coughing.
- Avoid touching face, eyes, nose and mouth before thoroughly washing your hands.
- Avoid contact with sick people.
- If you are sick, stay home and call your health care provider and notify your supervisor that you are sick and will not be working or attending class as the normal protocol dictates (e.g. calling the Compliance/HR line and notifying supervisor).
- Avoid handshaking, hugging and other intimate types of greetings.
- Avoid crowds, especially in poorly ventilated spaces.
- Avoid unnecessary errands — we recommend that everyone considers ways to have essential items, like food and other household supplies, brought to your house through online delivery services or through family or social networks, understanding that we have no authority to require you to do so.

General Administrative Control Measures

General Workplace Transmission Risk Reduction

Workplace social distancing

- One of the most well-advertised risk reduction control is social distancing in an attempt to reduce encounters between infected and susceptible (those that do not have the virus) individuals. The current CDC guidance is that if you have to be out in public, stay at least 6 feet from other people, however, research has shown that it is possible for the virus to be carried upwards of 27 feet.
- Therefore, the greater distance that you can place between you and another person, the greater the reduction of risk that you may become infected. In addition, recent reports have stated that as many as 50% of the population may carry the virus without
symptoms or mild symptoms, so you may not know if someone has the virus. To reiterate, the farther you can stay away from other people, the greater protection you are giving yourself

- Avoid working in groups; work alone (at least 6 feet apart) if possible and if it is safe to do so
- Interactions between workers when picking up or delivering equipment/materials will be minimized; schedule deliveries during times when worksite occupancy is low and organize staging of equipment/materials to minimize movement on site

**Contamination Reduction, Cleaning and Disinfection**

Since COVID-19 may survive outside of the body upwards of 72 hours, it is important that we limit touching high contact items/areas and clean and disinfect them as much as necessary to reduce the risk of contracting COVID-19 through contamination transfer from our hands to our eyes, nose and mouth.

*The following contamination reduction, cleaning and disinfection methods will be used at this worksite:*

- Workers are encouraged not share other workers’ PPE, phones, or other work tools and equipment
- This site has a “non-contact policy”, site personnel are not to shake hands, high five, etc. while the pandemic is on-going
- Workers are required to use their own food containers and water bottles from home
- Soap and water wash stations will be placed outside of portable toilets and located at common areas (e.g. break areas, tool, cribs, etc.)
- Signs reminding site personnel to avoid touching their eyes, nose, and mouth, frequently washing their hands, covering coughs/sneezes, locations of wash stations and social distancing policies will be posted around the site in common areas Hand washing guidelines will be posted at each wash station which will include: wash your hands often with soap and water for at least 20 seconds;
  - Before entering the Workplace and before you go home
  - After touching high-touch areas such as door knobs, handles, ATM key pad, etc.
  - When hands are visibly dirty
  - After going to the bathroom
  - After blowing your nose, coughing, or sneezing
  - Before eating or drinking
- Frequently touched objects (including tools), surfaces and areas will be cleaned and disinfected frequently with an EPA’s Registered Antimicrobial Products for Use Against Novel Coronavirus SARS-CoV-2
Employees – the following directly affect you, some things are new and may require your attention

Temperature Checks
- All employees will have their temperature taken upon arrival at the building
- Should you be found to have an unacceptable temperature of 100.4 degrees or higher you will be required to leave the premises until you have been fever free for forty eight (48) hours. During that time you may use personal leave or vacation time. So, if you are sick or have a fever, please stay home. If during the day you don’t feel well please advise your supervisor and or compliance immediately

Checking in/out from the work site
- Upon arriving at the workplace/campus there may be a line for temperature checks, maintain at least six feet between you and the person in front of you. Do not congregate in groups while waiting to enter or leave the workplace
- There is signage throughout the building to help you safely distance from others

Alternate Work Days, Telecommuting and Work Hours
- Alternate on-site work days, and telecommuting from home schedules have been established to reduce the risk of infection by reducing the number of workers on-site at any given time. Changes to the schedules can only be made by your direct supervisor.
- You will need to read, understand and comply with the new Telecommuting Policy
- WORK HOURS - Each employee’s telecommuting work hours must be completed during the regular work hours stated in the Collective Bargaining Agreement (CBA).
- During the work hours the employee must be available by telephone/google chat/email.
- OVER TIME - Employees who are not exempt from the overtime requirements of the Fair Labor Standards Act (FLSA) will be required to accurately record all hours worked using ADP. No overtime is permitted while teleworking without prior written approval from the supervisor.
- CLOCKING IN - go to ADP website (workforcenow.adp.com) go to myself tab -> Time & Attendance -> My time entry. You will clock in and out using this screen. You will only be able to use your IUPAT issued laptop to do so.
- LEAVE POLICY while telecommuting - The leave policies, flex schedule, and mis-swipes will remain the same as if you were in the office. If you will be using unscheduled leave when are scheduled to work from home; you are still required to send an email to EAGST@iupat.org with a copy to your supervisor or call the Compliance Department at 410-564-5948. If you do use leave you are still obligated to input the leave through ADP.
- EQUIPMENT /SECURITY- we will provide an employer-owned laptop to each employee who is telecommuting. Telecommuters must follow all remote system security policies and procedures, as well as the normal computer policies. Also,
because tokens will not work remotely, telecommuting employees will be required to install the DUO mobile app on their personal cellular devices. The security of the IUPAT property at an alternative work site Computer Security is just as important when working remotely as when in the office. While telecommuting, reasonable precautions must be taken to protect IUPAT hardware, software, and information from theft, damage, and misuse.

- **SAFETY**- Employees are expected to maintain their home workspace in a safe manner, free from safety hazards.

**Workplace Sick Policy**

- The IUPAT and Affiliated Funds COVID-19 sick policy will be followed while the pandemic is on-going. Note: If you think you have been exposed to COVID-19 or if you have symptoms of infection call your healthcare provider immediately and stay home except to get medical care and separate yourself from other people in your home until expert medical advice is given from your medical care provider.
- Workers shall stay at home and not come to work if they are experiencing COVID-19 symptoms or otherwise feel sick.
- A worker will be asked to leave the worksite when they start feeling sick or when they have been in close contact with a confirmed positive COVID-19 case. If someone goes home from the site due to sickness, the area where that person worked will be immediately disinfected with an EPA approved disinfectant (see contamination reduction, cleaning and disinfection section below).
- Workers are strongly encouraged to self-identify symptoms of fever, coughing, or shortness of breath each day, before the shift, mid-shift, and at home to their supervisor. The access coordinator will ask a sick worker if they have been in close contact with other personnel on site that day.
- IUPAT and Affiliated Funds will implement a symptom check for workers upon arrival at the site which will include no contact thermometers and a questionnaire asking if the worker has experienced any fever, trouble breathing, shortness of breath etc.
- Should you arrive on campus and be found to have an unacceptable temperature of 100.4 degrees or higher or answer Yes to any of the symptom questions, you will be required to leave the premises, go home (home isolation) and contact your medical provider. The CDC guidelines for when you can discontinue home isolation and return to work will be followed for recovered sick workers wishing to resume work. During that time you may use personal leave or vacation time.
- So, if you are sick or have a fever, please stay home. If during the day you don’t feel well please advise your supervisor and or compliance immediately.
- If you are a student from out of the area. You will be housed in a safe comfortable, designated location on campus until you are admitted to a hospital or are able to safely return home.
Actions To Take If You Are Sick:

- If you are experiencing the CDC identified virus symptoms, such as coughing, fever, sore throat, and/or shortness of breath, contact your physician or your local Department of Health to be screened and if appropriate, be tested for the virus. Stay home. DO NOT GO TO WORK. If mildly ill, most infected persons recover at home.
- Notify your supervisor immediately if you are sick, and/or experiencing any of the symptoms described in #1.
- Do not visit public areas.
- Do not take public transportation.
- Wear an approved face-mask or N-95 respirator when in public to avoid transmission to others (*OSHA has suspended the enforcement of fit-testing during this crisis. However, unless in a crisis or emergency, ensure that you have been evaluated and fit-tested prior to donning a respirator). 
- Contact a physician or your local Health Department Columbia to be screened via telephone and if necessary, be scheduled for testing and/or treatment. Do not visit an emergency room.
  - Maryland Department of Health, 877-463-3464 or 410-767-6500
  - District of Columbia Department of Health 202-442-5955
  - Common Wealth of Virginia Department of Health: Alexandria 703-746-4996, Fairfax County 703-246-2411, Prince William County 703-792-6300
- Do not visit a physician without an appointment and guidance from a physician.
- Isolate yourself from family members and use a separate bathroom and bedroom.
- Cough and sneeze into a tissue and discard in plastic bags; or cough into your elbow and always away from others.
- Take all precautions to maintain a clean environment including the washing of hands, disinfecting touch-points such as doors, handles, tools, equipment, counters, phones, etc.
- Stay a minimum of a 6 feet distance away from others.
- Do not share clothing, sleeping quarters, utensils, glassware, towels, bathrooms, etc., with any family member.
- Maintain electronic communication with physicians, family members and your supervisor as to your status.
- If you experience warning signs that reflect any of the following, seek medical attention immediately by calling 911:
  - Difficulty breathing
  - Pain or pressure in chest
  - Bluish lips
  - Confusion
- The decision to discontinue home isolation for persons with confirmed or suspected COVID-19 should be made in the context of local circumstances. Options include a
symptom-based (i.e., time-since-illness-onset and time-since-recovery strategy) or a test-based strategy. **Do not return to work** unless you have been cleared using one of the strategies below and have supporting documentation:

1). Symptom-based strategy
   - Persons with COVID-19 who have symptoms and were directed to care for themselves at home may discontinue isolation under the following conditions:
     - At least 3 days (72 hours) have passed since recovery defined as resolution of fever without the use of fever-reducing medications and improvement in respiratory symptoms (e.g., cough, shortness of breath); and,
     - At least 10 days have passed since symptoms first appeared.

2). Test-based strategy
   - Persons who have COVID-19 who have symptoms and were directed to care for themselves at home may discontinue isolation under the following conditions:
     - Resolution of fever without the use of fever-reducing medications and
     - Improvement in respiratory symptoms (e.g., cough, shortness of breath), and
     - Negative results of an FDA Emergency Use Authorized COVID-19 molecular assay for detection of SARS-CoV-2 RNA from at least two consecutive respiratory specimens collected ≥24 hours apart (total of two negative specimens).

Workplace meetings
- No more than 10 participants a distance of at least 6 feet between each participant shall be maintained

Breaks and Lunch
- On-site personnel will not all take breaks and eat lunch together, everyone will be expected to maintain at least 6 feet between each other as this will help maintain limited contact between workers

Bathroom Visits
- Be mindful of all surfaces touched and always wash your hands with soap and water
- Do not congregate or wait in line while waiting to use bathrooms or portable toilets
Common Congregation Areas
- In an effort to help ensure at least six feet is maintained at common congregation areas (e.g. worksite check-in/out locations, at elevators, etc.); distance identifiers (tape on floors, cones, etc.) shall be placed every six feet to guide site social distancing efforts.

Masks, Face Coverings, Gloves and Tissue
- Face Coverings are required and will be made available upon request. However, personal face coverings (either homemade or store bought) may be permitted, but if the CO decides they are not adequate, the individual may be required to use IUPAT and Affiliated Funds supplied PPE upon arrival to the building.
- These face coverings must be worn upon entering the building, while moving about the building (breaks, file rooms and using copy machines etc.) and when leaving the building.

Smoking Policy
There will be no smoking or vaping allowed within 20 feet of any entrance or exit of the buildings. Extended social distancing should be practiced when out for a smoke or a vape since smokers will not be wearing a mask at the time. We recommend that you stand 30 feet apart from the next smoker.

Facility
Lion’s Grill/Lunch Breaks
- The Lions Grill and dining area is closed until further notice.
- You may bring lunch, use delivery or carry out from local restaurants.
- You may eat lunch at your desk. We ask that you be mindful of food with strong odors out of respect for those around you.
- It is our intent to keep the refrigerator and microwave machine plugged in at this time. The refrigerators will be emptied daily at 4pm. Small personal coolers may be brought in if you prefer its use over community refrigeration.
- The vending machines in the amenities rooms are available for use but you should use tissues or napkins when using the buttons and maintain proper social distancing.

Gym Access
- There will be no access to the gym until further notice. However, the bathrooms in that area may be used.

Breakrooms
- All breakrooms will be closed, no sitting and gathering will be allowed.
There will be no use of tables or chairs in those areas. When using the water cooler in the break room be sure to use a tissue or napkin to press the buttons.
No more than one person at a time will be allowed in the break rooms.
Be mindful of all surfaces touched and always wash your hands with soap and water.
We ask that you all respect each other and look out for yourselves and each other during this time.

**Controlled Access Zones**
- The Department heads may establish Controlled Access Zones to your work area to limit the opportunity for infection and to prevent access from others who have no specific need to be in your workspace.

**OTHER**

**Commuting**
- Commuting to work on public transportation or in groups (e.g. avoid bus, rail, ridesharing, etc.) is not recommended. We recommend that you drive or walk to work on your own but we cannot require you to do so. If driving, park in designated parking areas if they are assigned.

**Students and Instructors will be advised primarily the same as employees:**
- Any student or instructor that is displaying any signs of Covid-19 will not be permitted to take a course at the iFTI.
- All students and instructors will be required to regularly wash their hands.
- Students and Instructors will be required to practice social distancing and to wear a face mask or an N95 when appropriate for instruction and hands on activities.
- Wash your hands when they are visibly soiled and after removing any PPE.
- Students and instructors will have to sign a waiver indicating that they do not have COVID-19, or have not had any known exposure.
- Students and Instructors will disinfect all shared gauges and equipment prior to use, between uses and after the last person is finished.
- Instructors will disinfect all equipment, gauges and common areas used specifically for training daily, during lunch and breaks.

Failure to follow the rules, policies and procedures outlined above could cause an additional close down of our facilities and further layoffs or terminations.

**OSHA**
The following OSHA Laws may relate to the COVID-19 pandemic and will be incorporated and followed in efforts to reduce COVID-19 transmission and to protect the health and safety of workers on this site.
Work at this site may be governed by the following OSHA laws pertaining to the COVID-19 pandemic:

- 1926.25 Housekeeping
- 1926.28 Personal Protective Equipment
- 1926.51 Sanitization
- 1926.59 Hazard Communication
- 1926 Subpart E Personal Protective and Life Saving Equipment
- 1910.1030 Blood borne Pathogen through 29 CFR 1926.21(b)(2)
- 1910.134 Respiratory Protection

**Records**
The CO shall maintain all records related to this Plan, including training, hazard identification, and illnesses tracking in accordance with [the Employer] record retention Program and applicable OSHA Laws.

**Plan review and Updates**
The CO shall review current information concerning the COVID-19 pandemic and the protection of worker health and safety including Federal Laws, orders and guidance, best practices issued through standards of care daily and revise this Plan as often as required until the pandemic is considered closed by the CDC or their State.

**To Learn More and Receive Updates**
You can find greater detailed information on Coronavirus on the following websites. These sites will update their information and guidance as new information concerning the Coronavirus outbreak becomes available so it is important that you check in regularly for updated information until the outbreak has been considered “ended” by the CDC.

- https://www.osha.gov/SLTC/covid-19
- https://www.nih.gov/health-information/coronavirus
APPENDIX A

Telecommuting Policy

Objective

Telecommuting is the practice of working remotely instead of physically traveling to a central workplace. Telecommuting is not an entitlement; it may be discontinued at any time by your employer. Other than as expressly stated, this policy does not change the terms and conditions of employment.

If for any reason an employee does not complete their work in a timely manner, their Supervisor will discuss this with the employee and determine an appropriate course of action, which may include revocation of permission to work remotely.

Work Hours

Each employee’s telecommuting work hours must be during the regular work hours stated in the Collective Bargaining Agreement (CBA). During the work hours the employee must be available by telephone/google chat/email. Employees who are not exempt from the overtime requirements of the Fair Labor Standards Act (FLSA) will be required to accurately record all hours worked using ADP. No overtime is permitted while teleworking without prior written approval from the supervisor.

When clocking in please go to ADP website (workforcenow.adp.com) go to myself tab -> Time & Attendance -> My time entry. You will clock in and out using this screen. You will only be able to use your IUPAT issued laptop to do so.

The leave policies, flex schedule, and mis-swipes will remain the same as if you were in the office. If you will be using unscheduled leave when are scheduled to work from home; you are still required to send an email to EAGST@iupat.org with a copy to your supervisor or call the Compliance Department at 410-564-5948. If you do use leave you are still obligated to input the leave through ADP.

Equipment/Security

The employer will provide an employer-owned laptop to each employee who is telecommuting. Telecommuters must follow all remote system security policies and procedures, as well as the normal computer policies. Also, because tokens will not work remotely, telecommuting employees will be required to install the DUO mobile app on their personal cellular devices. The security of the IUPAT property at an alternative work site Computer Security is just as important when working remotely as when in the office. While telecommuting, reasonable precautions must be taken to protect IUPAT hardware, software, and information from theft, damage, and misuse.

Safety

Employees are expected to maintain their home workspace in a safe manner, free from safety hazards.
APPENDIX B

High Touch Cleaning Checklist:

High touch items are among the most pathogen heavy surfaces in your facility. Routine cleaning and disinfecting of these items, along with frequent handwashing is critical to breaking the chain of infection and creating clean, safe, and healthy environments.

High Touch items include:

- CHAIR HANDLES & BACKS
- COFFEE MACHINES & POTS
- COUNTER TOPS
- DESKTOPS
- DOOR GLASS DOOR HANDLES & EDGES
- ELEVATOR BUTTONS & DOORS
- EMPLOYEE CELL PHONES
- KEYBOARDS & MICE
- LIGHT SWITCHES
- MAILBOXES
- MICROWAVES
- PAPER TOWEL DISPENSERS
- PHONES
- PRINTER/FAX MACHINES
- REFRIGERATOR HANDLES & DOORS
- SINK FAUCETS & HANDLES
- STAIR RAILS
- STAPLERS & STAPLE REMOVERS
- TABLETOPS
- TAPE DISPENSERS
- TIME CLOCKS
• TOASTER OVENS
• TRASH RECEPTACLES
• VENDING MACHINES
• WATER FOUNTAINS

DON'T OVERLOOK THESE COMMON GATHERING PLACES

• CONFERENCE ROOM TABLES & CHAIRS
• OPEN SHARED WORKSPACES
• BREAK ROOM AREAS (APPLIANCES, SINKS, CHAIRS & TABLES)
• RESTROOMS (RESTROOM FLUSH HANDLES, TOILET PAPER DISPENSERS)
APPENDIX C
Union Security and Data Privacy Cheat Sheet

The Union has Policies and Procedures related to data privacy and cybersecurity. Employees of the Union are required to read and be familiar with those policies. However, for quick and easy reference, here is a "Cheat Sheet" that you can keep at your desk for a quick reference guide.

<table>
<thead>
<tr>
<th>Cyber/Privacy Do's</th>
<th>Cyber/Privacy Don’ts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Union Technology for Union work→ Nothing personal</td>
<td>Give out/share your username and password</td>
</tr>
<tr>
<td>Lock your computer when you leave your desk</td>
<td>Download ANYTHING from the Internet</td>
</tr>
<tr>
<td>ALWAYS use 2FA</td>
<td>NEVER use a USB drive</td>
</tr>
<tr>
<td>Use complicated passwords</td>
<td>Reuse passwords</td>
</tr>
<tr>
<td>Be aware of physical surroundings.</td>
<td>NEVER use public WiFi.</td>
</tr>
<tr>
<td>Be aware of people looking over your shoulder at your computer.</td>
<td>Store a laptop in an unattended motor vehicle or Leave a laptop in a public place</td>
</tr>
<tr>
<td>Securely dispose of paper documents that contain Sensitive Data.</td>
<td>Store Sensitive Data on a Personal Device or locally on a company owned device</td>
</tr>
<tr>
<td>Only provide the minimum necessary information.</td>
<td>Leave Sensitive Data out where other people can see it</td>
</tr>
<tr>
<td>ALWAYS ALWAYS ALWAYS report any activity that seems strange or if you click on a link.</td>
<td>Email Sensitive Data</td>
</tr>
</tbody>
</table>

What is PII?

Personally identifiable information (PII) is any data that could potentially identify a specific individual. PII can be sensitive or non-sensitive. Non-sensitive PII is information that can be transmitted in an unencrypted form without resulting in harm to the individual. Sensitive PII is information which, when disclosed, could result in harm to the individual whose privacy has been breached.

Non-Sensitive PII includes: Name, Email, Home Address, Phone Number
### SENSITIVE PII includes:

<table>
<thead>
<tr>
<th>If Stand-Alone:</th>
<th>If Paired with another Identifier:</th>
</tr>
</thead>
<tbody>
<tr>
<td>● SOCIAL SECURITY #</td>
<td>● CITIZENSHIP OR IMMIGRATION STATUS</td>
</tr>
<tr>
<td>● DRIVER’S LICENSE or STATE ID #</td>
<td>● MEDICAL INFORMATION</td>
</tr>
<tr>
<td>● PASSPORT #</td>
<td>● ETHNIC OR RELIGIOUS AFFILIATION</td>
</tr>
<tr>
<td>● ALIEN REGISTRATION #</td>
<td>● SEXUAL ORIENTATION</td>
</tr>
<tr>
<td>● FINANCIAL ACCOUNT #</td>
<td>● ACCOUNT PASSWORDS</td>
</tr>
<tr>
<td>● BIOMETRIC IDENTIFIERS</td>
<td>● LAST 4 DIGITS OF SSN</td>
</tr>
<tr>
<td></td>
<td>● DATE OF BIRTH</td>
</tr>
<tr>
<td></td>
<td>● CRIMINAL HISTORY</td>
</tr>
<tr>
<td></td>
<td>● MOTHER’S MAIDEN NAME</td>
</tr>
</tbody>
</table>

### DSO and Deputy DSO Contact Information

Main Contact - dso@iupat.org  
DSO - Kurt Meyers kmeyers@iupat.org  
Office: (410) 564-5941  
Cell: (301) 943-2035  
Deputy DSO - Bennett Wilkey bwilkey@iupat.org  
Office: (410) 564-5949  
Cell: (443) 936-5785

Keep in mind this list is not all encompassing and that it is your responsibility as an employee of the Union to be familiar with the Policies. This is only intended to be a quick reference guide and NOT a Policy.
APPENDIX D
Cybersecurity and Data Privacy Policy (Main)

<table>
<thead>
<tr>
<th>Policy Area</th>
<th>Cybersecurity and Data Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved Date</td>
<td>7/1/2019</td>
</tr>
<tr>
<td>Approved By</td>
<td>General President Ken Rigmaiden</td>
</tr>
<tr>
<td>Effective Date</td>
<td>11/11/2019</td>
</tr>
<tr>
<td>Current Version</td>
<td>1.0</td>
</tr>
</tbody>
</table>

1. General Purpose

Cybersecurity and data privacy are important to all businesses. Particularly in this day and age where we hear, almost daily, of a cybersecurity breach. The Union takes the security of its employees and member’s data very seriously. In order to make our systems, and the way we use them safer, we have created this Cybersecurity and Data Privacy Policy, along with specific policies that address different aspects of cybersecurity (the "Policy").

2. Definitions
a. **Business Associate.** A person or entity who provides services for or to Covered Entities, as defined under HIPAA, involving the use and/or disclosure of protected health information (PHI). Union functions as a business associate in connection with the relationship it has with its clients and the information its clients share with Union to perform certain audit functions.
b. **Business Associate Agreement.** The agreements between the Covered Entity, as defined under HIPAA, and the Business Associate.
c. **Employee.** For purposes of this Policy, the term includes all permanent and temporary employees and contractors.
d. **Confidential Data.** Is non-public data relating to the organizing, representational and governance programs of IUPAT and its affiliates.
e. **Designated Security Officer (DSO).** The Union employee who is charged with overseeing, monitoring and enforcing the Policies.
f. **Disclosure.** The release, transfer, provision of access to, or divulgence in any other manner, of information to any organization external to the Union.
g. **HIPAA.** Health Insurance Portability and Accountability Act of 1996 (45 C.F.R. Parts 160-164), as well as Health Information Technology for Economic and Clinical Health Act.
(Title XIII of American Recovery and Reinvestment Act of 2009), and its respective regulations as may be amended from time to time.

h. **Information Technology (IT).** IT shall mean the Union’s IT Department.

i. **Member.** An Individual who is a certified Union member.

j. **Protected Health Information (PHI).** Individually identifiable information relating to the past, present, or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care services or products provided to an individual.

k. **Personally Identifiable Information (PII).** Any information that makes it possible to identify an individual, including without limitation, the combination of the individual’s name with: (i) a Social Security number; (ii) passport number; (iii) identification card; (iv) date and place of birth; (v) mother’s maiden name; (vi) biometric records; (vii) financial information (i.e. account number); and/or (ix) username and password. PII shall include, without limitation, any PII of Union’s employees.

l. **Public WiFi:** Any WiFi network that is not the Union Private Network, as defined below.

m. **Sensitive Data.** Includes PII, PHI, and any confidential data.

n. **Union.** The International Union of Painters and Allied Trades (“IUPAT”), Finishing Trades Institute (“FTI”), the Painters and Allied Trades Labor Management Cooperation Institute (“LMCI”), the International Painters and Allied Trades Industry Pension Fund (“IPF”) and Job Corps (collectively, the IUPAT, FTI, LMCI, IPF and Job Corps may be referred to as “Union”).

o. **Union Device(s):** Union-issued desktops, laptops, tablets, scanners, and photocopying machines.

p. **Union Private Network:** ("UPN") The private WiFi network that is password protected.

q. **Union Technology.** Any hardware, software, communications networks, internet, email, WiFi, or any other technology used by the Union, its members or employees to conduct the business of the Union.

r. **Use.** The sharing, application, utilization, examination, or analysis of Sensitive Data by Union.

s. **User.** Anyone who uses or accesses the Union’s systems or Union Technology.

3. **Purpose**

The following are policies, standards, and rules of behavior for the Union related to data privacy and security (the "Policies"). The Policies also govern the use of technology for all of the Union’s employees. The Union is committed to conducting its business with integrity and to comply, to the extent reasonably possible, with applicable information privacy and data security laws. As a non-profit organization with thousands of members in the United States and Canada, the Union has Sensitive Data. The Union takes issues of cybersecurity and data privacy very seriously. The importance of security is demonstrated by Union’s
commitment to creating and maintaining a secure environment and a culture that embraces the basic pillars of responsibility and accountability in dealing with these issues. Union has established the Policies for all employees and their use of the Union Technology. All employees are to use Union Technology in an appropriate manner, consistent with these Policies.

These Policies are intended to protect the confidentiality, security, and integrity of the Union, its employee data, member data, and the Union Technology. Strict observance to these Policies and compliance with all applicable federal and state information privacy and security laws is a condition of employment for all Union employees. Failure to abide by these Policies can result in disciplinary action up to and including immediate termination of employment or revocation of all privileges associated with access to the Union's systems. In evaluating the performance of employees, supervisors will consider the extent to which the employee, during the period being evaluated, adheres to the Policies and standards of conduct regarding privacy and security and participates in the privacy and security-related training and education programs.

The Union will strictly enforce these Policies in the sole discretion of the Union’s designated security and privacy team. Limited exceptions to the Policies may occur due to variations in devices and platforms. However, any substantial changes to this Policy will be done in writing with notice to all employees.

4. Privacy and Security Team
For the purpose of these Policies, Kurt Meyers is Union’s designated Privacy and Security Officer ("DSO") and Bennet Wilkey is the designated deputy Privacy and Security Officer ("Deputy DSO"). The DSO and Deputy DSO are responsible for the development, implementation, monitoring and maintenance of Union’s privacy compliance program and is charged with providing the overall management of Union’s security-compliance efforts.
Main Contact - dso@iupat.org
DSO - Kurt Meyers kmeyers@iupat.org Office: (410) 564-5941 Cell: (301) 943-2035
Deputy DSO - Bennett Wilkey bwilkey@iupat.org Office: (410) 564-5949 Cell: (443) 936-5785

5. Specific Policies and Procedures
The Union has enacted a series of policies and procedures that will govern the data collected, stored, transferred, destroyed, etc. In addition, these policies and procedures govern the use of all Union Technology. In addition, the Union has created an Employee Privacy Notice that demonstrates the Union’s commitment to transparency in the collection, storage and processing activities related to Employee data.
The policies related to the Union’s privacy and security are as follows:

- Physical Security Policy
6. **Failure to Comply**
If any employee or individual fails to comply with the Union's Cybersecurity and Data Privacy Policies, or is found to have violated the Policies in any way, that employee or individual may be subject to disciplinary action, up to and including termination.

7. **Right to Monitor, Audit and Terminate**
In the event that the Union becomes aware of any actions or conditions that violate the Union's Cybersecurity and Data Privacy Policies, it will request that appropriate corrective actions be taken. The Union reserves the right to monitor, assess and audit its systems, emails, text messages, social media or any other form or type of communication, including any hardware, software or applications used by an employee to ensure that its Cybersecurity and Data Privacy Policies are being strictly followed.

### Policy History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
<th>Approved By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>11/11/2019</td>
<td>Original Spec</td>
<td>Kurt Meyers</td>
</tr>
</tbody>
</table>
1. General Purpose

The Union is committed to protecting the confidentiality, integrity, and security of the devices that store Sensitive Data. It is imperative that employees treat Union Devices with utmost care due to the sensitive nature of the data that is stored on or accessed by the Devices. This Device Policy provides the guidelines and framework for all employees using these devices.

Union employees are not permitted to bring their own devices ("BYOD"). Only those devices issued by the Union may connect to the Union Private Network ("UPN"). Employees are not permitted to store any Union Data on their personal devices, this includes photos, emails, text messages, etc. The Union Cybersecurity and Data Privacy Policy is hereby incorporated by reference.

This Device Policy addresses the following:

- Acceptable Use;
- General Device Usage and Security
  - Workstations and Laptops
  - Laptops
  - Smart Phones
- Travelling Device Usage and Security
- Risks, Liabilities and Disclaimers.

2. Policy

   a. Acceptable Use:

The Union defines acceptable use as activities that directly or indirectly support its internal, employment, and membership services. The UPN may not be used at any time to store or transmit illicit materials or harass others. If you are using Union Technology:

- You may access the UPN system.
- You may Store and view Sensitive Data
- You may Conduct all Union-related business
- You may not conduct personal, non-work related business
- You may not store or transmit illicit materials, or harass others
You may not use a personal device:

- To connect to the UPN
- Conduct any Union-related business
- Access Sensitive Data
- Store, maintain or send Union Data or member-related Sensitive Data

b. **General Device Usage and Security:**

The Union expects its employees to respect and protect all Union Technology and equipment. Employees are responsible for the equipment and any devices, personal or otherwise, that store any client or company related Sensitive Data.

Employees are prohibited from using any other network than the UPN and Union Technology to conduct Union-related business. Employees are prohibited from using any application or software that has not been specifically approved, in writing, by the DSO or the Deputy DSO.

All issues of network connectivity, operating system issue or hardware-related issues are supported by IS.

The Union requires that employees use Union Technology in a secure manner. All Union’s workstations and laptops must be password protected. Passwords shall comply with Union’s Password Policy. The Union’s workstations and laptops will automatically lock with a password or PIN if they are idle for more than fifteen (15) minutes. Workstations and laptops are also protected by dual-factor and/or multi-factor authentication (2FA). Employees are required to use 2FA for all Union Technology. Employees are not permitted to bypass, or attempt to bypass, any of the cybersecurity features enabled on Union Technology. Employees are not permitted to change any settings on Union Technology.

Union employees are not permitted to download or upload any software and/or application to Union Technology. Sensitive Data cannot and should not be backed-up to a personal cloud.

USB drives are strictly prohibited and not allowed to be used on Union Technology under any circumstances unless obtaining prior written permission from IT. The only exception to this Policy is the use of USBs on a presentation laptop, which will not connect to the UPN and be regularly audited by IT.

i. **Workstations and Laptops**

The Union must maintain secure workstations and laptops to eliminate or minimize the possibility of unauthorized access to Sensitive Data. Employees should exercise prudence and common sense to maintain the security of information accessible from their workstations and laptops. At a minimum, the following procedures should be followed:

- All workstations and laptops should be locked or turned off when unattended.
- If you access Sensitive Data in a public setting, the employee should be mindful of their location and positioning of the laptop so that unauthorized persons cannot read the computer screens (e.g., by positioning the computer screen to face away from public areas or shielding the computer screen in some other way).
- Potential, actual, or suspected security incidents should be promptly reported to the DSO or the Deputy DSO if there is a reasonable belief that information has been or could have been wrongfully accessed or the workstation has been tampered with in any way.
Whenever a workstation or a laptop is not in use, it should be locked and secured so that only an employee with the actual authority to do so, can enter the username and password to gain access to the device for Union-related business.

Laptops should not be stored or kept in motor vehicles for any period of time when the employee is not physically present in the motor vehicle as well.

In the event that a workstation or laptop is stolen, the incident must immediately be reported to the DSO or the Deputy DSO.

In the event the username and password for any Union's workstation or laptop is compromised (i.e. an employee has reason to believe the username and password has been taken or is being used inappropriately), immediate notice must be given to the DSO or the Deputy DSO and he/she will immediately reset the username and password.

If the employee experiences a data-related incident (a suspected breach of the accounts or username/password) related to his or her personal accounts, the employee should report that to the DSO or the Deputy DSO.

Each employee is responsible for the security, integrity, and confidentiality of information located in his or her office space, workstation, laptop. It is the responsibility of each employee to securely use all Union’s workstations and laptops consistent with the Policies.

ii. Laptops:

Laptops may be periodically audited, on a schedule that is created by the DSO or the Deputy DSO (If the DSO or the Deputy DSO requests a laptop for auditing, the employee must provide the laptop to the DSO or the Deputy DSO).

No Sensitive Data may be locally stored on a laptop. If data is stored locally on a laptop due to an inability to securely connect to Union’s network, the data must be immediately saved to the network immediately upon obtaining a secure connection to the network and deleted from the laptop.

iii. Smart Phones:

The Union provides smartphones and, therefore, you are not entitled to use a personal mobile device to connect to the Union network or send/receive emails related to Union business. IS will implement security controls (as set forth below), will be permitted to access the device upon request, and pull any data off a Union-issued mobile device. Employees should make every effort to limit personal data on Union-issued mobile device. You are required to unlock and provide IS with any access requested at any time. Employees may not put any applications on their Union-issued mobile devices unless previously approved in writing by IS.

Security settings and controls will be set by IT and may not be changed under any circumstances by a Union employee.

- The mobile device is set for full encryption.
- The mobile device locks after 3 minutes of inactivity.
- The mobile device has the highest security settings enabled.

Sensitive Information may not be stored, maintained or sent via email or text message on any mobile device. If an employee violates this Policy and uses his or her own smartphone to conduct Union-related business, those communications are the property of the Union and may be accessed by the
Union upon request. If the device an employee uses for work-related communications is lost or stolen, the employee must immediately report the loss of the device to the DSO or the Deputy DSO.

If an employee violates this Policy and conducts Union business on a personal device, the employee specifically consents to:

- Provide any such communications upon request.
- Allow Union to retrieve its data from the employee’s device, as those communications are the property of Union and not the individual employee.
- Permit Union to remove any of the Union’s data and shut off access to Union’s systems if the device is lost, stolen, or the employee leaves Union’s employment.

**Travelling Device Usage and Security:**

Generally, Union workstations and laptops may not be used at any time to conduct personal, non-work related business. However, certain employees travel as part of their employment with the Union and, therefore, must be able to use their Union Technology for personal use. Traveling Union employees may use the Union Technology in the field or during a business trip to:

- Access personal bank accounts;
- Pay bills;
- Skype, google chat, facetime, etc. with their family;
- Watch movies;

Generally, employees are prohibited from using any other network than the UPN and Union Technology to conduct Union-related business. However, for traveling employees who are going to be on an airplane for two (2) hours or longer, the employee may connect to the airplane WiFi. Whenever possible, instead of using the airplane WiFi the employee should:

- Try to download any work locally
- Not access any of the Union files
- Not access any Sensitive or Confidential Data

To the extent possible, the employee should ask IT to scan or audit his/her laptop prior to reconnecting to the UPN. If the employee must use airplane WiFi, he/she should also try to use the Union VPN.

**Risks, Liabilities and Disclaimers:**

Lost or stolen devices must be immediately reported to the DSO or the Deputy DSO, including and especially all mobile devices.

Every employee is expected to use his or her device in an ethical manner consistent with the Union’s policies and guidelines. Every employee is required to adhere to Union’s acceptable use policy as outlined herein.

In the event an employee has any reason to believe or suspect Union’s workstation, laptop, smartphone or Union’s network infrastructure has been compromised because:

- A password has been compromised.
- They received a suspicious email and clicked on a link.
- They received a suspicious email and provided username and password information. and/or
- They received a suspicious phone call and have provided username and password information.
He or she must **immediately** report that information to the DSO or the Deputy DSO consistent with the Policies. The employee further agrees to work with IT to discover the cause of the infiltration and undergo additional security training, if needed. The Union reserves the right to take appropriate disciplinary action up to and including termination of employment for non-compliance with this Policy, with the most severe disciplinary action taken for employees that fail to report. Reporting a suspected incident will almost never result in disciplinary action.

3. **DSO and Deputy DSO Contact Information**

Main Contact - dso@iupat.org

DSO - Kurt Meyers kmeyers@iupat.org Office: (410) 564-5941 Cell: (301) 943-2035

Deputy DSO - Bennett Wilkey bwilkey@iupat.org Office: (410) 564-5949 Cell: (443) 936-5785

4. **Failure to Comply**

If any employee or individual fails to comply with this Policy, or is found to have violated this Policy in any way, that employee or individual may be subject to disciplinary action, up to and including termination.

5. **Right to Monitor, Audit and Terminate**

In the event that Union becomes aware of any actions or conditions that violate this Policy, it will request that appropriate corrective actions be taken. The Union reserves the right to monitor, assess and audit its systems, emails, text messages, social media or any other form or type of communication, including any hardware, software or applications used by an employee to ensure that this Policy is being strictly followed.

**Policy History**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
<th>Approved By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>11/11/2019</td>
<td>Original Spec</td>
<td>Kurt Meyers</td>
</tr>
</tbody>
</table>