WORK FROM HOME POLICY CHECKLIST

As COVID-19 continues to impact the world, more companies are forced to have their employees work from home to abide by social distancing best practices to help contain the spread, but also allow a business to remain productive while doing so.

This checklist is by no means exhaustive of all the things you may encounter, but it gives you a list of things to consider when creating a work from home policy.

- ☐ Determine if Work from Home is feasible for your organization
  - Are there any customer agreements or internal policies that would prohibit a remote work situation?
  - Do you have a plan for work from home for needed resources, communication, expense reimbursements, software licenses, etc.?
  - Determine what frequency you will revisit your work remote decision to ensure it is effective and still necessary
  - How does this affect your workers' compensation policy?
  - Should you consider liability insurance that covers the employee's home whenever it is being used for the employer's business or should your employees need to maintain homeowner's or renter's liability insurance?
  - Are any home office permit or licenses required by local zoning laws?

- ☐ Is your IT Infrastructure set up properly to support work from home?
  - Does every remote worker have the necessary equipment (computer, monitor, mouse, keyboard, phone, headset, desk, chair, lighting, any other workspace needs?)
  - Does every employee have high-speed internet and a secure connection to access your server and/or any software programs?
  - Surge protector or uninterruptible power supply
  - Network router and firewall
  - Backup drive or personal saver
  - Do any of your employees need to send large files (CAD Files)? Most home networks and computers can't send files that large.
  - Is your helpdesk set up to properly support every remote worker in case needs/problems arise?
  - Collaboration tools (such as Microsoft Teams, Zoom, Skype) in place for every employee that provides:
    - video conferencing
    - chat or instant messaging functionality
    - cloud storage & file sharing tools
    - project management tools
    - virtual collaboration tools
  - Do your employees need training on how to work from home?
  - What is your remote access product? Can it accommodate additional users?

- [ ] Ensure Data privacy and security
    - What is your company's written information security program ensuring that accessing, transmitting and storing of confidential data is safeguarded? You need a work from home policy.
        - This should include permitting access through a VPN or another secure connection
        - Require multi-factor authentication
        - Email security & encryption
        - Restrict access to only secure devices (company issues computer or phone)
        - Password manager
    - What is your plan to send out policy reminders to your employees about the areas listed below?
        - What data is confidential? What kind of applications and data do users need to access and are these applications located on-premises or in the cloud?
        - Awareness around phishing attacks
        - Where, when and how to report an incident
        - Rules around system updates, antivirus updates, and patches
        - Saving company data only on company network (NOT PERSONAL DEVICES)
        - Restricting access to employees only
        - Setting devices to lock after period of nonuse
        - Avoid printing confidential company information unless essential
        - No sending corporate information to personal emails or cloud storage
        - Create a map of where all your users are located. There are data security, labor and privacy laws that vary throughout jurisdictions
    - What type of device is being used on your network and who owns it? Who is tracking this for your business?
    - Obtain a signed acknowledgement that they understand that certain aspects of their employment will be monitored without notice, including computer files, documents prepared or used by the employee in the scope of their employment, and computers and telephone lines during work hours.

- [ ] Employee agreement for remote work
    - Requirements for completed work assignments
    - Maintaining availability during normal work hours (unless a compromise has been set up)
    - Adherence to the company's data privacy, security, and confidentiality policies
    - Timesheets/Records of employee time
    - For employees that are not exempt from FLSA overtime requirements, you will need to carefully monitor their work hours to avoid a violation of unpaid overtime. This can be solved by having employees sign a policy where they are not allowed to work OT without your written consent.

- Communication plan
    - Schedule for regular meetings between management
    - Schedule for regular meetings between managers and their direct reports
    - Plan to effectively communicate confidentiality policy, written IT security programs, business continuity plans, bring your own device policies, etc.
    - Ensure employees understand how to system access instructions and help desk
    - Effective best practices for a safe and effective workspace
    - Regular updates on the state of your business and any changes your team needs to be aware of

- Consider tax issues associated with employees working from home, including those out of state, and reimbursement for costs related to equipment and service-related costs needed to perform work duties.