CIRSA HAZARD ALERT

Published by the CIRSA Loss Control Department | SAFER TOGETHER

Hazard Alert – Telecommuting Safety

Telecommuting can provide numerous benefits to employees and employers alike, but it is not free from potential hazards. Here are some ways to help manage the safety of employees who work from home.

ERGONOMICS

Telecommuting Full Time

Employees who telecommute on a full-time or long-term basis should have a permanent designated workspace. This helps create a more productive environment and helps ensure the area is set up properly from an ergonomic standpoint. Just like in the office, the workspace should have a desk, chair, and equipment following the guidelines below.

While seated in a supportive task chair, feet should be flat on the floor (or on a footrest). The thighs should be parallel to the floor, and the chair back supporting the employee's back should be in an upright position. The chair should also have a properly adjusted lower back lumbar support.

Shoulders should be relaxed, with the elbows resting near the body. The employee should be able to reach the keyboard without extending their upper arms forward. If the keyboard is placed on the desktop, the desk height should be at, or slightly below, the elbow height to provide the most comfort.

The mouse should be placed at the same level as the keyboard.

A free-standing external monitor is ideal as it can be properly adjusted to the correct height and position. The monitor should be in line with the chair and keyboard, at approximately arm's reach distance. The top edge of the monitor should be at eye level. To minimize eye strain, match the brightness of the monitor with the ambient lighting in the room.

Adjustable height desk with dual monitors

Fixed height desk with single monitor

Telecommuting Safety (cont.)

Telecommuting Occasionally or Temporarily

Employees who telecommute occasionally or on a temporary basis may not have the need or space for a permanent designated workspace, but should still make the space as conducive as possible to working. This may be a kitchen table, counter or other area that is available and can be set up properly for conducting work.

The employee should attempt to set up a temporary workspace in the same manner as a full-time telecommuter, which will enhance productivity. This will also allow for greater comfort and reduce strains.

An employee without a full-time designated workspace will likely be working on a laptop. Laptops provide a convenient way for employees to work outside the office, but they are notorious for not being ergonomic.

Track pads attached to the laptop are useful, but can be difficult to use for long periods of time. Simply connecting a wired or wireless mouse can make a significant improvement.

A laptop monitor is typically too low for extended use and may cause neck and upper back strain. An easy and inexpensive way to remedy this is to use a laptop stand, which raises the screen 6-8 inches higher than the work surface. An external keyboard must be used in this configuration to ensure the worker is not placed into an awkward posture while typing.

This setup can be easily moved if the employee needs the space for other purposes, like eating dinner!

Laptop placed directly on table, versus on a stand with external keyboard and mouse.

PHYSICAL HAZARDS

The designated work area should be in an area of the home which is safe and convenient. Employees should evaluate their designated work area to ensure there are no physical conditions which may pose a hazard and cause a potential injury. The details below can be used to help identify these things.

Telecommuting Safety (cont.)

Clutter and obstacles such as cords, uneven rugs, and other items may pose a slip, trip and fall hazard. Just like in the office, the work area in your home should have unobstructed, clean walking surfaces at all times. This includes pathways to the kitchen (break room), restroom, and nearest exit.

The home should be equipped with working smoke detectors which are tested at least every six months. A portable fire extinguisher should be located nearby to ensure quick access.

All computer and work equipment should be plugged into a surge protector to protect against damage. Do not overload electrical outlets with multiple devices as this may cause an electrical failure.

The workspace should have adequate lighting and temperature controls. To avoid issues caused by extreme temperatures; workspaces should not be in garages or detached buildings if they are not properly heated or cooled.

Employees who telecommute should not work from their couch, recliner, bed or other soft surface furniture which places them in an ergonomically incorrect posture. This type of furniture can cause excessive rounding of the back and shoulders, leading to potential musculoskeletal injuries.

CYBERSECURITY

Cybersecurity is a concern at home as well as in the office. If employees are connecting to their own home internet provider, there are a few steps they should take to prevent a data breach.

The Wi-Fi network should be password protected to prevent unauthorized users from accessing the home network. This could allow others to access files and systems from the work laptop without the employee's knowledge.

Employees should always use a VPN (Virtual Private Network) when working remotely, unless the entity's IT Department has other procedures, in which case those procedures must be followed. A VPN connection allows the employee to transmit data from their laptop to your network as if they were directly connected to the private network.

For added security a physical firewall or one built into the router can help prevent unauthorized access. Your IT professional may be able to provide guidance on how to properly configure this for the greatest security.

Employees who work remotely should not use unsecured Wi-Fi networks such as those in coffee shops or hotels. These networks are frequent targets of criminals to gain access to computers and devices. If available under the entity's IT procedures, a Wi-Fi hotspot device or a cell phone hot spot may be a suitable alternative.

Personal data devices such as external hard drives and flash drives should not be used. These devices are easily lost and can transmit viruses if they are compromised. At a minimum, any external flash drive should be password protected. Employees should comply with IT Department procedures related to the use of portable devices.

In addition to cybersecurity, telecommuters should take appropriate steps to safeguard the entity's information and assets. Any documents brought home for telecommuting purposes should be secured from viewing by others. Laptops should not be left unsecured or used for any non-business purposes.