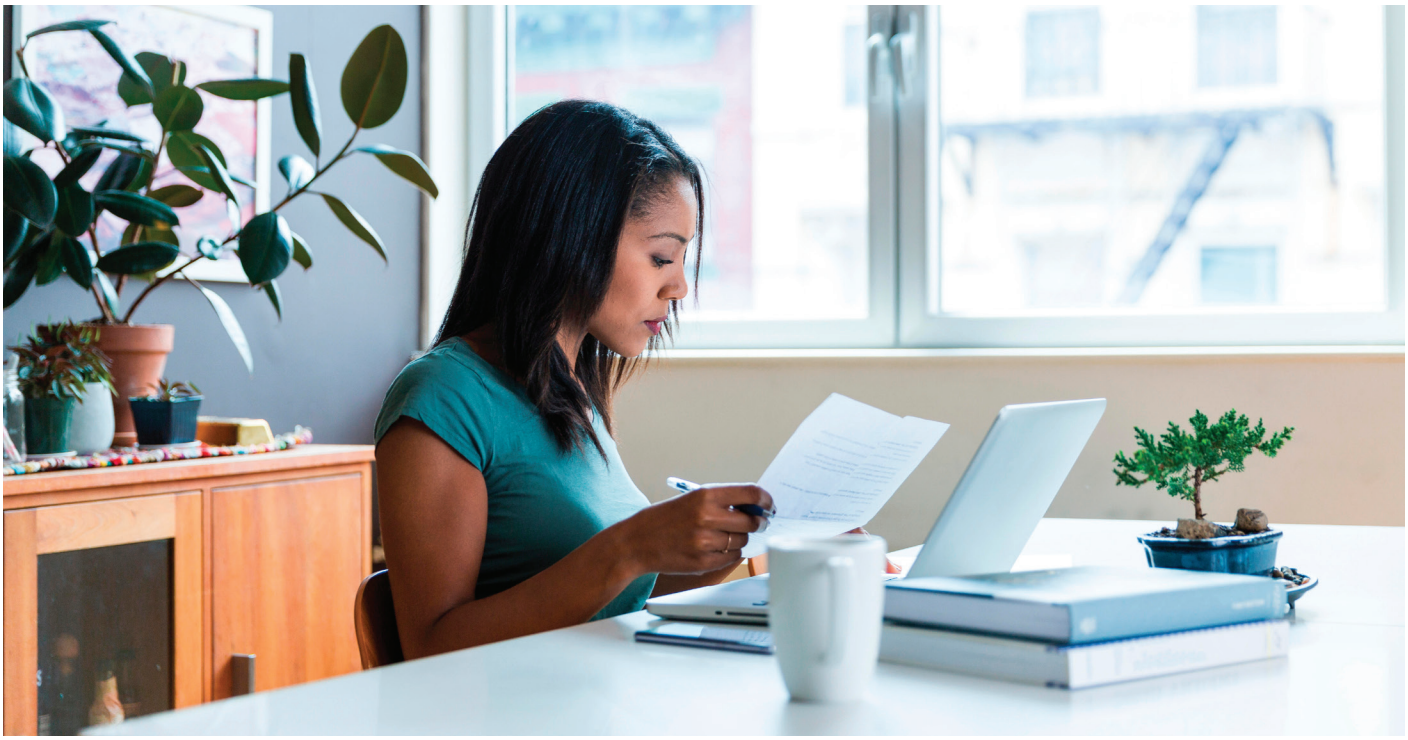
ZURICH

Telework and home office safety

Flexible work arrangements that allow employees to work remotely are growing in popularity at many companies. There are many advantages to telework, however, more employees working from home could result in an uptick in workers' compensation claims. Several safety issues need to be considered when setting up employees to work remotely to ensure a clean, safe and ergonomically sound home/work office environment.



Introduction

The U.S. Office of Personnel Management defines telework as "a work arrangement that allows an employee to perform work, during any part of regular, paid hours, at an approved alternative worksite (e.g., home, telework center). It is an important tool for achieving a resilient and results-oriented workforce. At its core, telework is people doing their work at locations different from where they would normally be doing it."[1] This definition excludes home-based businesses, those who work off-site to catch up on tasks after standard working hours, and those who work remotely when they travel.

Discussion

Remote work options are the top choice for organizations implementing workplace flexibility policies and programs according to a survey conducted by WorldatWork and FlexJobs.[2] Companies and government agencies view telework as a way to control costs while improving productivity, as well as recruit and retain top talent. However, its success depends on using it for the right positions and the right people, as well as implementing an effective infrastructure. Infrastructure to improve communication and collaboration may include internal instant messaging, a company social network and the ability to share desktops.

1 Telework.gov. U.S. Office of Personnel Management. Accessed 25 March 2020. www.telework.gov/about

2 "Telework on an Ad-Hoc Basis Ranks Most Popular Flexibility Option for U.S. Employers." WorldatWork. 12 November 2015.

When selecting which jobs may be possible candidates for telework, consider the following:

- Nature of business – can the work be performed at home or other location
- Level of client contact needed
- Ability to work independently
- Reporting requirements or the degree of supervision required – focus on results management, not physical presence
- Types of equipment required – IT support and involvement is crucial
- Level of security, including remote connectivity and relevant materials

There are many business and employee related benefits of telework. Employers state increased productivity, reduced turnover, reduction in absenteeism, bigger pool of job candidates, reduction in real estate costs, and a decrease in traffic/congestion as top advantages of telework. Environmental benefits can include a reduction in your overall carbon footprint through reduction in gasoline and utilities usage, reduction in air pollution (CO_2 emissions, greenhouse gases) generated and reduction in miles traveled each year via automobile and airplane. Advantages for employees can include increased productivity, reduced/eliminated commute time and balancing of career as well as family priorities. Telework can help businesses and governments successfully recover from natural disasters such as earthquakes and hurricanes, pandemics, as well as acts of terrorism. Some of the potential advantages of using a telework program as a part of business continuity strategy are minimized disruption, reduced recovery expense, a boost in competitive advantage and improved public health.

While telework represents a broad opportunity to improve productivity and reduce infrastructure costs, it also presents some challenges. For example, home offices present unique exposures from an employer's standpoint, as the workstation and related surroundings are not under the employer's control. Employers can, however, be held responsible for injuries sustained by the employee while they are performing normal work-related duties, even if the employee is offsite. The employees also have an added burden of ensuring that their home offices are safe and secure and that their home office operations do not endanger their personal assets and families. A recent study showed that 43 percent of employed Americans said they spent at least some time working remotely.[3] With the increase in telework, employee safety for those working at remote locations requires increased scrutiny.

Guidance

Safety and security issues

Several recent court cases have raised some concerns about telework activities and the potential for workers' compensation claims. Additional court cases may be forthcoming. Consider the following safety and security issues and potential mitigation strategies when establishing any telework or work-at-home program. In addition, the sample checklist, included as an appendix to this RiskTopics guide, can be used by telework employees to help them evaluate telework locations.

Factors to consider	Explanation	Mitigation Strategy
Office space	A physically separate workspace is desirable. Interruptions by family members can be distracting.	• Look for a remote space away from daily home activities. • The space should be large enough to accommodate sufficient room for furniture, equipment and working files. • Temperature, ventilation and lighting should be adequate. • Develop an inventory of equipment, including serial numbers.
Office furniture	The desk and chair will likely be the area most often used in the office. It should be ergonomically sound.	Be sure to choose furniture (desk and chair) that incorporate ergonomic features such as adjustable height, tilt and rounded edges. Please refer to the Zurich brochure "Computer and Laptop tips" for guidance on proper workstation setup.

3 Chokshi, Niraj. "Out of the Office: More People Are Working Remotely, Survey Finds." The New York Times. 15 February 2017. www.nytimes.com/2017/02/15/us/remote-workers-work-from-home.html.

Factors to consider	Explanation	Mitigation Strategy
Business-related visitors / Personal safety	Employees should be discouraged from holding meetings and inviting business clients into their homes, but at the same time, they may encounter delivery persons, technical support personnel, etc. Business-related activities, cards and correspondence may also increase the vulnerability of the home, particularly if the worker is perceived to carry valuable merchandize or equipment at home.	Before allowing any visitors into the home, the following should be considered: • Require the person at the door to show a valid ID, indicating their name, company name and telephone number. • If the visitor is unexpected, consider calling the company the visitor represents to verify the purpose and person making the visit. If possible, do this prior to opening the door for the individual. • Consider using a corporate address or a local post office box for receiving mail.
Climate	In cooler areas, employees may use space heaters to supplement heating.	• Do not place space heaters underneath work surfaces and keep them away from combustibles. Be sure they are placed so that there is adequate air circulation. • Do not plug a space heater in the same circuit as other electronic equipment.
Data security	While many issues relating to data security are similar to office workers, the remote location represents a higher exposure for the worker. Business computers at home may hold sensitive client information, credit card information, debit/checking account numbers, social security numbers, etc. that will pose a problem if that information is illegally accessed from its database. Storing of such information can also lead to potential fraud. Use of unsecured wireless networks also increases chances of hacking.	• Appropriate use of required passwords and encryption should be considered to protect electronic information. • Wireless networks, if used, should always be secured through encrypted passwords. • Advise employees to go into their Wi-Fi router's management software to ensure it's running the latest firmware, which can update security flaws. • Connection to corporate networks should be made using a secure means (e.g., VPN). Promptly install patches and updates, including to their anti-virus software, to all devices on their home network. • Making copies of files by moving a copy to an encrypted network drive may eliminate the potential loss of data in the event of a computer virus malfunction or other issue. • A policy should be developed covering employee use of social networking sites, particularly when accessed from company computers. • Remind employees to be wary of suspicious emails, downloads, USB drives or other things that could introduce malicious software onto their computer and into the network. These could include spoofing and phishing attacks from bad actors pretending to be IT personnel asking for your credentials. • If document security is an issue, office doors should be equipped with a key lock, but not a double-cylinder dead bolt. The filing cabinet where files are stored should also be locked. Discarded paper documents should be secured by using an appropriate shedding device.

Factors to consider	Explanation	Mitigation Strategy
Electrical safety	Overloading an outlet by plugging in many devices can heat the wires to a very high temperature, which may cause a fire. Electrical cords with frayed, cut, exposed wires and missing ground prong can cause electrical shock.	• All electrical equipment and cards should be free of hazards that would cause physical harm (frayed wires, bare conductors, loose wires, or missing ground prong). • Extension cords and multi-outlet power strips should not be permitted. If an extension cord or a multi-outlet power strip is used, make sure the cord or strip is rated for the product, the exterior insulation is in good repair, and protected with ground-fault circuit-interrupters (GFCIs). • Do not run extension cords through walls, doorways, ceilings, floors or over sharp edges. • Ensure combustible materials (e.g., cardboard packing material for computers/printers/docking stations) are not stored within three feet of electrical panels, heating systems, water heaters or other ignition sources. • Consult manufacturer's recommendations when installing equipment. Grounded electrical outlets are required for most products. Surge protectors should be used when making electrical connections to protect equipment against changes in power supply. • Computers and other electrical/electronic equipment should be disconnected from the power source before cleaning. • Liquids and aerosols should not be sprayed into electrical equipment. • Avoid placing beverages and other liquids around energized electrical equipment.
Fire safety	Office equipment such as desks, computers, papers, ink, and toners contribute to the fire load should a fire breaks out in the office area.	• Heat-producing equipment such as computers, heat registers, radiators, etc., should be located to permit adequate air circulation around them. Slots and openings in equipment cabinets should not be blocked. • Halogen bulbs, such as those used in some desk lamps, operate at very high temperatures; adequate clearance from combustible materials such as drapes or curtains is essential. • Limit the use of candles or potpourris or extinguish them when leaving the work areas. • Smoking should be controlled by using ashtrays. The ashtrays should be cleaned daily. • Discard waste paper frequently and do not place waste paper bins near electrical outlets. • Smoke detectors should be installed at every level of the home, per manufacturer's recommendations and tested periodically. • Portable fire extinguishers with a multipurpose rating should be placed in easily accessible locations.

Factors to consider	Explanation	Mitigation Strategy
Life safety/ Emergency preparedness	In choosing a location, consider means of egress in the event of an emergency.	• Accessible and direct means of egress should be available in the event of an emergency. Have an evacuation plan. • An office arranged in the basement or attic may not provide adequate egress. Possible solutions include replacing an attic vent with a large window and having a means available of safely getting from the window to the ground, preferably an approved fire escape. • Post Emergency phone numbers (i.e., hospital, fire department and police department). • A first aid kit should be easily accessible.
Slip, trip, and fall hazards	Electrical cords and wires used for computers, printers and fax machines. Rugs, file cabinets and other household items placed in walking areas and on stairs.	To minimize tripping hazards in a home office: • Ensure walking surfaces and paths are clear and free of clutter, boxes, and other household items. • Place electrical cords along the wall, not across walking paths, under rugs, or in a tangle underfoot. • Never leave file cabinets in the open position, especially the cabinet located near the floor because it creates a tripping hazard. • Ensure drop or area rugs are taped or secured to the floor to prevent the rug from bunching up.
Bookcases	Bookcases may pose a threat of tipping.	• Fasten bookcases to a wall. • Pay attention to the weight limitations of each shelf while loading the bookshelf. Do not exceed the maximum rated capacity.
File cabinets	File cabinets may pose a threat of tipping.	• Look for means to secure the filing cabinet such as securing to one another or to a wall. Place the heaviest loads in the bottom drawers of the filing cabinet.
Stairs	Navigating stairs in multilevel homes can give rise to additional slip, trip and fall hazards.	• All staircases with more than four steps should have a fixed handrail. • Avoid going up and down the stairs with office equipment such as laptops, files, etc. One hand should always be free to hold on to the railing. • Stairs should be kept free of obstructions and clutter to prevent slip, trip and fall incidents.

Conclusion

Telework has become a business necessity for some companies. It can improve employee morale, improve productivity, save energy and help in business continuity planning. While telework has many potential benefits, there are challenges relating to the safety and security of the employee and business data. By evaluating these safety and security issues and taking steps to mitigate any issues found, telework can be a viable option for businesses. A sample checklist is included as an appendix that can be used by telework employees to help them assess their homes and create a safe and secure workplace.

Additional Resources

U.S. General Services Administration, Guide to Telework in the Federal Government:
https://www.gsa.gov/governmentwide-initiatives/telework

WorldatWork: www.worldatwork.org

U.S. Office of Personnel Management, Telework Guide
https://www.telework.gov/guidance-legislation/telework-guidance/telework-guide/

Appendix A: Telework Program Sample Worksite Assessment Checklist

Employee Name:		Company:	
Department:		Business Telephone:	

Dear Teleworker:

The following checklist is designed to help you assess the overall safety of your alternative worksite. Each participant should read and complete the self-assessment checklist. Upon completion, the checklist should be signed and dated by the participating employee and submitted to immediate supervisor.

The alternative worksite is located at *(address)*:	
Describe the designated work area *(e.g., den, bedroom area, etc.):*	

Sample Worksite Assessment Checklist	**Yes**	**No**
1. Is the work area equipped with a centrally monitored alarm system or sufficient locking mechanisms for all points of entry?		
2. Is the employee's computer equipped with virus-screening software, secure wireless connections, VPN, etc?		
3. Are there accessible and direct means of egress from the work area in case of an emergency?		
4. Is the work area equipped with smoke detectors, carbon monoxide detectors, and/or portable fire extinguishers?		
5. Has the presence of flammable/combustible liquids, gasses or chemicals such as pesticides, radon etc., been evaluated?		
6. Is electrical equipment plugged into rated surge protectors to prevent overloading of circuits?		
7. Is all electrical equipment free of recognized hazards that would cause physical harm (frayed wires, bare conductors, loose wires, flexible wires running through walls, exposed wires fixed to the ceiling)?		
8. Does the office area have adequate spacing around furniture with well-secured filing cabinets and bookcases?		
9. Are the phone lines, electrical cords and extension wires secured under a desk or alongside a baseboard (to minimize a tripping hazard)?		
10. Are aisles, doorways and corners free of obstructions to permit visibility and movement?		
11. Do chairs have any loose casters (wheels)? Are the rungs and legs of chairs sturdy? Are the chairs designed to allow easy ergonomic adjustments?		
12. Are all stairs with four or more steps equipped with handrails?		
13. Is the office space neat, clean and free of excessive amounts of combustibles?		
14. Are floor surfaces and covering such as carpets and runners clean, dry, level, and free of worn or frayed seams?		

Employee's signature:		Date:	
Supervisors signature:		Date:	

Note: Employees are responsible for informing their supervisors of any significant changes to their work environment.

March 2020

Zurich
Risk Engineering
1299 Zurich Way, Schaumburg, IL 60196-1056
800 982 5964 www.zurichna.com

A1-112013357-A (03/20) 112013357

BBB ACCREDITED BUSINESS

ZURICH®