

# MANAGING COMPLIANCE FOR A REMOTE WORKFORCE

skillsoft®



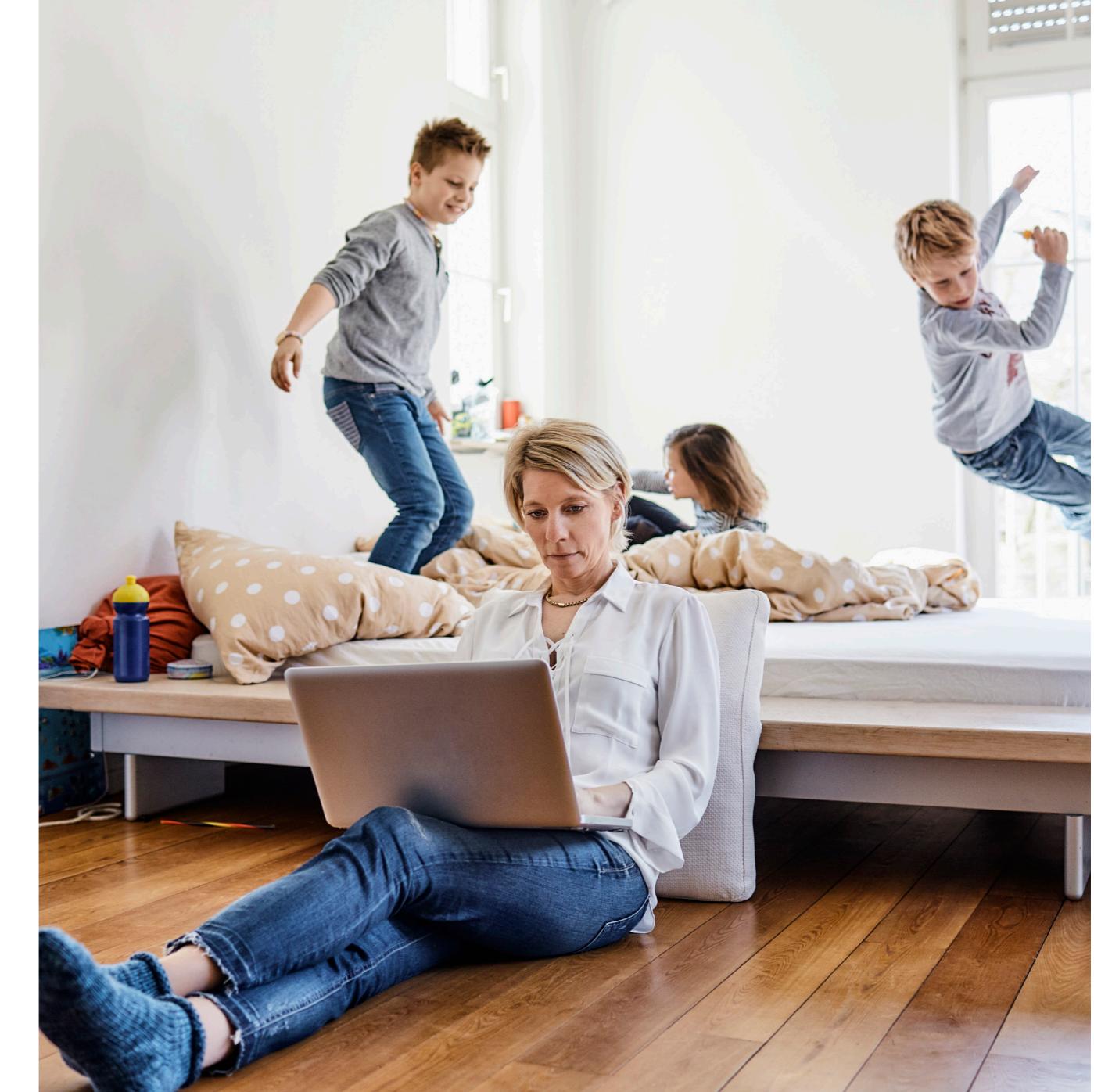
# INTRODUCTION

Prior to the pandemic, only 6% of employees primarily worked remotely. Now, it's expected that 22% of professional workers will work remotely by 2025. Many of these employees may be working remotely for the first time and have not considered the legal and safety hazards of a home office environment. This can result in considerable risk to employers.

Compliance leaders must continue to adapt their safety and legal programs to support both in-person and remote work. Some adaptations for a remote workforce are apparent: compliance policies will require review and possibly need to be updated, employers will need to consider the safety risks of home office environments, and employees will need to be educated on policy changes and risks across the company. The devil is in the details.

This report explores three key risk areas that are most likely to be impacted by the transition to remote work.

- Home Office Safety
- Online Harassment and Bullying
- IT and Cybersecurity Risks



**40.7 MILLION** Americans are expected to work fully remote in the next five years.

# HOME OFFICE SAFETY

We're all familiar with the typical workplace safety guidelines in office environments. With more employees working from home offices than ever before, injuries and illnesses that occur may be considered work-related if the injury or illness occurs while the employee is performing work for pay or compensation in the home.

Over the years, the Occupational Safety and Health Administration (OSHA) has provided limited and conflicting guidance related to home-office safety for employees. It is essential to understand what regulations apply and additional guidance is available to employers to guide your decisions to ensure employees are safe.

**MORE THAN TWO OUT OF FIVE AMERICANS**  
working from home report feeling new or increased  
pain in their shoulders, back or wrists since they  
started working from home.



# OSHA'S REGULATORY PERSPECTIVE FOR HOME OFFICES

OSHA has shared examples of what does and does not constitute work-related injury in home situations.

## THE CASE IS CONSIDERED WORK-RELATED IF:

- An employee drops a box of work documents and injures their foot
- An employee's fingernail is punctured by a needle from a sewing machine used to perform garment work at home, becomes infected, and requires medical treatment

## THE CASE IS NOT CONSIDERED WORK-RELATED IF:

- An employee is injured because they trip on the family dog while rushing to answer a work phone call
- An employee working at home is electrocuted because of faulty home wiring



It befits employers to ensure that employees have safe work environments, even at home. While OSHA won't "hold employers liable for employees' home offices and does not expect employers to inspect the home offices of their employees," there are steps that you can take to protect employees who are working from home.

You will need to consider how employees evaluate their work environments, possibly provide employees with necessary additional equipment, revise existing policies to accommodate home-office work, and provide relevant tools and training for employees. As the employer, you should be aware of hazards in the employees' work area and provide training based on common hazards related to emergency and disaster preparedness, electrical safety, fire safety, ergonomics, back safety, and slips, trips, and falls.

In developing materials to support home office safety, consider flexible tools, such as online training, checklists, and communication, to drive adoption and reinforcement across the workforce.

### [Learn more about Compliance for a Hybrid Work Environment](#)

Of course, as mandated by OSHA, you will want to address potential language barriers among your workforce by providing your materials in the appropriate languages for your workforce.

## **KEY STEPS FOR REMOTE OFFICE SAFETY**

- Understand OSHA's regulatory perspective for home offices and work-relatedness of injuries
- Provide tools and guidance for employees to identify and reduce ergonomic hazards in their home-office environment
- Establish methods and tools for employees to identify common hazards and prevent accidents in the home workspace
- Ensure that your organization's environmental, health, and safety (EHS) policies are clearly communicated, understood, and implemented consistently among employees
- Provide safety training and track participation

# ONLINE HARASSMENT AND BULLYING

When a workforce relocates to working from home, new considerations come into play regarding harassment and bullying. Harassment and bullying can happen in the remote workplace as easily as it can occur in the physical workplace.

When working from home, employees can become less formal and sometimes too casual, increasing the organization's risk. The use of videoconferencing or phones in place of in-person engagement may further the tendency to feel that an interaction can be less formal.

Employers need to ensure that their employees are looking at their behavior through a fresh lens. While bullying and harassment often come in a verbal form, they can exist online as well.

**10% OF WORKERS** report being bullied by email, phone, or social media.

## MANY DIFFERENT FORMS OF HARASSMENT AND BULLYING CAN TAKE PLACE VIRTUALLY. THEY MAY INCLUDE:

- Threats made via email or instant messaging
- Electronic communications that contain racist, gender-biased, or other offensive material
- Spreading rumors about an employee or purposefully keeping them out of the loop on a project that should include them
- Text or instant messages complaining about an employee's work in an excessive manner
- Inappropriate material on display during video calls
- Shutting down someone's contributions to a discussion, for example, by muting their line selectively
- Unwanted invitations to date

Take time to review your harassment policies and update language to ensure they include harassment through digital channels and clarify that misconduct in a remote environment is as serious as if the behavior occurred in person. For example, the policies may need to include visual harassment, such as offensive images, articles, and personal attire.

Once any policy updates are documented, you will want to provide communication and training that reminds the employees of different forms of harassment and bullying that can occur virtually, giving specific examples. Because all employees are operating under increased stress due to the pandemic, their judgment and mental health may be affected. This can lead to increased harassment. Make it clear to your employees that harassment won't be tolerated, even under strained work conditions.

[Learn how to make emotional wellness part of your DEI Strategy.](#)

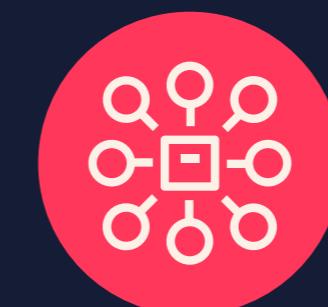
Lastly, to ensure that all employees feel that they have a forum to disclose incidents, you should remind them of anonymous reporting hotlines. A report from SHRM noted that anonymous hotlines accounted for [57% of misconduct reports](#). Remote employees, whose routine check-ins with management might be infrequent or through new channels, should have a place to turn.

## HELP EMPLOYEES ADAPT TO REMOTE WORK

It is sensible to offer help to your employees to adapt to their new work from the home environment.



Provide guidelines for not suitable for work (NSW) items



Encourage vigilance even in informal channels like chat



Discourage the use of unsecured communication channels

# IT AND CYBERSECURITY RISKS

A remote workforce adversely impacts cybersecurity. The scramble to establish teams remotely meant a trade-off and cut corners that increased risks for many companies during the pandemic. Since then, these organizations have worked to bolster their security by using technologies such as VPNs. But technology is only as good as its use—and revisiting and formalizing policies is crucial to reducing risk.

**74%** of organizations attribute business-impacting cyberattacks to remote work tech vulnerabilities

Perhaps the most significant implication of moving to remote work is the impact on a company's sensitive or confidential information. For many employees working out of home offices or transporting materials between offices and homes, the potential for individuals to misuse or accidentally disclose confidential documents increases. To combat this, companies should review and update their records management, data protection, and information security policies, and communicate changes to the team.



Employees also need to be vigilant about security measures. There has been an increase in incidents of phishing and other cybersecurity attacks targeting the home office worker. Hence, employees need to understand that they should be using the secure networks that the company has provided for them when conducting company business. Helping them understand the risks of conducting business on personal devices, and providing the team with guidelines for mobile devices, safely reinforces the right behaviors.

It is also prudent to recommunicate the proper use of company assets. Without day-to-day oversight, an employee may feel emboldened to use company assets, like computers or other equipment, for inappropriate purposes like personal use or fraudulent or illegal activity.

### A FINAL NOTE

Managing compliance for a remote workforce has its complications. With the right efforts to evaluate risks, one must also assess one's current processes and policies and communicate expectations to the workforce. Companies can ensure that the appropriate measures are in place and followed to help reinforce positive compliance outcomes for everyone's safety, security, and well-being.

### KEY STEPS FOR REMOTE CYBERSECURITY

- Evaluate current security and data privacy policies and update them to clarify the employee's role when working from home
- Establish methods and tools for employees to identify and reduce behaviors and situations that increase risk in remote work
- Assess vulnerabilities
- Track installation of patches that fix vulnerabilities
- Provide modular training on IT security and data privacy and track participation
- Consider providing training material in multiple formats to reinforce compliance concepts
- Provide training and tools in multiple languages, localized for regional differences
- Communicate new policies and changes and track attestations to confirm employees' receipt of new material

# ABOUT SKILLSOFT



Skillsoft (NYSE: SKIL) delivers transformative learning experiences that propel organizations and people to grow together. The Company partners with enterprise organizations and serves a global community of learners to prepare today's employees for tomorrow's economy. With Skillsoft, customers gain access to blended, multimodal learning experiences that do more than build skills, they grow a more capable, adaptive, and engaged workforce. Through a portfolio of best-in-class content, a platform that is personalized and connected to customer needs, world-class tech and a broad ecosystem of partners, Skillsoft drives continuous growth and performance for employees and their organizations by overcoming critical skill gaps and unlocking human potential.

Learn more at [www.skillsoft.com](http://www.skillsoft.com).

 [linkedin.com/company/skillsoft](https://linkedin.com/company/skillsoft)  
 [facebook.com/skillsoft](https://facebook.com/skillsoft)  
 [twitter.com/skillsoft](https://twitter.com/skillsoft)  
 [skillsoft.com](https://skillsoft.com)

 US 866-757-3177  
 EMEA +44 (0)1276 401994  
 ASIA +65 6866 3789 (Singapore)  
 AU +61 2 8067 8663

 FR +33 (0)1 83 64 04 10  
 DE +49 211 5407 0191  
 IN +91 (0) 40 6695 0000  
 NZ +64 (0)21 655032

