Project result 3
Continuous Professional Development Curriculum

Module 3

Ethics and Safety

Prepared by GIE

Module 3 - Ethics and Safety Introduction

The Project Result 3 is addressed to **VET tutors,** outlining the **curriculum framework** which enables them to offer training activities adapted to the current needs of small and medium companies to carry out professional work in telework, increase productivity and employee satisfaction, and transform this temporary organization into a situation on the labor market

It aims at developing the **digital, soft**, and **transversal skills** and **competences** of the **employees**, so that they can adapt to the new work environment, without feeling the changes at psychological level, being affected their productivity, motivation, and work results.

Aim of Module 3: Ethics and safety module will empower trainees to cultivate an ethical approach of working remotely preserving their personal and professional safety

Face-to-face learning activities

Theoretical background of ethics and safety when working remotely

Become a master of ethics when working remotely

I am not the slave of online and remote working

Assuring the professional integrity and originality of work

Activity 1
Theoretical background of ethics and safety when working remotely

Learning Outcomes

At the end of this activity, the trainees will be able to:
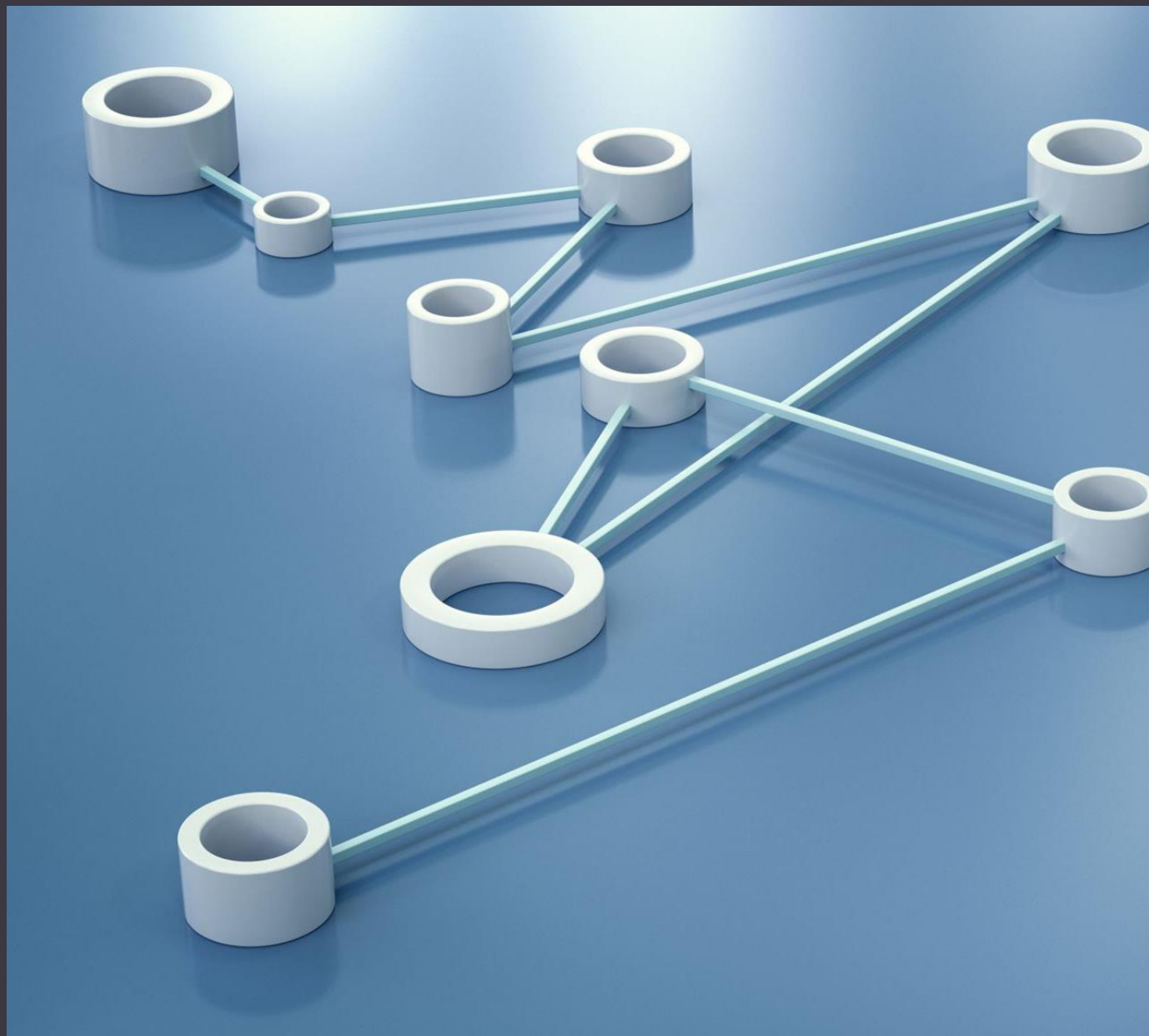
Knowledge

- **K3.1.** Understand the principles of ethics when working remotely

Knowledge

- **K3.2.** Understand the basic elements of online safety

ETHICS

Think and write down the first challenge which crosses your mind that you faced when working remotely. Focus on the concepts of safety and ethics.

ETHICS

- a system of moral principles, the rules of conduct recognized in respect to a particular class of human actions or a particular group, culture, etc.

Ethics in business and SMEs

Business ethics is the study of proper company conduct when it comes to potentially contentious issues including corporate governance, insider trading, bribery, discrimination, corporate social responsibility, fiduciary duties, and much more. The law frequently directs business ethics, however there are occasions when business ethics offer a fundamental standard that enterprises can abide by to win the public's acceptance.

Implementing proper corporate rules and practices with reference to arguably contentious matters is referred to as practicing business ethics. Corporate governance, insider trading, bribery, discrimination, social duty, and fiduciary responsibilities are a few topics that come up in an ethical discussion. The law typically sets the standard for business ethics by offering a fundamental set of rules that companies can choose to abide by in order to win the public's trust.

Principles of Business Ethics

Understanding the fundamental moral principles that guide desired ethical behavior is crucial, as is how a lack of these moral values contributes to the failure of many otherwise bright, talented individuals and the organizations they represent.

Generally speaking, there are 12 business ethical principles.
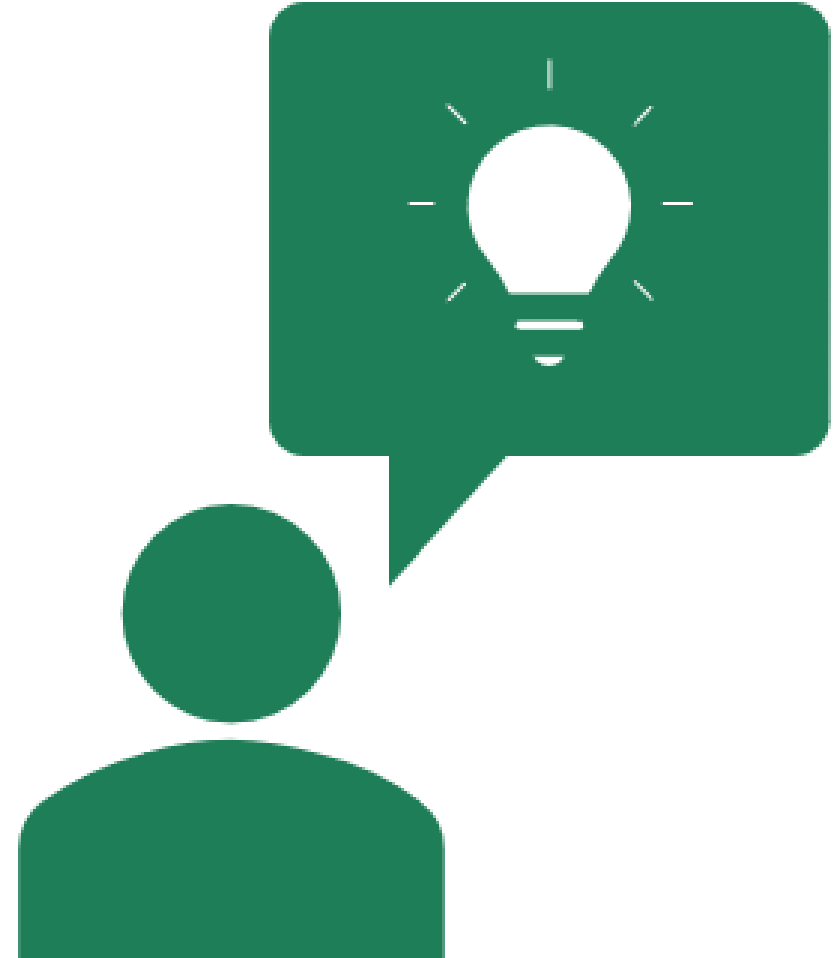
1. Leadership is the deliberate attempt to incorporate the other 11 principles into daily decision-making and behavior in all facets of one's personal and professional life.

2. Accountability is the act of holding oneself and others accountable for their deeds. dedication to upholding ethical standards and ensuring others do the same.

3. Integrity integrates other values, such as honesty, reliability, and trustworthiness. A person with integrity always acts honorably and makes an effort to hold himself to a higher standard.

4. Respect for others: Respecting others is an essential element in creating ethical workplace cultures. Everyone needs to be treated with respect, privacy, equality, opportunity, and empathy.

5. Honesty: Promoting an ethical culture requires telling the truth in all circumstances. Inaccuracies, omissions, and under- or overstating the truth don't help a company perform better. In order to create solutions, bad news should be delivered and received in the same way as good news.

6. Respect for laws: As part of ethical leadership, all local, state, and federal laws should be upheld. Leaders should err on the side of legality rather than taking advantage of a loophole if there is a legal gray area.

7. Promote ownership inside a company, provide people the freedom to take ownership of their job, and take responsibility for your own actions.

8. Transparency: A stakeholder is a person who has an interest in a business, such as a shareholder, an employee, the community where the business operates, or an employee's family. Companies should make sure information about their financials, price adjustments, hiring and firing procedures, wages and salaries, and promotions are accessible to anyone interested in the success of the business without disclosing trade secrets.

9. Compassion: All parties involved in a commercial transaction should be handled with consideration for their needs, including consumers, partners in company, and employees.

10. Fairness: Everyone ought to be treated equally and given the same opportunity. It is probably unfair if a practice or behaviour would make you feel uneasy or prioritize personal or corporate gain over equality, politeness, and respect.

11. Leadership should exhibit loyalty by keeping information private and showing a dedication to the team and the business. Loyalty among management and staff ensures their dedication to optimal practices.

12. Awareness of and care for an organization's environmental implications is crucial in a world where resources are few, ecosystems have been harmed by previous practices, and the climate is changing. Every employee should be encouraged to look for and report remedies to procedures that can worsen already done harm.

Why Is Business Ethics Important

Business ethics are crucial for success in contemporary business for a number of reasons. The most significant benefit of specified ethics programs is the creation of a code of conduct that influences behavior across all levels of employees, from CEOs to middle management to the newest and youngest.

When every employee acts morally, the business develops a reputation for moral conduct. As its reputation rises, it starts to gain the advantages a moral organization enjoys:

- **brand awareness and expansion**

- **improved negotiating skills improved belief in goods and services**

- **customer loyalty and expansion**

- **Draws in talent and investments**

Remote work ethics

Businesses all across the world have switched part or all of their employees to remote working arrangements. Even while this move may be beneficial for public health issues, working remotely involves different ethical issues and fraud prevention considerations than an in-person work setting.

Here's how you can assure the ethics and the effectiveness of your work-from-home procedures and identify areas for improvement.

Productivity

Employers not used to virtual work environments may be concerned about their remote employees' productivity. One way to address productivity is to set clear goals and expectations of what needs to be accomplished and in what time frame. Results should be prioritized over the hours worked or perception of hours worked. Consider holding weekly one-on-one meetings with your team members to discuss progress and remove obstacles to increase efficiency. Highlight achievements and celebrate individual successes—you might consider using a tool to record results and demonstrate ongoing praise for accomplishments.

Some employers have implemented productivity monitoring software to determine how much their employees are working; be careful with this kind of solution as it can send a message to your staff that you do not trust them. You can remind your employees of using their company-issued equipment for business purposes only, which should reduce time spent on non-business websites. You can also forbid time theft in your internal code of conduct and require employees to review and sign it. You can ask hourly employees to complete detailed hours per project and assess how efficient they are with using their time toward achieving goals; they can also sign timesheets attesting that their time is accurate.

WELLNESS

Your staff might still require some time to get used to working from home because it has its own advantages and difficulties. You may support your employees by being aware of their requirements, such as those related to caring for a family member. If the job permits it, employees may benefit from unusual work hours. To provide your employees with additional assistance, think about establishing mentor connections within the organization. Sometimes, employees feel more at ease confiding in coworkers from different groups. Create a confidential channel for staff to provide management with feedback so that problems may be resolved quickly.

Make contact with your staff to inquire about their motivation and mental well-being. Pay attention to culture because it is essential to employee retention and work satisfaction. Maintain company-wide gatherings and foster teamwork through project work and decision-making. Keep your company's beliefs prominent; instead of having them displayed on a wall inside an office building, put them online. To further foster togetherness, discuss your principles at meetings. Highlight the advantages of remote work, such as shorter commutes, more control over your relationships, and a more individualized workspace, and talk about how it fits with your organization's values.

FRAUD

It could be more difficult to build up reliable measures to stop fraud when employees operate from home. Consider the best way to prove that various parties participated in decision-making and financial control. Whether done through a chat message, email, or software, approvals must be kept up to date.

Workers' compensation fraud is a different type of fraud to take into account. It may be increasingly challenging to evaluate whether an accident or illness qualifies for workers' compensation as more employees work from home. By asking your employees to describe or take pictures of their workspaces, encouraging them to adopt healthy routines like taking appropriate breaks, and getting their written consent that their workspaces meet the organization's safety and security requirements, you can reduce the risk of accidents or illnesses brought on by the workplace.

CONFIDENTIALITY

Because of the growing emphasis on cybersecurity brought on by virtual settings, greater care must be taken to protect confidentiality. To safeguard their computers, routers, and other internet-connected devices, teach your staff the proper password conventions and other security measures. Verify that data backup procedures are in place and that backup files are stored in a secure environment.

Asking employees to encrypt their routers, preferably with Wi-Fi Protected Access 2 (WPA2) or Wi-Fi Protected Access 3 (WPA3), and to utilize a virtual private network (VPN) to access files on the company's network are two security measures that could be implemented. Between the employee's computer and the organization's remote server, a VPN creates a secure connection. When discussing sensitive business information, you should also think about removing any Alexa-enabled devices from the room and switching off Siri.

Last but not least, staff should periodically be provided with security training so they are aware of potential dangers and new fraud techniques.

PRINCIPLES OF ETHICS

Same-day shifts - Remote workers are expected to adhere to their regular daily and weekly schedules. Employees' hours will not change from when they were based on campus. Employees are aware that if necessary or required, they can still attend meetings while working remotely.

Employment Terms and Conditions Remain the Same - Regardless of working remotely, an employee is still subject to their current terms and conditions of employment. Pay or salary, benefits, leave requests and approvals, attendance requirements, job-related responsibilities, performance expectations, adherence to the company and departmental policies and procedures, and employee contracts and handbooks are all examples of this.

PRINCIPLES OF ETHICS

Work assignments for employees are decided by supervisors- Employees who work remotely will continue to have regular meetings with their supervisor to receive precise assignments and responsibilities, to define quantifiable outcomes and/or results, and to review both ongoing and finished work. The employee shall accomplish all given tasks in accordance with work procedures that they and their supervisor have mutually agreed upon in accordance with standard operating procedures for the department.

All purchases and relocations of items used for remote work are approved by supervisors - In general, employees are responsible for providing the furniture, equipment (including IT equipment), materials, supplies, and services (such as phone, energy, internet, etc.) required to efficiently carry out the primary responsibilities of their position while working from home. However, if asked by the employee, the supervisor may consent to the acquisition of furniture, equipment (including IT equipment), materials, and supplies for working remotely. Whatever the company purchases, it will always be its property.

PRINCIPLES OF ETHICS

Employees Pay Their Own Utility and Other Living Expenses - Employees are liable for all operating expenses, home upkeep, and any additional fees (such as utilities, phone, energy, internet, etc.) related to using their home for remote work.

Employee is in charge of maintaining the company property - The University's furniture, equipment (including IT equipment), resources, and supplies are the responsibility of employees who work remotely. Except for natural wear and tear, employees commit to return all University property upon request in good condition. Employees consent to not resell, lease, assign, transfer, or otherwise make university property available to any third party.

PRINCIPLES OF ETHICS

The Company Does Not Assume Responsibility or Liability for Employee Personal Property Loss or Damage - The Company does not assume responsibility or liability for employee personal property loss or damage that may occur while the employee is working remotely.

Company Property May Not Be utilized for Personal usage - In general, it is not permitted to convert any company property utilized for remote work to personal usage. Examples include the prohibition against using business electronics (such as computers, laptops, tablets, digital cameras, camcorders, or related supplies like thumb drives) for domestic or private usage. It is not permitted to use the company's tools or equipment for personal projects. Paper and other office supplies from the company may not be utilized for private or household purposes. Only legitimate business may be conducted in company vehicles. No personal use, including carrying out errands for oneself, is permitted. The state ethics laws allow for the de minimis personal use of electronic devices (such as laptops, tablets, etc.) for activities like reading personal email or quickly perusing the internet. Employees can get help with specific ethical queries from the company's interim ethics officer.

PRINCIPLES OF ETHICS

Records on devices- the company data stored on personal or institutional electronic devices or in other ways are subject to the confidentiality policy of the company. Remote workers are accountable for ensuring that all company records, whether kept on private or institutional electronic devices, are appropriately archived and retained in accordance with the law in force and the internal policies.

The Duty of Employees to Promote a Healthful Remote Work Environment - To the degree practicable, employees who work remotely will uphold the same hygienic and secure working environment as their on-site workspace.

PRINCIPLES OF ETHICS

Employees Are Covered by Worker's Compensation - Injuries sustained while performing official tasks at a remote location during regular business hours continue to be covered by the Worker's Compensation Law for remote employees. Any accidents or occurrences at work must be reported right once to the employee's boss and the workers compensation claims manager.

Privacy, confidentiality, and IT security - Employees who work remotely are nevertheless subject to the confidentiality and privacy regulations that apply to company records, personal health information, and employee information. See Employee Privacy Rights and Confidentiality in the Company policy. Additionally, staff members must know the fundamentals of information security and how to encrypt emails when necessary.
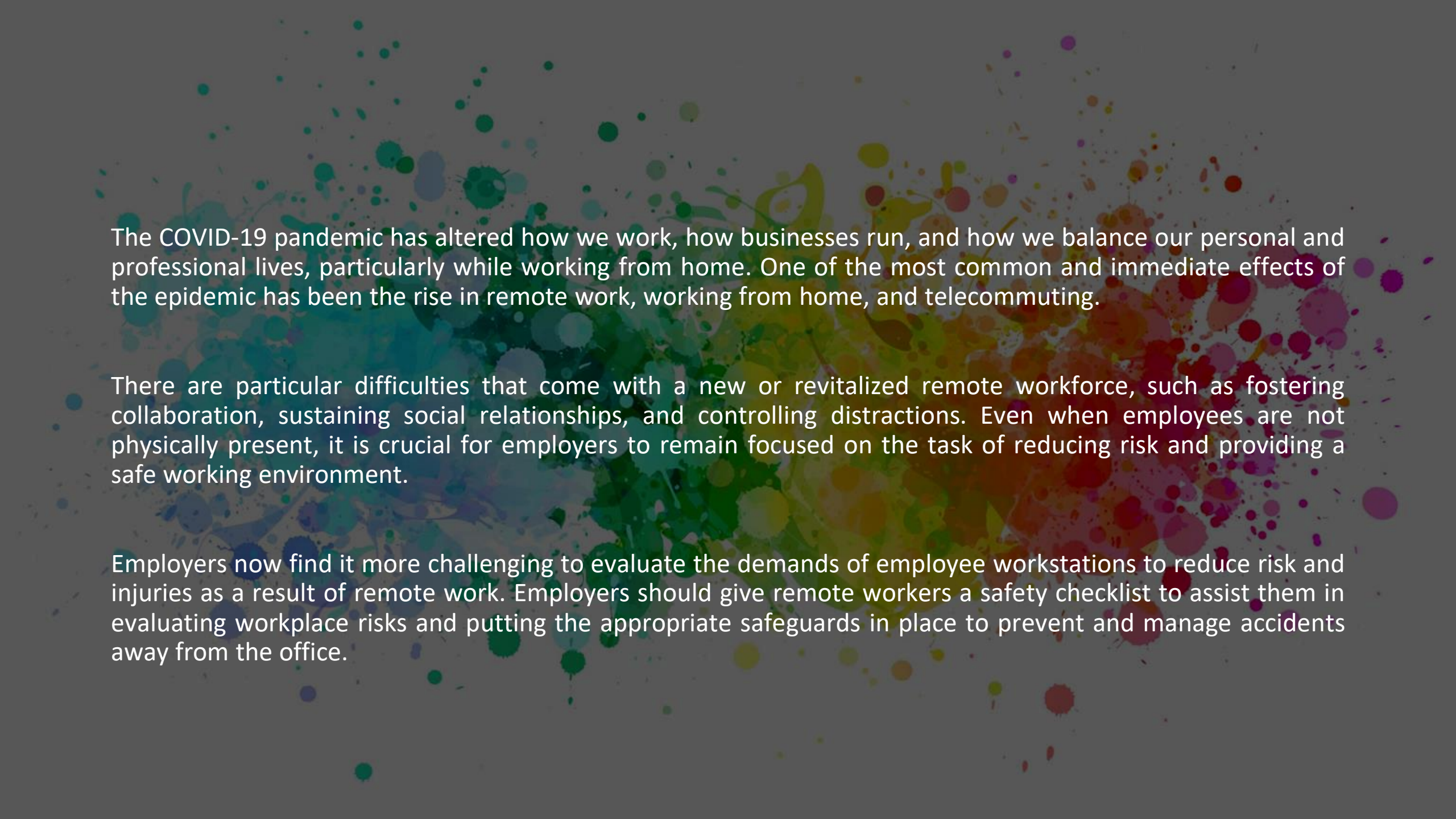
SAFETY
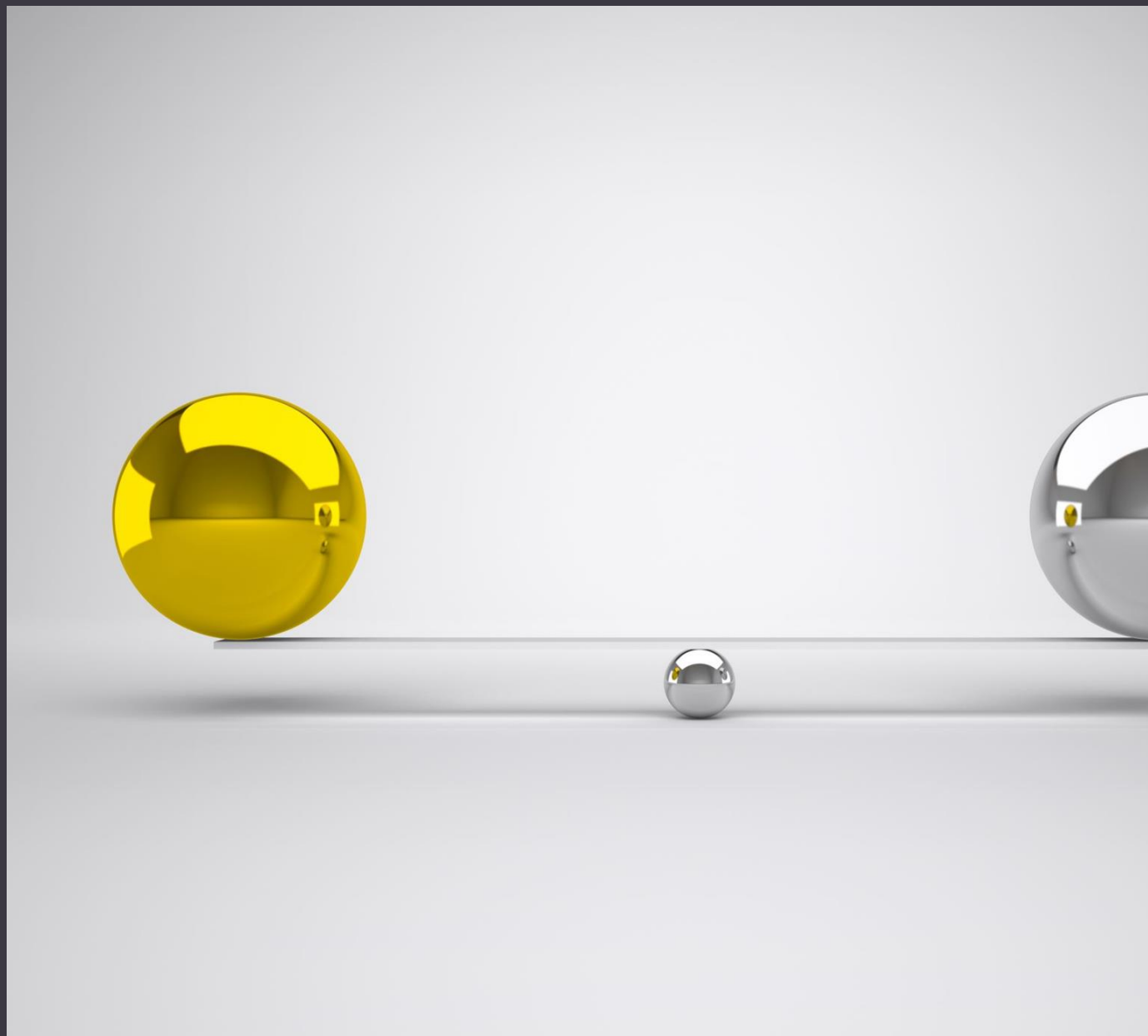
SAFETY

•the state of being safe; freedom from the occurrence or risk of injury, danger, or loss; the action of keeping safe

•Source: https://www.dictionary.com/

The COVID-19 pandemic has altered how we work, how businesses run, and how we balance our personal and professional lives, particularly while working from home. One of the most common and immediate effects of the epidemic has been the rise in remote work, working from home, and telecommuting.

There are particular difficulties that come with a new or revitalized remote workforce, such as fostering collaboration, sustaining social relationships, and controlling distractions. Even when employees are not physically present, it is crucial for employers to remain focused on the task of reducing risk and providing a safe working environment.

Employers now find it more challenging to evaluate the demands of employee workstations to reduce risk and injuries as a result of remote work. Employers should give remote workers a safety checklist to assist them in evaluating workplace risks and putting the appropriate safeguards in place to prevent and manage accidents away from the office.

•As many danger concerns in an office location can transfer to an employee's home area, it is beneficial to develop a safety plan specifically for remote workers. Ergonomic problems, stumbles and falls, and stress brought on by the job, including mental health, are all included. It is not practical to identify every remote work scenario, though.

•In order to lower the risk of illness or injury while working remotely, it is also the responsibility of the employee to make sure they are evaluating their present workspaces and implementing necessary safety protocols.

•Remote work can result in physical harm that lasts a lifetime. Remote employees frequently experience eye strain and musculoskeletal ailments such as neck or back pain. These repetitive stress injuries, also known as overuse injuries, are brought on by inactivity or an improper workstation layout. Long work hours, mental stress, and a lack of social interaction can all contribute to exhaustion and a drop in productivity.

CHECKLIST FOR REMOTE WORK SAFETY ⫴⟶

Ergonomics

• Make sure your workplace adheres to these Mayo Clinic recommendations to avoid weariness and physical harm.

• Select the appropriate area. A good workstation should be well-lit to prevent eye strain, have a suitable work surface like a desk or table, and be removed from busy sections of the house to promote concentrated work during working hours. Move and stand up. Try to alter your posture frequently to lessen muscle tightness and pain. Avoid remaining still for long periods of time.

• Evaluate your posture. Your head shouldn't bend such that your ears are at shoulder level, and neither should your shoulders curve inward or forward. Imagine a cord pulling you upright from the top of your head to prevent you from slouching. By doing this, back and neck pain can be avoided.

• Observe your monitor carefully. Make sure the top of the computer screen is at eye level before positioning it. Thus, neck and eye discomfort won't occur. Try using a wireless keyboard and mouse when using a laptop and raise the laptop on some books to bring the top of the screen level with your eyes.

• Pick the appropriate chair. Your knees shouldn't be higher than your hips when you're seated. This can lessen the pressure on your spine when you are seated and help prevent lower back pain.

Falls, Trips, and Slips

- Common accidents like trips, slips, and falls are just as relevant in remote settings as they are in offices. Ask staff members to check their remote workstation to make sure the floors are free of any potential risks.

- Discard any obstructions from the floor. Toys, cartons, books, and dangling or loose cords are a few examples of this.

- Fix any sagging carpeting and stabilize rugs' raised corners. If the loose portions are stepped on while walking, damaged or frayed carpeting and loose rugs can easily result in trips. In order to prevent tripping, make sure to fix any worn patches.

- Observe your footing. Another location where slips, trips, and falls can happen is on stairs. Be careful not to carry too many goods in your hands when on the stairs if your job demands you to climb or descend flights of stairs. Always keep one hand free to grasp the railing with.

Fire Protection

• For your remote workspace, appropriate fire safety is a requirement, just like in an office setting

• Check the cords. Extension cords and electrical cords must to be in good shape. Make that your outlets are not overloaded with power and that they are not frayed, broken, or have bent prongs. Unplug any cord that feels warm to the touch or is radiating a lot of heat. Use general fire safety precautions.

• Make sure the following are present in or close to your workspace to prevent potential fires: a functional smoke detector At least twice a year, check the batteries to see if they need to be replaced. a fire extinguisher that is operational

• Make sure you routinely inspect your fire extinguisher and use it in accordance with recommended procedures. Fire extinguishers should be kept in a location that is simple to get to, and their physical condition should be checked for dents and hose slits. The locking pin should also be checked, and the pressure gauge should be checked to make sure the needle is in the green.

• Have a fire evacuation strategy in place: To protect everyone's safety, you and your home should be aware of the evacuation strategy. This strategy should specify where you would meet outdoors, away from the property.

Insomnia and Mental Health

- For remote workers, it is even more crucial to manage stress levels and mental wellness in general. You, as the employer, should actively care for the wellbeing and mental health of your remote workers.

- Make sure that nobody is unintentionally working too much. Even so, it's important to urge staff members to take frequent breaks, eat lunch, and, if at all feasible, keep normal office hours.

- Maintain constant communication with your staff. Make time for casual chats to take the place of those that employees on-site would be having at the office while sipping coffee or strolling about.

- Request a workspace from the workforce. As a result, they can work without being distracted in most situations. This will aid in simulating the actual separation between home and work life.
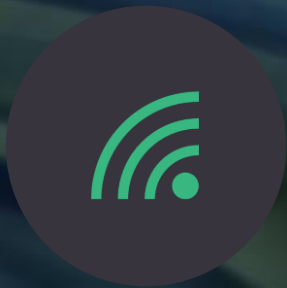
CIBER-SECURITY

•Everyone in the office is accountable for cybersecurity. Your business may prevent becoming the next target of a cyber-attack by reminding your staff of these basic internet safety recommended practices. Learn how to keep your workplace secure online, strengthen your company's cybersecurity defense, and reduce risk by reading the advice provided below.

1. Secure it - In today's businesses, employees may work remotely and are frequently dispersed among several sites. No matter where you choose to set up shop for the day, electronics need to be carefully locked down. Make sure staff members are aware that they should always keep mobile devices, including laptops and cell phones, protected using a strong passcode. Secure passcodes can be created in a variety of methods. While some devices employ a PIN or matrix passcode for authentication, others use biometric scanners. Make sure your text password is different for each account if you're using one.

2. Two is preferable to one - Employees should be compelled to utilize two-factor authentication for all important applications and accounts. It's easy to recall how it operates because it combines any two of the following: Something you possess (like an ID badge or a code created at random)something that defines you (like a fingerprint)something you are aware of (like a password)In addition to the standard password, two-factor authentication adds an additional degree of security. It lessens your chance of becoming a victim of account compromise because hackers need access to both your additional security technique and your account password in order to access the account. Make sure that personnel who access sensitive networks or data must have it.

3. VPN wins the day - Always use a VPN (Virtualized Personal Network) when conducting business outside of the corporate network to safeguard your security. By encrypting traffic, a VPN functions as a secure tunnel over the internet. Employees are able to travel while depending on the defense controls at headquarters by deploying a VPN to your office's secure network. Employees should be required to VPN into a secure network since utilizing unsecured public networks exposes your organization's accounts and data to hackers and compromised infrastructure.

4. Remain vigilant - Everyone at your company, from the founder to the newest intern, needs to keep in mind: if something seems suspect, it probably is! To persuade the receiver to act, malicious actors will use urgent subject lines, billing-related attachments, and spoofed senders. Describe the following email and online browser hints: Never open or download anything from unknown senders, and always hover your mouse over links to be sure you're going to the right URL before clicking. By putting these security best practices into practice, you can stop ransomware and spam from spreading.

5. Training is essential - The effectiveness of your company's cyber protection depends on having knowledgeable employees who can use best practices to thwart threats. You should make sure that your staff members are aware of the fundamentals of cybersecurity, such as how to spot a suspicious email and when to connect via a VPN. SANS is the foremost institution for professionals seeking cybersecurity training, offering courses on a variety of subjects. Their security awareness training courses assist in educating staff on subjects like two-factor authentication, phishing, and other related material.

6. Make a list - What you don't realize you have, you can't defend. Make sure to establish up procedures for tracking all of your company's hardware and software assets. You can quickly identify the devices that are connected to your network and automate the documentation of all the software on business systems by using solutions like an active discovery tool or a software inventory tool. The first two CIS Controls suggestions are, in fact, inventories of hardware and software. As a result, you should give them top attention while taking cybersecurity measures. The CIS Controls are a list of cyber defense measures with a priority order that businesses can use to strengthen their cybersecurity. They contain actions that anyone can perform to fortify systems and stop an attack.

Activity 2
Become a master of ethics when working remotely

Learning Outcomes

At the end of this activity, the trainees will be able to:

Knowledge

- **K3.3.** Identify the challenges in respecting the ethics of working remotely;

Skills

- **S3.1.** Practice self-monitoring;
- **S3.2.** Demonstrate compliance and discipline;

Competencies

- C3.1. Cultivate originality of work.

LEARNING BY DOING
-A-

1. You are part of a new project team in the company.

2. The project needs to be started by scratch: concept, definition, development, approval, implementation, evaluation.

3. Perform a SWOT analysis on the project life-time development

* Keep in mind that:

- *You will work in teams;*

- *The project development needs to be adapted to the fully-remote working environment.*

LEARNING BY DOING
-B-

Highlight the aspects of the SWOT Analysis related on ethics and safety

LEARNING BY DOING
-C-

Replicate to the weaknesses and challenges of ethics and safety when working remotely, in order to show compliance, discipline and cultivate originality in their work

Activity 3
I am not the victim of online and remote working

Learning Outcomes

At the end of this activity, the trainees will be able to:

Knowledge

- **K3.4.** Identify the risks of working online;

Skills

- **S3.2.** Demonstrate compliance and discipline;
- **S3.3.** Practice online safety measures;

Competencies

- **C3.3.** Cultivate a balanced behaviour between personal and professional life;

ROLE-PLAY

We are a full team in a company

→

Positions: accountant, secretary, project manager, assistant manager, project implementation team member, trainer, human resources responsible, work security responsible etc

→

The team is working remotely

→

Enlist: (A) the duties of each job (B) 3 benefits of remote working for the allocated position (C) 3 challenges of remote working for the allocated position (D) 3 risks of remote working for the allocated position

How can we apply the online safety measures and how can we organize the work, to practice safety measures, demonstrate compliance, discipline and assure a proper balance between personal and professional life?

Activity 4
Assuring the professional integrity and originality of work

Learning Outcomes

At the end of this activity, the trainees will be able to:

Skills

- **K3.1.** Apply content development safety measures;

Competencies

- **C3.2.** Preserve professional and personal integrity.

How will I safely develop my work content based on online sources and how will I assure my author rights on the developed work content?

Questions and suggestions

☺ **Thank you!**