INSTRUCTIONS FOR SECURE REMOTE WORK

2021

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

www.huoltovarmuuskeskus.fi

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

Security of supply refers to society's ability to maintain the basic economic functions required for ensuring people's livelihood, the overall functioning and safety of society, and the material preconditions for military defence in the event of serious disruptions and emergencies. The National Emergency Supply Agency (NESA) is an organisation operating under the Ministry of Economic Affairs and Employment. It is tasked with planning and measures related to developing and maintaining security of supply.

Publisher:
National Emergency Supply Organisation
The National Emergency Supply Organisation is a network that works together for the good of Finland's ability to function and the security of supply required to ensure it. It includes the National Emergency Supply Agency and its board, the National Emergency Supply Council and industry-specific sectors and pools.

Author of the report:
This guide was drafted in collaboration with independent experts from KPMG Oy Ab.

Images: Shutterstock

Layout: Up-to-Point Oy

Year of publication: 2021

ISBN: 978-952-7470-13-8

Table of contents

INTRODUCTION

The COVID-19 pandemic has dramatically increased the number of people who work remotely. In response, the Digital Pool has already published a quick guide on how to choose secure tools for remote work. The quick guide is available ***here*** (in Finnish). This guide provides a more comprehensive set of technical and functional instructions for remote work, with the help of which companies can adopt more secure applications and systems related to remote work and develop their remote work guidelines and the know-how of their personnel.

The work on the remote work instructions was started in June 2021. To assess the prevailing situation, the work started with an online questionnaire and a series of interviews conducted in August-September 2021. The purpose of the questionnaire was to collect information on e.g. whether companies offer opportunities for remote work, what kind of hardware (the employer's/personal) and solutions (virtualisation, web applications, etc.) remote work is carried out with, whether device management is used and what kind of instructions companies have on the storage of work equipment, travel, security classification, etc. A total of 125 companies responded to the questionnaire, and the results are detailed in appendix 2. The timing of the questionnaire had a major impact on companies' perspective on remote working due to the effects of the COVID-19 pandemic. The questionnaire results and the observations recorded in the 21 interviews were analysed and utilised alongside other information sources in the drafting of these instructions. This guide is not exhaustive, **nor can companies ensure a sufficient level of information security and data protection solely by following the instructions provided within**. In the end, each company is responsible for establishing information security practices that correspond to their own operating environment, corporate culture and capabilities.

Key observations based on the questionnaire:

- A distributed remote work environment increases the importance of well-understood operating models, processes and practices and decreases natural interaction.
- Companies are well-prepared for remote work overall.
- Half of the respondents did not have any defined guidelines for the remote work environment or requirements concerning the storage of work equipment.
- The most common technical solution for enabling remote work was a VPN connection (88%).
- Strong identification was being used by 76% of respondents.
- 33% of respondents did not have any defined remote access requirements based on security classification.

Based on the questionnaire, companies have faced challenges at least in:

- the establishment, reliability and speed of network connections as remote work increased rapidly
- the performance of networks when employees use the mobile network in more remote locations or population centres

- the interpretation of remote work instructions, such as compliance in home conditions
- the handling and sharing of classified information
- the level of competence of different users, due to which there was demand for plain and simple instructions for users.

Nearly all of the interviewed companies already had remote/flexible working guidelines in place before the COVID-19 pandemic. For some companies, this meant that remote work had been defined in accordance with working time legislation, while others had practical instructions (such as conduct during travel or in public spaces). Based on the observations, the pandemic has had only a minor impact on operating methods – the primary focus has been on ensuring the capacity and functioning of VPN connections. Only very few (if any) changes have been made to written remote work instructions. However, the need for remote work instructions is readily apparent, as employees who transition to remote work can no longer just ask the colleague sitting next to them for help with information security or data protection matters that they are unsure about. Remote work will also continue in accordance with various hybrid models, taking into account customer and confidentiality requirements. Based on the interviews, many companies have invested in reminding employees of information security and data protection issues and promoting employee coping during remote work.

A general observation based on the interviews is that when it comes to protecting information and information security, the same rules apply both at the office and elsewhere. The place where information is handled is largely irrelevant as long as the company's policies regarding the classification, ownership and storage of information have been documented, taught and communicated. The technical solutions that companies have implemented to secure connections, for example, are effective overall, but there is room for improvement as regards content protection. Because of this, the recommendations provided below recommend paying attention to the protection of information content and the implementation of strong identification, for example.

Cover at least the following in your company's information security and other guidelines:

- Secure your network connections:
  - Define which applications and services used by your company are secured with a VPN connection, and automate protected point-to-point connections between terminal devices and the company's network.
  - Only connect devices approved by the company to the company network.

- Define roles and protect content:
  - Define the systems and information that employees have access to in different operating environments in a role-based manner.
  - Prepare classification policies for the information shared and handled within the company.
  - Make sure that strong identification is used with all the methods by which the company's protected information content can be accessed.

- Identify users:
  - Define a password policy for the company that covers e.g. the length, complexity and changing of passwords.
  - Tell employees not to save their passwords in any files stored on their workstations, excluding password management software.

- Make sure that your software and hardware are up to date:
  - Make sure that software and software updates are automatically distributed to workstations.
  - Make sure that hardware drivers and firmware are updated even when working remotely.
  - Do not allow employees to install or update their own software on company computers, unless the employee's work tasks or role require them to do so.

- Provide training and guidance on how to identify risks and protect against them:
  - Organise mandatory information security training for employees on a regular basis.
  - Ensure that the training teaches employees to identify information security and data protection risks and protect against them.

Instruct employees to take care of information security in remote work conditions as well:

- Operating outside of company facilities:
  - Protect information from being seen or heard, including by family members.
  - Do not connect external USB devices to workstations.
  - Change the default passwords of any IoT devices at home during their setup.
  - Recognise the risks associated with travelling abroad and assess the required level of preparedness.
  - Do not charge your phone or laptop with chargers offered by outsiders.

TECHNICAL SOLUTIONS

Securing network connections

The most common and simplest instruction for securing network connections is to avoid public Wi-Fi networks. Some companies consider the personal Wi-Fi networks at employees' homes to be comparable to public networks. This is understandable, considering that home routers and online storage systems are the most commonly cracked devices based on the latest observations of the Finnish Security and Intelligence Service.

Wi-Fi networks are wireless local area networks in which data is transmitted in a kind of plain format. A public Wi-Fi network can be likened to a CB radio: if you are on the right frequency, you can hear everything.

Yle.fi: Open Wi-Fi is attractive – do not forget the risks

There are several different methods for securing network connections. One of them is to instruct employees to use their smartphone's mobile connection instead of their home Wi-Fi connection. Another option is a workstation with built-in mobile connectivity.

Foreign intelligence services use corporate and personal network routers for cyber espionage.

Finnish Security and Intelligence Service press release, 10 March 2021

Some companies forgo efforts to secure personal networks in favour of a secure P2P (point-to-point) connection between terminal devices and the company network. This method is also called VPN (virtual private network) tunneling. The connection is established either automatically or by the user. Once the connection is established, all network traffic is routed via an encrypted VPN tunnel that external parties cannot access. Using a VPN is considered to reduce the risk of hacking and data breaches.

Whether all network traffic is routed via a VPN depends on the company's own policies. Some companies have been forced to increase their VPN capacity in order to route all network traffic through a VPN tunnel. VPN tunnels can also have service-specific restrictions. **As such, companies should define which types of network traffic need to be VPN-protected.** For example, Google Meet, Teams and Zoom can be excluded from the VPN tunnel, freeing up network capacity for other types of network connections.

Workstation security also encompasses other elements, such as personal firewalls and protection against viruses, malware and advanced threats. In addition to these, security can be improved through logging. This refers to the collection of log data by devices connected to the internet and operators for the purpose of later determining what, why and when something has happened, if necessary. More information on logging is available ***here***.

As regards securing network connections, information security can be improved by:

- instructing employees to avoid using public Wi-Fi networks
- instructing employees to replace their personal Wi-Fi connection at home with a (mobile) connection provided by the company or harden their router and always use a VPN connection
- defining which programs and services used by the company are secured with a VPN connection, and automating secure point-to-point connections between terminal devices and the company's network
- utilising other elements as necessary, such as a personal firewall
- configuring browser security settings
- instructing employees on best practices for configuring routers and other network devices, e.g.
  - blocking online access to router settings
  - replacing default passwords with difficult-to-guess and sufficiently long custom passwords, with the recommended length being at least 20 characters
  - hardening the router by closing unneeded open ports
  - updating the router firmware.

Identification and user groups

Strong identification

Strong identification reduces risks compared to only using a traditional username and password combination by adding an additional element to the user identification process. In most cases, strong identification does not replace a username and password, but may hide them from the user for the purpose of streamlining identification. Strong identification can be implemented using several different mechanisms[1], the usability and security of which vary depending on the operating environment and requirements.

There are major differences between companies in regard to the mechanisms approved for strong identification. Attitudes towards biometric identification, in particular, vary considerably due to information security and data protection reasons.

Due to the risks associated with using only a username and password, **investing in the implementation of strong identification is one of the best ways to improve the information security of remote work**. Strong identification should be implemented for all the methods by which the company's protected information content can be accessed instead of being limited only to specific applications or mechanisms.

User groups

There are major differences related to industry and corporate culture between companies in how remote work can be carried out, who can work remotely and what the requirements and conditions for remote work are. For some companies, the office is just one of several places where work takes place, while for others it is an essential part of work. The company's industry and corporate culture are major deciding factors in this. In the case of manufacturing companies, it is clear that the majority of work has to be carried out at the company's facilities due to the machinery involved, as a result of which such companies usually offer few opportunities for remote work.

Contracts with clients can also impose restrictions regarding the place of work. Similarly, the handling of confidential information/systems may require work to be carried out at the company's facilities. In most cases, client contracts also require the implementation of other physical and technical security solutions.

In response to the increase in remote work, some companies have divided employees into different user groups based on where and with what kind of IT solutions they carry out their work. For example, employees can be divided into those who work exclusively at office/manufacturing facilities, those who occasionally work remotely and those who predominantly work remotely. **Knowing which**

1) Examples include biometric identification (face, fingerprints, iris), authenticator applications, single-use ID, unique or safety keys, certificates, SMS or email

2) Role-based access control

employees can work remotely and under what conditions makes it possible to implement role-based access control (RBAC[2]), i.e. define which systems and information employees have access to based on their roles in different operating environments (if the operating environments differ from one another).

As regards identification and user groups, information security can be improved by:

- implementing strong identification at the company, and ensuring that strong identification is used with all the methods by which the company's protected information content can be accessed
- defining the boundary conditions for remote work and communicating them to employees
- defining the systems and information that employees have access to in different operating environments in a role-based manner.

Password management

The purpose of a password is to prevent the unauthorised use of a user account. It is important to use good and **sufficiently complex passwords** because **usernames are usually easy to guess** (being an email address formed from the person's name, for example).

Employees should be instructed never to save their passwords in any file saved on their workstation, with the exception of password managers. To increase security and make sure that employees do not set excessively simple passwords, it is recommended to set requirements for the length of and types of characters used in passwords. The general rule is that the longer the password, the better.

Very long passwords are, however, difficult to remember and run the risk of being forgotten. Furthermore, long passwords are more likely to be written down, which increases the risk of disclosure. One solution is to use passphrases instead of passwords, such as "MyfirstcarwasaVolkswagen", which can be shortened to something like "My1carwasaVolkswagen".

Every company must **establish a policy concerning passwords and the changing thereof**. Repeated failed login attempts must result in the user account being locked. The National Cyber Security Centre points out that in the case of services that you only use infrequently (once a year or less), you can request a new password to be sent to your email address every time you use the service.

A good password

- *At least 15 characters*
- *Includes both upper and lower case letters*
- *Includes special characters (%&//()=)*

National Cyber Security Centre

Password managers

The National Cyber Security Centre recommends using a password manager[3]. A password manager is an application that stores other passwords behind a single master password. **The master password must never be the same as a password used in some other service**. Security can be improved further by using two-factor authentication, which will protect the password manager even in the event that the master password is compromised. It should be noted, however, that cloud-based password managers have also been subject to some information security challenges.

Benefits of password managers

- *Passwords are safe behind a master password*
- *Generating and storing strong passwords is easy*
- *Protection against attacks targeting passwords*

As regards password management, information security can be improved by:

- defining a password policy for the company that covers, among other things, the length, complexity and changing of passwords
- instructing employees not to save their passwords in any files stored on their workstations
- instructing employees to secure their passwords with a password manager – the master password must never be the same as a password used in some other service.

3) Password managers available on the market include 1Password, Bitwarden, Dashlane, Enpass, F-Secure ID PROTECTION, KeePass, Keeper, LastPass and RoboForm

Software installation and updates

Many companies follow the **principle** of **not allowing employees to install their own software or update software on company computers**. It is good practice to automate the distribution of software to workstations, allowing the company's IT department to maintain awareness of what applications (and what versions thereof) are installed on workstations. All installations and updates should be carried out via a software portal (such as the Software Center on the MS Windows operating system). This practice makes company workstations less appealing for non-work-related use, which in turn decreases the risk of potential threats.

Regular automated software updates ensure that software (and thus information security) are kept up to date. A commonly used practice is to force software updates regardless of user action. When doing so, users are notified of upcoming updates in advance so that they can organise their work accordingly. Updates can also be programmed to take place outside of working hours (such as in the evenings or at weekends) so that they do not reduce the network capacity required for work.

Users are often offered the option of postponing updates by a few hours. This is to prevent forced software updates from taking place at inopportune times, such as in the middle of a client meeting. However, companies should ensure that **if updates are not carried out by a specified deadline, access to the company network or servers is blocked** until the updates are installed. Centralised software and update distribution ensures that software is kept up to date. The installation of updates should be monitored by the company's IT department, which can also address any problems that come up. Software updates should not be dependent on the employee having to access the workstation and the workstation being connected to the company's internal network. Nowadays most companies are able to manage software installations and updates remotely as well.

Hardware driver and firmware updates

Hardware driver and firmware (BIOS) updates have become increasingly critical as more and more vulnerabilities keep being discovered. As such, their updating should be ensured in remote work situations as well. While there are technical solutions available for handling driver and firmware updates, their management and reliability may cause risks, especially in remote access environments.

As regards mobile devices, companies utilise device management software to ensure compliance and the distribution of applications and updates. Device managers can also be used to block access to confidential material in the event of an emergency (the theft or misuse of a device).

Device management solutions must cover the company's obligation to protect any third party information in its possession and the company's interest in protecting its own information. Because of this, the company must be sufficiently aware of the technical implementation and the legislative requirements, especially when the devices being managed are also used for personal use or not owned by the company.

As regards the installation of software and updates, information security can be improved by:

- prohibiting employees from installing or updating their own software on company computers, unless the employee's work tasks or role require them to do so

- ensuring that software and updates are automatically distributed to workstations
- ensuring that if updates are not carried out by a specified deadline, access to the company network or servers is blocked until the updates are installed
- ensuring that hardware drivers and firmware are updated even when working remotely.

Content sharing and protection

Companies generate large amounts of information that needs to be shared and handled by multiple employees. In fact, the appropriate sharing and handling of information can be considered a prerequisite for effective cooperation and networking. There are various protocols for the sharing and handling of information with the help of which the party disclosing the information can present requirements for the handling and further sharing of the information to the recipient. These include the Traffic Light Protocol (TLP) and the Chatham House Rule, with the former concerning documents and information exchange more broadly and the latter having to do with information exchange at meetings and information events. During the COVID-19 pandemic, many meetings have been carried out under the Chatham House Rule, which means that the participants are allowed to freely utilise the information that they receive, but are not allowed to disclose the party disclosing the information, their organisation or the identities of the other participants. You can learn more about the Traffic Light Protocol and the Chatham House Rule ***here***.

Information is also the key asset of many companies. Because of this, **information, or content, protection is becoming an increasingly important issue for many organisations**. When dealing with massive amounts of information, protecting it all is simply not practical. Besides, companies also have a lot of business-related information that they want customers and cooperation partners to be able to access (such as information on the company's products, solutions and services). On the other hand, there are also types of information that every company wants to keep to themselves, such as prices and other trade secrets. The protection of personal data, meanwhile, is governed by the EU's General Data Protection Regulation (GDPR). More information on personal data protection is available here.

Finnish companies have received fines totalling hundreds of thousands of euros for violating the EU's General Data Protection Regulation, or GDPR.

Helsingin Sanomat 10 September 2021

"You need to protect not only systems, but content as well. Content protection is becoming increasingly important."

Microsoft

Classification of internal company information

Factors that every company should consider when it comes to information protection include information classification, ownership and life-cycle management. Companies typically have three to four different classifications for information – such as public, internal, confidential and secret – for the purpose of managing it. This management is facilitated by policies, based on which access to classified information is controlled. These policies also define ownership and responsibilities (including any administrator-level rights). Every company should incorporate information classification and protection into their information security training (see also the Information security and data protection training section).

Protecting information through classification is not complicated, yet relatively few companies engage in it. There are also commercial services available for the type of information classification de-

scribed above. Content protection can also be facilitated by restricting access to information based on time, i.e. granting access to information belonging to a specific classification level for a period of 30–40 days. The handling of classified information is described in greater detail in appendix 1 of this guide.

Technology is rarely the limiting factor when it comes to content protection, although it can be more difficult to manage in the contemporary multi-supplier ecosystem than in the past. In contrast, **mature information classification, ownership and especially life-cycle management are challenging**. Sustainable information protection requires the company's internal processes to support information ownership across organisational changes.

Information protection is affected by where and what kind of information is handled. The higher the classification level, the less the information should be handled remotely. Information at different classification levels can only be stored on specific devices. A good rule of thumb is to minimise the carrying of information and the use of centralised solutions. With remote work becoming increasingly prevalent and the use of Teams and similar services increasing, many companies have started to accumulate different types of materials on Teams, which must be taken into account in the company's information management structure and life-cycle model. When it comes to the handling and storage of business-critical information, classification must be mandatory. This kind of information must always be secret and shared internally through safe and approved mechanisms, such as secure email or file sharing services that require strong identification. This ensures that the information is not disclosed to external parties.

There are plenty of commercial solutions available for email encryption and reliable recipient identification, facilitating the flexible use of classified information.

It should be noted that data protection regulations impose obligations on data controllers that cannot be disregarded even with the consent of the data subject. The protection and confidentiality obligation requires sufficiently strong encryption[4] and the identification of relevant parties.

"Particular attention should be paid to the protection of confidential information during remote work, and tasks causing high or excessive risks should be completely excluded from remote work."

CSC – IT Center for Science

As regards content sharing and protection, information security can be improved by:

- ensuring that content is protected as well – it is not enough to only secure the system
- ensuring that the company processes and protects personal data in accordance with the GDPR
- preparing classification practices for the information shared and handled within the company
- ensuring that content is protected in accordance with the aforementioned practices
- providing employees with training on company practices and ensuring that employees comply with them
- ensuring that higher classification level materials are not handled remotely or preventing access to them by technical means.

4) *https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf*

FUNCTIONAL SOLUTIONS

Information security and data protection training

Nokia subsidiary suffers data breach – shocking truth revealed two months later

Tivi 24 August 2021

When it comes to information security and data protection, it is essential to understand what types of information are sensitive and how sensitive information should be protected. It is not enough to use traditional 'common sense.' **Information security and data protection practices must be documented, communicated and trained**. Personnel training is one of the cornerstones of every company's information security and data protection practices. Every company or organisation must have information security guidelines that employees can use to remind themselves of the issues covered in training.

Information security training should be organised regularly, preferably annually, and records should be kept of participation to ensure that employees incorporate what they learn into their everyday work practices. It is especially important to have the company's management commit to information secure practices, so that they can allocate resources for personnel training. Information security training should be mandatory. Even if training is only provided once a year, employees should be reminded of information security and associated risks (such as phishing) every now and then.

The training should also cover information classification so that employees are aware of what types of information are sensitive and which classification levels different types of information belong to (see the Content sharing and protection section). Information sharing between employees should be carried out using methods approved by the company and in accordance with the information classification scheme. The company should plainly communicate which types of information can be shared in each channel, such as Teams, Onedrive for Business and Workplace by Facebook. For example, Teams should not be used to share information of a higher classification level than confidential.

Company policy regarding social media and third party messaging applications

Especially during remote work, the boundary between personal life and work can become blurred, because of which company security guidelines should also cover the use of personal communication channels for work-related matters. Social media channels[5] and third party messaging applications[6] are not suitable for handling work matters, even if messaging applications can be considered more secure than mobile phones. Neither should social media channels be used to share work-related photos, as they can unintentionally contain internal company information or references to clients. Furthermore, photograph metadata can contain location information or reveal insight into other protected assets.

As regards information security and data protection training, information security can be improved by:

- organising mandatory information security training for employees on a regular basis
- training employees to understand what types of information are sensitive and how to protect sensitive information
- monitoring the completion rate of training and the internalisation of the provided information
- ensuring that the company has security guidelines and that employees know where to find them.

Online meeting tools

The information security of remote meetings can be improved with minor measures, such as preparation. Before the start of an online meeting, participants should ensure that they do not have any material open on their workstation that could significantly damage the company if disclosed to third parties. This will ensure that no one accidentally shares any internal company material on their screens during the meeting.

When it comes to sharing material during online meetings, employees should be instructed to only share the application window in question (Word, PowerPoint, Excel, etc.) instead of their whole screen. A good, safe and polite practice is to enable cameras when there are new or unfamiliar people participating in the online meeting. Once introductions have been made, cameras can be turned off to reduce the amount of bandwidth required for the meeting. When it comes to using cameras, many companies prefer using backgrounds that support their branding and – most importantly – make it more difficult to ascertain the person's physical location.

Taking into account potential threats, companies should also provide instructions on what can be discussed in online meetings. The participant must assess the risks and take the topic of conversation into consideration. Many companies have also prohibited the sharing of files via Teams, for example. From a technical standpoint, it is possible to ensure that the messages sent via the chat function are saved in a different location than attachments. File sharing should be carried out using the company's own server environment in accordance with the company's information classification policy.

The information security of online meetings can be further improved by requiring participants to log in instead of having them join via open links. This feature is available on Zoom, at least. Organisations wanting to use Zoom for internal communication or the sharing of confidential information

5) Such as Facebook, Snapchat, Instagram, Twitter and LinkedIn
6) Such as WhatsApp, Signal and Telegram

should use the Business or Enterprise version of Zoom (see the guide Ohjeita turvallisten etätyövälineiden valintaan (in Finnish)).

As regards online meeting tools, information security can be improved by instructing users to:

- close any unnecessary applications and files on their workstation before the meeting
- keep their camera on at the start of the meeting and introduce themself to the other participants
- only share the application window instead of the whole screen if they need to share something on their workstation during the meeting
- use a background image (one available on the online meeting tool or provided by your company)
- be aware of what they are allowed to discuss, what kind of files they are allowed to share and what they are allowed to save during the meeting.

Use and storage of devices (outside of company facilities)

At many companies, remote work is subject to the same basic principles as work carried out at company facilities. Remote work guidelines usually cover the handling and printing of information material, protecting material from being viewed or heard and the storing of devices. Employees should be instructed at the start of their employment relationship that workstations are intended for work-related use only. **In other words, work computers are not to be used for leisure activities and should never be used by other family members**. Here is a good rule of thumb: **do not do anything on your workstation that you are used to doing on your own laptop**. It is a good idea to point this out to employees during training. Although this is a relatively strict rule, companies rarely attempt to prevent small-scale personal use. Employers generally understand that employees may occasionally need to access online banking services or read personal emails, for example.

It is the responsibility of employees to ensure that the discussions that they have during work are not overheard and that outsiders cannot read sensitive information off their screens. In this context, outsiders refer not only to family members and guests, but also parties who have access to the employee's home (such as maintenance workers, property managers and landlords).

Good general methods for protecting against eavesdropping and unauthorised viewing include **using headphones** (prevents outsiders from hearing the other party's voice), avoiding talking near open windows and **using a privacy filter**. When discussing confidential matters, even family members should be prevented from hearing the conversation. With remote work becoming increasingly common, companies should equip all of their workstations with privacy filters. Some companies also utilise technical security solutions on their workstations.

Storing devices safely

When it comes to storing devices, guidelines vary depending on the type of material that they can be used to process. In general, it is important to **always lock the screen when you are momentarily away from the device**. Many companies use technical means to ensure that **the screen is**

automatically locked if the device is not used for five or ten minutes, for example. When a work device is not used, it should be turned off and moved out of sight. Storing devices in a locked cabinet is usually not required, as a device that is turned off and equipped with encrypted mass storage is considered sufficiently secure in terms of conventional risks. In general, devices should be stored in a place where they cannot be accessed by others. **However, as a rule, workstations or work phones should not be stored in a car, for example**.

Another area of activity relevant to information security is printing. In many organisations, the COVID-19 pandemic has reduced printing and contributed to the realisation of the so-called clean desk principle. The clean desk principle means that employees should not leave any documents, forms or other papers at their workstations or working area at the end of the day. Companies maintain that the principle should be followed at both the office and home. To ensure information secure printing, it is good practice to **identify the user before printing**, so that the document is only printed out after the user has confirmed their identity using an RFID and PIN combination, for example. Printers can also be stored in locked rooms that can only be accessed with employee keys. This will reduce the risk of inadvertently printed material ending up in the wrong hands.

As regards the use and storage of devices, information security can be improved by instructing:

- employees at the start of their employment relationship that workstations are intended for work-related use only
- employees not to let anyone else (even family members) use their workstations
- all employees to protect workstations from the eyes and ears of outsiders
- all employees to always lock their workstations when away from them
- all employees to shut down their workstations and move them out of sight when not used
- employees never to store their workstations or work phones in their cars
- employees not to print out work-related documents at home. If documents need to be printed out, they should be protected from viewing.

IoT devices

Nowadays more and more households have IoT (Internet of Things) devices in them that listen to users for the purpose of responding to voice commands. New technologies always require some getting used to and regular risk assessment.

Any listening smart home devices in the vicinity of the working area should be taken into account during remote work and, if necessary, switched off or have their listening modes disabled. **When discussing information at security classification levels I–III, there cannot be any listening devices in the same room**.

Homes may also have smart devices or camera technology that record video footage and upload it to an online cloud service to be processed or stored. Devices connected to the internet can also have features that allow a user to order them to start or stop recording remotely. Whether such devices are recording cannot be ascertained without powering off the device or physically obstructing it. As such, devices capable of recording should be handled as if they are always recording, meaning that to prevent electronic surveillance, confidential material should never be handled in their view.

IoT devices should be considered to be network access points that can be used to scan and examine network activity. As these types of devices proliferate, the importance of using a VPN tunnel and encrypted connections increases. Household IoT devices should be connected to a different network than workstations and work phones.

Companies should not only provide their personnel with training about the risks associated with IoT devices, but also secure their own network traffic in a reliable manner. Employees should not install or connect any external devices on or to their workstations without permission, as doing so can potentially compromise the confidentiality of information.

As regards IoT devices, information security can be improved by instructing employees to:

- change the default passwords of their devices during setup
- turn listening smart home devices off or disable their listening features for the duration of work
- regard listening and video recording smart home devices the same way as external or unfamiliar persons
- not install or connect any external devices on or to workstations without permission
- only connect devices approved by the company to the company network.

Travelling abroad

Travel – both foreign and domestic – is subject to the same guidelines as working in public spaces. As instructed previously in this guide, information should always be protected from unauthorised viewing and listening. When travelling abroad, the risks can be higher and partly different. Preparations for a trip abroad should be made in good time. For example, the Finnish Security and Intelligence Service advises travellers to update their devices and applications to the latest versions before a trip. Another good piece of advice is to activate device access codes and set the screen lock timeout to be as short as possible. More instructions are available ***here*** (in Finnish).

Companies' needs in regard to protecting laptops and other devices during travel abroad vary depending on the areas of activity of the company and the destination countries. Guidelines concerning domestic travel and travel to other Nordic countries are more general than those concerning so-called high-risk countries. The basic guidelines for all travel – both foreign and domestic – are similar to those

for public spaces: **public Wi-Fi networks** (such as airport and hotel networks) **should be avoided, work matters should not be discussed within earshot of others, workstations should be protected with screen filters** and **connections should be protected with a VPN**. Instead of Wi-Fi networks, workstations should be connected to the internet using a company phone's mobile connection.

When travelling abroad, users should remain vigilant and be aware of local conditions and risks. Some companies advise their employees not to trust hotel safes and security lockers, for example. Employees should be constantly aware of where their work equipment and devices (workstation and mobile phone) are during the trip. In other words, you should pay particular attention to keeping your assigned laptop with you at all times. Similarly, you should take care of your mobile phone in the same way as your credit card – never hand it over to another person.

People who work in such fields as politics, public service or in the business community may find that this makes them targets of intelligence operations.

Preparing for travelling to high-risk countries

Risk preparedness can be further increased when travelling to countries where information security or leakage risks are higher. Conducting a risk assessment before the trip is recommended, and in some cases deciding not to travel can be a valid choice. From the perspective of preparedness, **it is a good idea to consider different scenarios – situations in which risks increase**. If something seems too good to be true, it usually is. While industrial espionage and drugging may sound more like the plot of an action film than real life, such risks should not be underestimated. If you are travelling alone and are suddenly approached by an unfamiliar person who wants to have drinks with you, for example, you should be wary of their motives.

Think about the details that you share with strangers. Also keep in mind that excessive alcohol consumption can make you more susceptible to influencing attempts.

Finnish Security and Intelligence Service

During the trip itself, the focus should be on ensuring the security of laptops and devices and preventing their unauthorised use. The risk of company information ending up in the wrong hands can be reduced by taking along hardware (workstation and mobile phone) that only contain the minimum amount of information required. In other words, employees should not bring along the hardware that they use in their daily work. **According to the Finnish Security and Intelligence Service's instructions, you should avoid carrying smart devices, such as laptops, tablets, mobile phones or smartwatches**. When travelling to high-risk countries, you can also use security bags designed for this purpose. For these kinds of trips, it is also good practice to bring along devices nearing the end of their life-cycles, which can then be decommissioned after the trip. Alternatively, the device can be reinstalled afterwards based on a risk assessment. For data exchange, you can also bring along empty USB sticks that you do not bring back to Finland afterwards.

As regards foreign travel, information security can be improved by instructing employees to:

- identify risks and assess the appropriate level of preparedness
- avoid using public Wi-Fi networks when travelling
- consider what they can say to unfamiliar people and not accept any gifts
- avoid charging their phone or laptop with chargers offered by outsiders
- avoid connecting external USB devices to their workstation
- if necessary, bring along a device that can be decommissioned after the trip.

Appendix 1. Supplementary material

CLASSIFIED MATERIAL

Any material that needs to be handled should be classified and its ownership should be determined. This facilitates the appropriate handling and life-cycle management of classified information. Many companies have their own security classification practices and are also subject to requirements based on external frameworks and partnerships. Since these requirements vary, the applied practices should respond to different business needs in this regard as well.

Many companies provide services to authorities, and sometimes the service provision involves handling classified material. Provisions on the classification of government documents are laid down in **the Act on the Openness of Government Activities** (sections 16, 24 and 25), **the Act on Information Management in Public Administration** (section 18) and **the Government Decree on Security Classification of Documents in Central Government** (section 3). Classified material is divided into four security classification levels (I–IV) based on content; the smaller the number, the more critical the content.

All organisations should strive to ensure that information is always handled in a secure manner, regardless of classification. The disclosure of classified material between authorities and other parties is always subject to agreement, and there are detailed criteria in place for the secure handling of classified material. Material at security classification levels I–III can only be received, viewed and stored in security-audited company facilities. Access to classified information is only granted to specific persons based on needs (see the Identification and user profiles section, page 8). Information security must be ensured by technical means so that classified information above security classification level IV cannot be accessed remotely.

No company or organisation should allow anyone to print out or take with them information at security classification levels I–III. Printouts increase the risk of human error and classified material being disclosed to outsiders. For the same reason, **classified information must not be accessible remotely via personal terminal devices**: the possibility of a person sitting next to or behind you on public transport, for example, being able to view classified material must be excluded.

The increase in remote work due to the COVID-19 pandemic has led to some case-by-case flexibility regarding the requirements set by authority clients. This flexibility has only applied to information classified at security classification level IV, with remote handling being temporarily allowed provided that the circumstances are secure and the previous operating model is resumed immediately once the pandemic and the restrictions imposed by it ease.

The same instructions apply to spoken information as well. **Classified material must not be discussed in any environment where the discussion could be heard by outsiders**. For example, a telephone discussion taking place in a public space must be cut short if it involves classified information. The threat of espionage targeting mobile phones is real, and caution must be exercised in the use of other communication devices and platforms as well. As a general rule, classified material should only be handled using the tools designated by the client, which cannot include Teams or similar services. More detailed instructions for choosing secure means of communication are available **here** (in Finnish).

As regards classified material, information security can be improved by:

- ensuring that classified material is always handled in accordance with legislation and in ways defined in agreements
- ensuring that material at security classification levels I–III cannot be accessed remotely
- ensuring that employees cannot print out or take material at security classification levels I–III with them
- ensuring that classified material is not discussed anywhere within earshot of outsiders.

Phishing

University of Oulu subject to widespread phishing – passwords of more than 750 people fell into the wrong hands

Helsingin Sanomat 3 September 2021

Phishing has increased dramatically in recent years. Common phishing methods include scam phone calls and messages (email or SMS) aimed at getting the recipient to disclose information to a third party.

Companies provide information about phishing via multiple channels and follow the National Cyber Security Centre's bulletins about phishing campaigns, for example. Educating employees about phishing is considered very important. This education can be provided via information security training, targeted email messages or campaigns (warning of scams or rising trends) for the entire personnel, blog posts (e.g. illustrative cases of phishing), other communication and tips posted on the company intranet, for example.

In addition to this education, personnel should be regularly reminded that **the company IT department will never ask for passwords or online banking codes**. On a related note, in most Finnish organisations IT personnel are not English-speakers and **will only contact employees in response to a service request submitted by the employee**.

One method that has proven effective in educating employees is the utilisation of gamified services. Many companies have reported using a phishing simulation service[7], which involves sending simulated phishing emails to employees and seeing how many of them recognise the message to be a phishing attempt. These simulated messages contain phishing indicators, such as an incorrect email address, typos, etc. When an employee reports the message as a phishing attempt, they score points or can be instructed to complete a training session going over key points regarding phishing messages. Completing the training awards points as well, with employees able to compete with each other for high scores. The service provider can help the company monitor what kind of messages their employees most commonly fall for, which serves as useful information for adapting training content. Following such a campaign, the results should be openly shared with employees.

Transparent operating culture and rapid response are key

Companies should promote a transparent and rewarding operating culture instead of one where employees are judged for making mistakes. This way the threshold for reporting issues remains low. Employees should be provided with positive feedback for their vigilance, even when the reported message turns out not to be a phishing attempt. In accordance with an encouraging operating culture, employees can also be rewarded for identifying phishing messages or security risks.

7) Such as Hoxhunt

Phones are typically infected with malware via unprotected Wi-Fi networks, unofficial app stores, email attachments and malicious websites.

F-Secure

The faster information security issues or incidents are identified, the easier it is to address them and minimise their impacts. Employees should be able to openly report on anything that happens. The reporting of information security risks should be made as easy as possible from a technical standpoint. This can include adding a phishing button to MS Outlook using a Report message or Report phishing addon, for example. The function can be implemented by persons with global admin rights, and Microsoft also utilises it for email filtering. Google's Gmail service automatically scans the identifying information and content of messages moved to the spam folder to help improve its email filter. Phishing monitoring can also be carried out with the help of artificial intelligence and automated processes by having the company's data traffic monitored around the clock by a security operations centre. In the event of any suspicious data traffic, the system will issue an alert, and any exposed user accounts can be suspended.

If the damage has already been done, it is crucial to determine the extent of the damage (whether a data breach has occurred). If the data breach concerns personal data and may cause a risk to the rights and freedoms of natural persons, it must be reported to the Office of the Data Protection Ombudsman – more detailed instructions are available **here**. Account passwords can be reset even based on a suspicion. If a data breach has already occurred, the affected computers must be immediately taken offline and then investigated and diagnosed by the information security department, which also carries out the necessary measures. After this, the computers can be reinstalled and put back into service. What is most important is to have a clear process in place for this that everyone is aware of.

In addition to phishing, users are threatened by various types of malware. Malware targeting mobile devices is especially common, usually causing unwanted device behaviour (such as showing advertisements or spying on the user). If you suspect that your mobile device has been infected with malware, contact your company's IT experts and have the device serviced.

As regards phishing, information security can be improved by:

- covering phishing in information security training
- ensuring that the company has a process in place for handling data breaches
- warning personnel separately of ongoing phishing campaigns
- reminding employees that the company IT department will never ask for their passwords of online banking codes
- promoting transparency – the lower the threshold for reporting potential data breaches, the faster the issue can be fixed and the damage contained
- responding rapidly – if personal data is at risk, the data breach must be reported to the Office of the Data Protection Ombudsman.

Supporting coping and supervisory work as part of information security

Secure remote work is not just a matter of technical solutions and appropriate employee conduct. Information security is also affected by employee strain and exhaustion. Tired employees are more prone to making mistakes and not considering risks.

Employee coping can be supported by improving remote working conditions. For example, the employer can grant financial assistance for the procurement of more ergonomic furniture (such as an office chair), or equipment previously used at the office (such as an external display) can be brought home. An area that should be given particular attention is employee coping, as the increase in remote work has also increased the risk of physical and psychosocial stress and accidents. Employees should be encouraged to take breaks and maintain their energy levels. For example, companies can agree to end Teams or other online meetings five minutes to the hour so that employees have a moment to rest before the next meeting. It also remains important to agree on the length of the working day, as the boundary between working and leisure time has become increasingly blurred during the COVID-19 pandemic.

On the one hand, remote work has increased the flexibility of work. On the other hand, it has also challenged existing routines and schedules. Recognising strain and exhaustion has become more challenging as employees no longer interact with the work community in the same way as before. Needs related to pressure and stress management have also increased. This puts an even greater emphasis on the role and competence of supervisors. With this in mind, supervisors can be provided with training in maintaining workplace well-being and team spirit and promoting good ergonomics. The Finnish Institute for Health and Welfare has prepared guidelines for supporting remote work. You can read them **here**.

In general, at least the following factors should be taken into account in regard to coping:

- Prolonged remote work may diminish the traditional benefits of remote work.
- Companies should develop remote work methods that take into account the needs of individual employees and the community (which tasks can be handled remotely and which require presence at the office/client facilities).
- It is important to communicate to employees what kind of methods they should employ to maintain working ability, what kind of help and support is available, what occupational health care offers and how the employer contributes to improving the ergonomics of work spaces, for example.
- Groups of employees can take turns working remotely and at the office so that there are fewer employees present at the office at once, making it easier to keep a safe distance.
- Ensure that supervisors contact their subordinates regularly.
- If you use virtual modes of communication or arrange virtual meetings, make sure that new employees know the related practices and how to use them.

Finnish Institute for Health and Welfare (THL)

As regards coping and supervisory work, information security can be improved by:

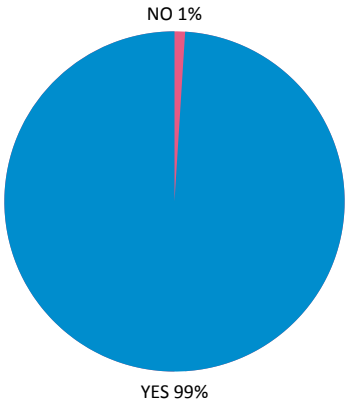
- taking care of employee coping during remote work as well[8]
- encouraging employees to take breaks and maintain their energy levels
- not scheduling several remote meetings back to back without breaks
- supporting supervisors by developing competence related to workplace well-being and maintaining team spirit.

8) By arranging walking meetings, for example

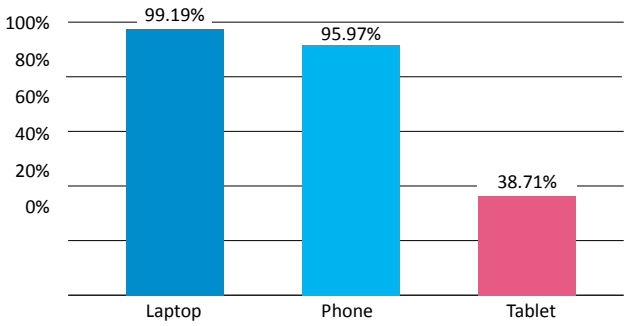
Appendix 2.

SUMMARY OF THE QUESTIONNAIRE RESULTS

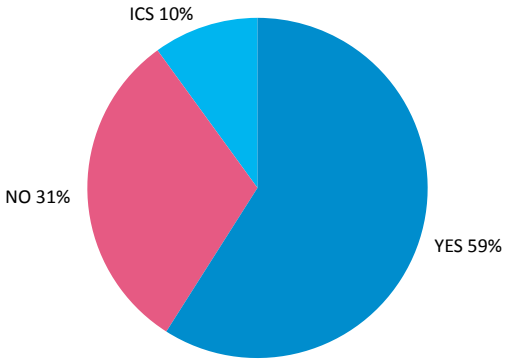
Does your company offer the option of working remotely? (n = 125)



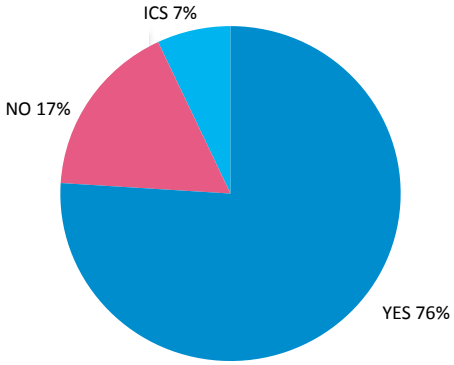
Does your company offer the option of working remotely using equipment provided by the company? (n = 124)



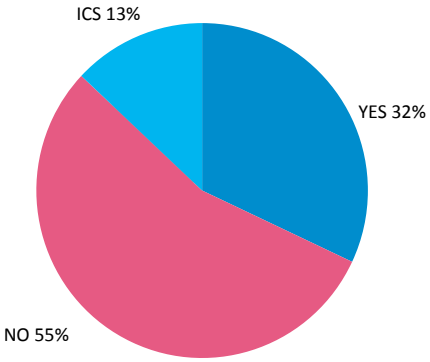
Company laptop: Does your company offer the option of using company services via a virtualisation solution? (n = 123)



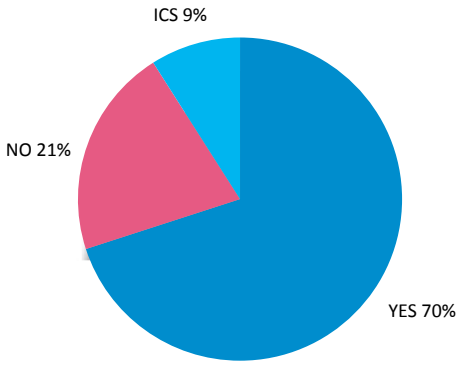
Company laptop: Does your company offer the option of using company services via web applications? (n = 123)



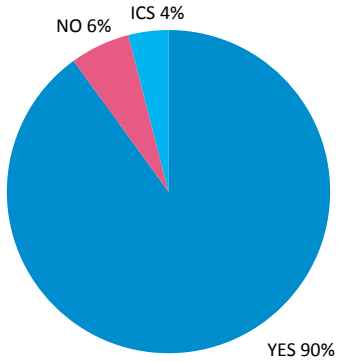
Company phone: Does your company offer the option of using company services via a virtualisation solution? (n = 119)



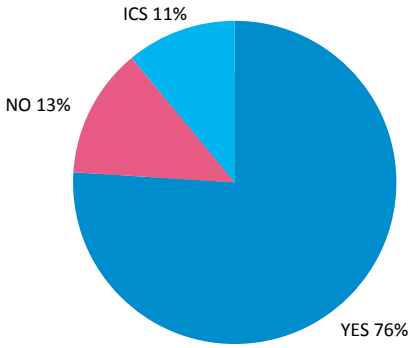
Company phone: Does your company offer the option of using company services via web applications? (n = 119)



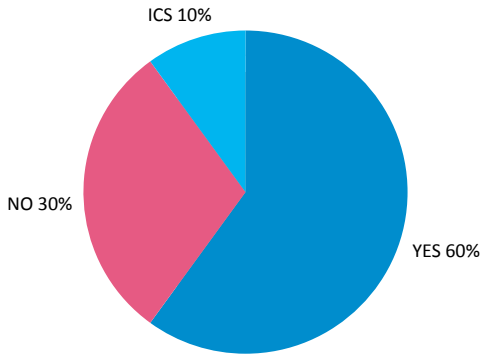
Does your company use a device management solution for laptops? (N = 114)



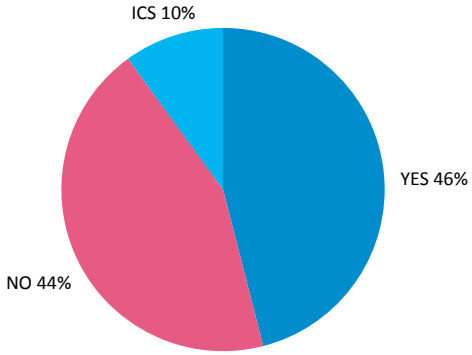
Does your company use a device management solution for phones? (n = 74)



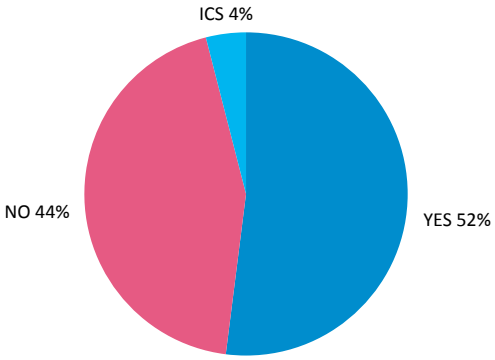
Does your company limit the use of software and services during remote work based on the operating environment? (n = 124)



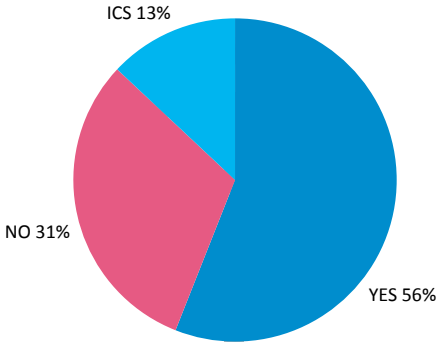
Are work tasks during remote work limited by technical means or with instructions based on the operating environment? (n = 124)



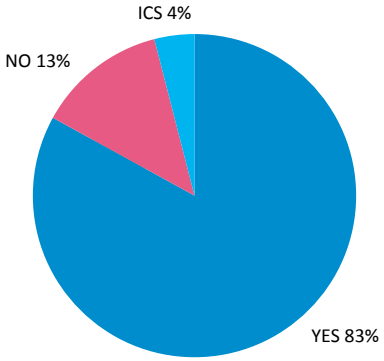
Has your company defined requirements for the working environment during remote work (space, equipment, environment)? (N = 124)



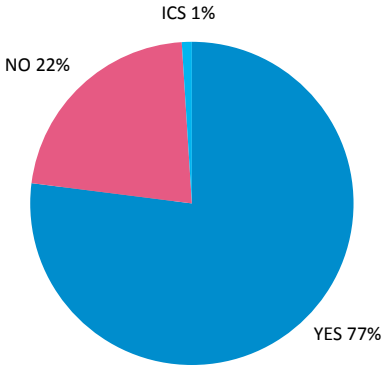
Has your company defined remote access requirements in accordance with security classification levels? (n = 79)



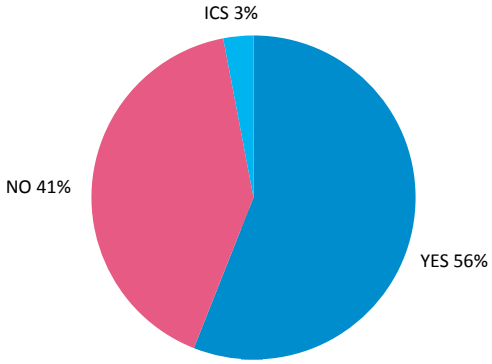
Does your company have a policy for secure password management? (n = 124)



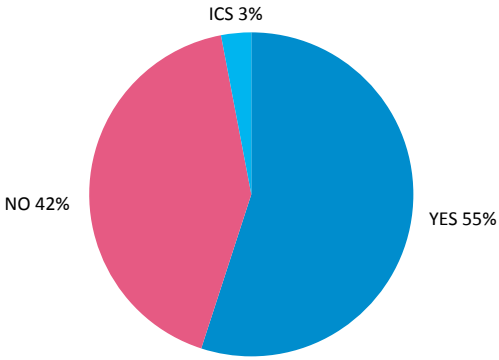
Does your company require strong identification to access services? (n = 124)



Has your company defined how work equipment should be stored during remote work? (N = 124)



Has your company defined guidelines for travel? (N = 124)



Appendix 2.

INTERVIEW QUESTIONS

Background information

1. When were your company's remote work guidelines drafted?
2. Has it been necessary to update the guidelines since? If so, for what reason?

Risk analyses

3. Did your company carry out risk analyses on the remote work guidelines before they were implemented?
4. Were the guidelines drafted internally or was their drafting outsourced to a third party? Were external operators or other experts consulted during the drafting of the guidelines?

Remote work guidelines currently in place

5. Which of the technical solutions currently used at your company have proven most effective? (possible themes: home user, travel user, admin user)
6. Which have proven the easiest to implement?
7. Has your company provided instructions on how to secure personal Wi-Fi networks (SSID, changing the default password, MAC filtering, changing default portal login info)?
8. Has your company provided instructions on or a solution for secure password management (KeePass, etc.)?
9. What do your company's guidelines say about the handling of paper material during remote work?
10. What do your company's guidelines say about the storage of work equipment at home?
11. What do your company's guidelines say about safe remote work during travel? Are the guidelines different for domestic and foreign travel?
12. What do your company's guidelines say about external persons when working from home (family members, neighbours, guests)?
13. What do your company's guidelines say about software updates, can updates be installed when working from home? How is the installation of updates monitored?
14. How has the COVID-19 pandemic affected your company's remote work guidelines?

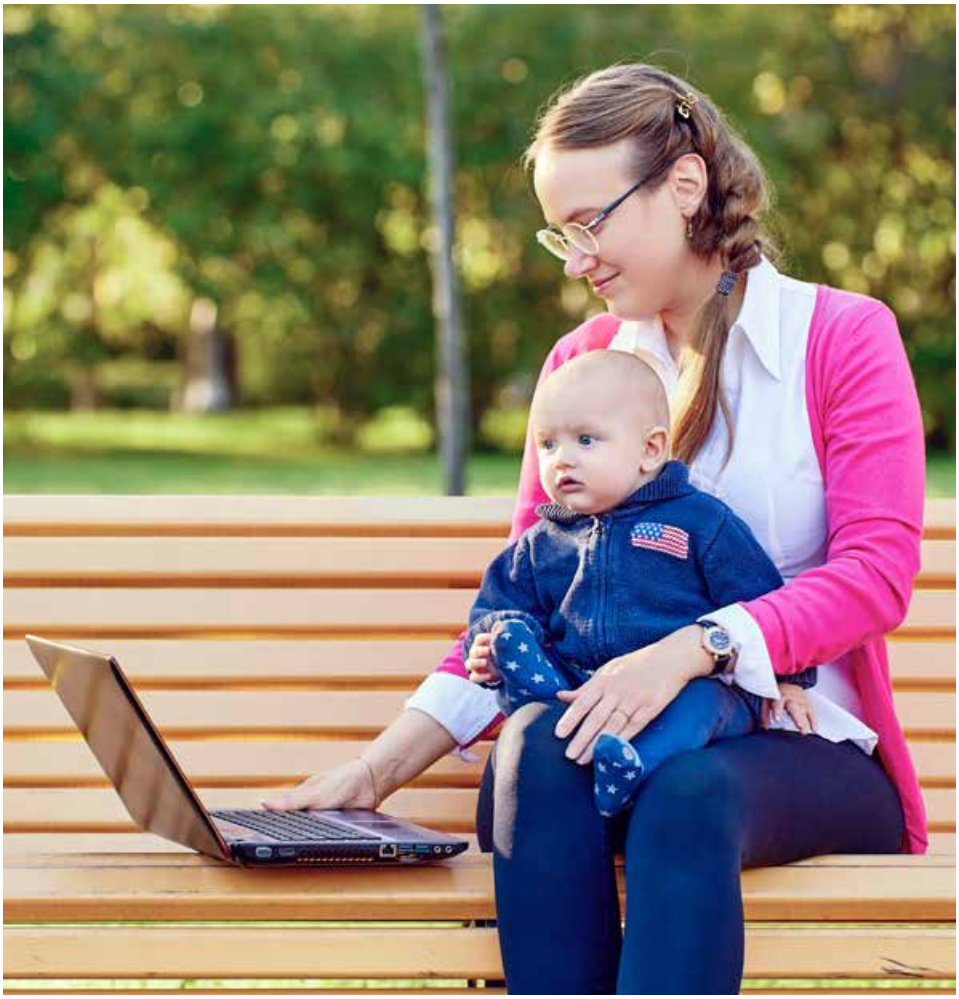
Identified problems / things to improve

15. What kind of challenges has your company specifically tried to address with remote work guidelines?
16. 16. Has your company defined separate processes for addressing problems that come up during remote work or do you follow the same processes as at the office?

17. Based on the questionnaire, employees have had problems establishing connections and with the reliability of VPN tunnels. How has the reliability of connections been taken into account at your company?
18. How has your company prepared for phishing attempts?
19. How does your company monitor connections (e.g. accounts cracked by phishing)?
20. What kind of instructions would you like to receive regarding securing connections?

Teams

21. Does your company provide instructions / would you like to receive instructions on the secure use of Teams (what kind of information can be shared, what kind of information can be discussed)?
22. Does your company provide instructions for participating in Teams meetings outside of the home?



HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI