Working from home

Recommendations for workstation design

www.bitkom.org

bitkom

Published by

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Contact

Marc Danneberg | Bitkom e. V.
T 030 27576-526 | m.danneberg@bitkom.org

Responsible Bitkom committee

Expert Committee Vendor-Neutral Tendering

Project management

Marc Danneberg | Bitkom e. V.

Title image

© green-chameleon – unsplash.com

Content

List of tables

Acknowledgements

This publication is based on the results of the work of the VBG's prevention field office. This guide is the result of intensive cooperation between experts from public administration and representatives of Bitkom member companies. It owes its existence to the extensive work of the »Product-neutral tendering for home offices« project group. We would like to express our particular gratitude to:

- Andreas Frisch, DIN-Normenausschuss Bauwesen (NABau)
- Dr. Heiner Genzken, Intel Deutschland GmbH
- Stefan Gniza, VBG – Ihre gesetzliche Unfallversicherung
- Jürgen Graf, Fujitsu Technology Solutions GmbH
- Goran Hauser, Intel Deutschland GmbH
- Dr. Niklas Hellemann, SoSafe GmbH
- Dr. Heidi Koithan, Lexmark Deutschland GmbH
- Jürgen Meß, VBG – Ihre gesetzliche Unfallversicherung
- Florestan Peters, SoSafe GmbH
- Stephan Peters, Qualcomm CDMA Technologies GmbH
- Jens Polster, Konica Minolta Business Solutions Deutschland GmbH
- Christian Richter, VBG – Ihre gesetzliche Unfallversicherung
- Jörg Roskowetz, AMD Advanced Micro Devices GmbH
- Wolfgang Schestak, Fujitsu Client Computing Limited
- Daniel Schiwek, HP Deutschland GmbH
- Axel Simon, Hewlett-Packard GmbH
- Marco Sönksen, Berlin Police
- Andreas Stephan, VBG – Ihre gesetzliche Unfallversicherung
- Klaus-Peter Wegge, Siemens AG

1 Introduction

Decentralised and hybrid forms of work becoming ever more important. The Coronavirus crisis fundamentally changed the way many employees organise their work within a very short period of time, and flexible workplace models will become part of the new normal in the world of work even after the pandemic is over. This guide supports employers and employees in designing home office workstations. It focuses on ergonomic, technical and organisational requirements.

The aim of the document is to illustrate different workstation situations in the home environment and to support the choice of work equipment with information and explanations on workstation design. It also addresses issues of IT security and accessibility of home office workstations.

Reference is also made at this point to other Bitkom guides relating to product-neutral tenders for ↗ **laptops**, desktops-PCs, ↗ **thin clients**, ↗ **printers and multifunctional devices**, and ↗ **monitors**, among other things. These guidelines provide public contracting authorities with a reliable and comprehensible aid so that they can formulate their invitations to tender in a product-neutral manner, i.e. without using protected brand names or naming specific manufacturers and taking into account current technical requirements. In this home office guide, the different product groups are briefly described in terms of their use in the home environment. If more in-depth information on the technical criteria of the individual product groups can be found in the guides for product-neutral tenders, this is noted accordingly.

2 Differentiation between teleworking and mobile working

A distinction must be made between teleworking and mobile working with respect to the requirements for a workstation in the home environment.

Usually, employees who telework alternate between working at a computer workstation located at the company's premises and at a teleworkstation within their own private sphere. This can also be arranged in such a way that the employees work largely from their home office and only occasionally visit the company premises. A teleworking workstation is a permanently installed computer workstation in the employee's private environment, which is subject to the regulations of the Workplace Ordinance and which the employer is responsible for setting up. The prerequisite for this is a provision in the employment contract or an agreement between the employer and the employee. A teleworking workstation is ideally designed and set up similarly to an on-site VDU workstation.

With mobile working, a VDU activity is performed at a location outside the workstation, for example in a restaurant, on the train or in a hotel, and can occasionally also take place in the employee's own home. In principle, mobile work is subject to the regulations of the Occupational Health and Safety Act and the Working Hours Act, but the Workplace Ordinance (ArbStättV) does not have to be taken into account when equipping the workstation.

According to the SARS-CoV-2 Occupational Health and Safety Rule, a home office is a special form of mobile working that enables employees to work temporarily in their homes after prior consultation with the employer.[1]

For the purposes of this guide, the term »home office« covers both mobile working from home and permanently established teleworkstations. The following recommendations apply to mobile working (functional equipment) and teleworking (optimal equipment) in a home office. Under certain conditions, workstations with functional equipment can also be used as teleworkstations (see Chapter 3.1.1).

---

1 The SARS-CoV-2 Occupational Health and Safety Regulation specifies the requirements for occupational health and safety with regard to SARS-CoV-2 for the period of the epidemic situation on a national level as determined in accordance with Article 5 of the Infection Protection Act. The SARS-CoV-2 Occupational Health and Safety Regulation is determined or adapted by the advisory occupational health and safety committees at the Federal Ministry of Labour and Social Affairs (BMAS) together with the Federal Institute for Occupational Safety and Health (BAuA) and published by the BMAS in the Joint Ministerial Gazette. Further information on the legal bases can be found in the annex to this publication. [↗ **https://www.baua.de/DE/Angebote/Rechtstexte-und-Technische-Regeln/Regelwerk/AR-CoV-2/pdf/AR-CoV-2.pdf?__blob=publicationFile&v=66**] For more detailed information on the legal basis of telework and mobile working, see the annex to this guide.

3 Requirements for VDU workstations in the home environment

Functional and ergonomic requirements must be taken into account when equipping and designing workstations at home. The frequency with which a home office is used and the specific work content are also important in this regard: As a rule, communication can already be maintained with the provision of a mobile terminal. This may be sufficient to enable occasional (even sometimes daily) work from an employee's home office, but regular work from home places more far-reaching demands on the equipment and design of the home office workstation.

The following explanations and recommendations refer to work situations in which work is done regularly and for full working days from a home office. A distinction is made between functional and optimal equipment or workstation design.[2]

	Functional	Optimal	Remarks / explanations
Time spent working from home	up to 50 percent of working hours	more than 50 per cent of working hours	The percentages suggested here are only to be understood as rough guidelines. In addition, the specific content of the work is a decisive factor when it comes to equipping the workstation. When deciding whether the functional or the optimal category should be used as a guideline for workstation design, various criteria and requirements for the workstation must therefore be taken into account.
Main activities	E-mail and text processing, preparation of reports and presentations, participation in video conferences and online workshops, etc.	E-mail, text and image processing, preparing reports, presentations and comprehensive evaluations, participating in and leading video conferences and online workshops, regular contact with customers and partners (e.g. support, consulting, press relations), frequent printing and scanning (e.g. drafting contracts), frequent use of specialised procedures and software (e.g. ERP systems, dashboards, graphics programmes) etc.	The main areas of activity outlined here should be understood as examples of use. The tasks and their requirements for equipping a home office vary from case to case.
Teleworking	Suitable for teleworking within the meaning of the Workplace Ordinance under certain conditions.	Fully suitable for telework within the meaning of the Workplace Ordinance.	

Table 1: Categories of home office workstations

2 Agreements can be made between employer and employee stipulating that the Workplace Ordinance (ArbStättV) is in principle to be taken into account, even in the case of occasional work assignments from the home environment. In this case, the recommendations for teleworkstations (optimum equipment) apply irrespective of the amount of time spent working from home.

3.1 Functional equipment

Home office workstations in the functional category are fundamentally suitable as mobile workstations for working at home for several days (e-mail and text processing, preparing reports and presentations, participating in video conferences and online workshops, etc.). Under certain conditions (use of only one monitor, reduced paperwork, presence of an office swivel chair, free movement area of at least 1.5 m² at the workstation, etc.), this equipment also constitutes a suitable workstation for teleworking within the meaning of the Workplace Ordinance.

3.2 Optimal equipment

The optimal category describes an equipped VDU workstation that can be used without restrictions for (alternating) telework. The recommendations for equipment and workstation design are thus suitable for work situations in which activities are carried out very frequently or exclusively in the home environment.

4 Choice of work equipment

Working from a home office can provide new freedom to be flexible and creative and to reconcile work, family and leisure time. However, what needs to be considered is that a home office environment has special requirements that need to be taken into account when choosing work equipment, in order to, among other things, exclude health problems and minimise IT security risks. A home office workstation can be characterised by the following aspects, depending on the employee's living situation:

- Professional and private use of the workstation and work equipment
- Limited space (work equipment is regularly set up and dismantled / stowed away)
- Ambient noise
- No support and assistance functions directly on site

The following section describes which functionalities and equipment features should be considered when choosing work equipment for use in a home office – though the actual working and living situation is always the deciding factor.

Reference should also be made at this point to other Bitkom guides for product-neutral tenders for ↗ laptops, ↗ desktop PCs, ↗ thin clients, ↗ printers and multifunctional devices and ↗ monitors. These guides describe the different technologies and application potentials in detail. The guides also contain recommendations on the minimum technical requirements and evaluation criteria that can be taken into account as part of the purchasing decision.

4.1 Terminals

The decision as to which terminal or which combination of terminals should be used in a home office depends to a large extent on the degree of mobility (how often is the terminal moved? Is the device used at different workstations?). The organisation of work thus plays a decisive role in the choice of work equipme.

BYOD concepts are not a solution for continuous home office use, if only because of IT security requirements and the responsibility of employers towards their employees.[3]

4.1.1 Smartphone and tablet

Even with a smartphone or tablet, electronic communication can fundamentally be maintained while travelling and while working from home. Writing longer texts, answering e-mails in detail or dealing with complex work tasks quickly becomes tedious on these devices, making a laptop

3 see also Glossary

or desktop PC irreplaceable when it comes to equipping a home office workstation. Smartphones and tablets can be used in the home office as supporting devices (for taking notes, as additional cameras or screens, for using app-based productivity tools, etc.).

4.1.2 Laptop, 2-in-1 device (convertible) and desktop PC / monitors

The laptop or desktop PC are the central work tools when working from a home office. Since the keyboard and touchpad are firmly integrated into laptops, the ideal distance from the screen cannot be maintained when working for longer periods of time. Therefore, the use of a separate mouse, keyboard and external monitor is recommended (for the optimal as well as the functional equipping of a home office workstation). The recommended distance between the eyes and the screen is 50 to 80 centimetres. An external monitor also provides the optimal viewing height, where the top edge should not be above eye level.

The laptop screen is often used as a second monitor. A laptop stand can be used to adjust the height to the coupled, external monitor. If a raised laptop is used not just as a second monitor but also for data input, then external input devices (keyboard, mouse) are particularly important for ergonomic reasons.

In a home office, a docking station or port replicator can also be used. External monitors and input devices as well as other accessories (e.g. headphones, headset, web camera, etc.) do not have to be connected to the laptop every time. A docking station can be manufacturer-dependent, in which case it only fits the manufacturer's intended laptops. Meanwhile, many docking stations are equipped with a USB Type-C port, allowing them to be used universally. A port replicator is connected as a separate device to a free USB port. A single USB cable transmits the signal from several ports

4.1.3 Thin client

Since home office terminals are often located in unsecured networks, the risk of being exposed to cyberattacks increases. Thin clients offer a good solution here, because their operating concept (read-only operating system and no local storage of user or application data) can offer improved protection against unauthorised data access compared to classic PCs.

Regardless of the type of mobile thin client, i.e. a thin client with the characteristics of a laptop, or a stationary thin client: an appropriate corporate infrastructure is required for operation, which is mandatory for thin client access. More details can be found in the ↗ Bitkom guide for the product-neutral tendering of thin clients.

4.2 Technical accessories

Working in a home environment can pose special requirements in terms of the functionality and ergonomics of technical equipment. For example, in a home office, the equipment might be moved and stored quite frequently, especially if the workstation has been integrated into a living area or is used alternately by different members of the household. In addition, depending on the living situation, ambient noise can impair concentrated work more than in an office environment. These particularities must be expressly taken into account when deciding on technical accessories.

4.2.1 Input devices

As already described under 4.1.2 for laptops, the use of a separate mouse and keyboard is generally recommended. These are connected either with a connection cable or wirelessly with the terminal device or a docking station or a port replicator (receiver at the USB connection or Bluetooth). Due to limited space and mobility requirements, it may be advisable to aim for as few cables as possible. With keyboards in particular, however, it should be taken into account that wireless interfaces can pose an increased security risk if third parties manage to send unauthorised commands to the client via them. This should be taken into account when planning the equipment and in the IT security concept (see also chapter 7 on IT security).

4.2.2 Headphones

Headphones can be connected to the smartphone or computer (wired or cordless) and used for telephone calls and video conferences when travelling or at home. A distinction can be made between open and closed systems: Open headphones allow sound waves to pass through in both directions, i.e. ambient noise remains audible and the user does not feel completely cut off from the outside world. Conversely, people sitting nearby (in the home office, office, train, etc.) may feel disturbed by the sound that is escaping from them and into the surrounding space. Closed headphones allow hardly any noise to penetrate outwards and muffle ambient noise.

Regardless of the design principle, classic headphones are divided into on-ear and over-ear systems, which has an impact on wearing comfort, although this must always be assessed individually. The cushions of on-ear headphones are shaped to sit directly and relatively snugly on the ear, while over-ear headphones wrap completely around the outer ear. As a rule, over-ear systems are larger and therefore somewhat more difficult to transport.

In order to reduce ambient noise more than just mechanically, noise-cancelling headphones are equipped with active noise cancellation. For this purpose, microphones localise the ambient sound and emit a corresponding negative signal (counter-sound). When the two sound impulses meet, the external sound is attenuated. Active noise cancellation differs from transparency mode, which is where external sounds are picked up more effectively and passed on to the ears. Important signals and announcements can be heard very clearly.

If employees frequently take on active tasks in video conferences, online seminars or customer meetings, it is worth considering equipping them with a headset that comes with microphone for voice recording. This can often improve recording quality considerably.

4.3 Printers and multifunctional devices

As a rule, a printer or a multifunctional device that can process print media up to DIN A4 is used in the home office. As far as functional equipment is concerned, we recommend the use of a printer, so that it is still possible to carry out necessary scanning and copying processes at the workstation in a timely manner. However, if the employee spends far more than half of his or her weekly working time working from home, it is advisable to provide a multifunctional device. Whether a multifunctional device is used in individual cases depends on the activity of the respective employee. If a printer or multifunctional device is used in the home office, data security must be guaranteed. It may therefore be necessary to use a document shredder and a lockable cabinet. In general, the IT baseline protection module »SYS.4.1 Printers, copiers and multifunctional systems« should be observed when handling printers, multifunctional devices and documents in the home office and the necessary protective measures should be taken.

Furthermore, in the case of printers and multifunctional devices, it should be borne in mind that processes for ordering or procuring consumables (e.g. toner or ink, imaging unit, paper) must be established. It should also be considered whether the printer or multifunctional device is to be integrated into solutions for overall output management.[4] This has a major influence on the selection of a system. Many providers offer customer portals that allow employees to manage their device themselves and, for example, order consumables.

The printer or multifunctional device for a home office should be WLAN-capable in order to provide employees with a flexible installation location. The BSI module NET.2.2 WLAN use must be observed here.

4.4 LAN and WLAN infrastructure for secure working

The way we work has changed dramatically in the last decade. Teams are now spread out and, especially with the pandemic, are no longer necessarily at their desks in the office. The ability for employees to connect from home or outside of their previous workstation, to collaborate with other team members and to access the tools and data needed to do their job is critical for any organisation. Ensuring this connectivity and collaboration in a secure and compliant manner is a key concern, given that many businesses and public sector organisations need to support an increasingly decentralised and distributed workforce.

4 see also Glossary

KEY CONSIDERATIONS

Secure remote connectivity – Speed, simplicity and security are paramount to supporting an ever-growing remote workforce, i.e. an increasing number of employees working from home. Security and compliance considerations must provide maximum protection and risk mitigation without compromising service level and availability expectations. As network access in these cases is usually via private or public internet access, access cannot be controlled at the network level. However, to ensure a high level of security even remotely (analogous to the employer's on-site networks), it is necessary to encrypt the connection and link the network access, i.e. the individual authorisations, to the user's role. In concrete terms, this means that network access control and segmentation must at least be based on the user's role and the connection location.

With a growing, decentralised workforce, providing connectivity can be a challenge. To deal with ever-changing external factors as well as business forces, a large number of users need to be brought online without impacting the network infrastructure or operations. Features such as automatic provisioning provide easy setup, configuration and management of the network, without on-site IT support, for simplifying the onboarding of new remote users. VPN connectivity can be extended to users using VPN clients or remote access points, which then establish a VPN connection to a physical gateway or virtual gateway.

A seamless user experience – Remote users need access to all the applications, data and resources they have become accustomed to or need for their work. This means that their remote experience should be identical to their experience when they are physically in the office. Remote access points (RAPs) are ideal for this purpose when used at a teleworkstation or home office. VPN clients offer an almost similar function on the terminal and thus also enable use wherever there is unprotected internet access.

In summary, this means that further specific solutions are used in the provision of secure and high-performance internet access (remote access points, VPN client, controllers and gateways, policy manager, policy enforcement firewall). More detailed information and explanations on these technologies can be found in the glossary.

5 Recommendations for equipping workstations in the home environment

Recommendations for workstation design in the home office are outlined below. A distinction is made between functional and optimal equipment (refer to Chapter 3 »Requirements for VDU workstations in the home environment«).

5.1 Workstation

Equipment[5]	Functional	Optimal	Remarks / explanations
Desk work surface	120 x 80 cm	160 x 80 cm	
	Not height adjustable Height 740 ± 20 mm	Height adjustable	Starting from the adjusted chair (see below), adjust the height of the table so that when the lower arms rest on the tabletop they form a right angle with the upper arms. If the height of the work table cannot be adjusted: Sitting position for upper body as above, then check if leg position fits as with chair, if necessary, with a footrest or higher table.
Legroom width	At least 85 cm	At least 85 cm 120 cm recommended	
Legroom depth	At least 80 cm	At least 80 cm	
Work chair	Conference or office swivel chair	Office swivel chair with appropriate castors	Seat height should be adjusted as much as possible – feet flat on the floor, upper and lower legs forming an angle of slightly more than 90°. If the feet are not on the floor, a footrest can help.
Free moving space at the mobile workstation	120 x 80 cm	160 x 100 cm	The movement area is important – different postures should be able to be adopted at the workstation, movement should be possible while sitting (dynamic sitting) and it should also be possible to switch between sitting and standing. Tripping hazards must be eliminated.

Tabelle 2: Functional and optimal equipment of workstations

5 Agreements can be made between employer and employee stipulating that the Workplace Ordinance (ArbStättV) is in principle to be taken into account, even in the case of occasional work assignments from the home environment. In this case, the recommendations for teleworkstations (optimum equipment) apply irrespective of the amount of time spent working from home.

5.2 Technical equipment

With regard to the minimum and evaluation criteria that can be taken into account in the procurement of **↗ laptops**, **↗ desktop PCs**, **↗ thin clients**, **↗ multifunctional devices** and **↗ monitors**, you can refer here to the Bitkom guidelines for product-neutral tenders.[6] In the case of technical equipment: As a general rule, no distinction between functional and optimal equipment is necessary. Where additional features can be considered for optimal equipment (e.g. possibility to connect a second, external monitor), this is shown below. This concerns the areas of laptops as well as printers and multifunctional devices.

Equipment	Functional	Optimal	Remarks / explanations
Laptops			
Display resolution	1.366 x 768 Pixel (HD)	1.920 x 1.080 pixels (Full HD and higher)	Higher values are available on the market. As a general rule, screen sizes are reduced with higher resolutions. Adjustments to the font and symbol sizes may be possible in the operating system.
Screen diagonal	from 12.5"	13" – 17"	Size, shape and weight must be appropriate to the work task. If only one laptop is used, at least 15" is recommended. If at least one external monitor is also used, then the laptop display can also be smaller.
Antireflection coating	Low reflection (non-glare)	Low reflection (non-glare)	
Processor type (CPU)	Multi-core	Multi-core	
Working memory (RAM)	At least 8GB	At least 8GB	
Mass storage	At least 128GB SSD	At least 200GB	
Ethernet	RJ45 Ethernet 10/100/1000 Mbit, can be achieved with adapter	RJ45 Ethernet 10/100/1000 Mbit, can be achieved with adapter	Small and flat laptops in particular often do not have an RJ-45 interface due to their design; corresponding adapters are available on the market.
WLAN	WLAN according to IEEE 802.11ac (Wi-Fi 5) (dual band 2.4 and 5 GHz)	WLAN according to IEEE 802.11ax (Wi-Fi 6) (dual band 2.4 and 5 GHz)	
Bluetooth	BT 5.0	BT 5.0	
WWAN	4G LTE (integrated), data transmission rate ≥100 Mbit/s for download and ≥ 50 Mbit/s for upload	4G LTE (integrated), data transmission rate ≥100 Mbit/s for download and ≥ 50 Mbit/s for upload	Higher data transmission rates (e.g. 5G) are available on the market.

6 ↗ Guidelines | ITK-Beschaffung

Equipment	Functional	Optimal	Remarks / explanations
USB	2 × USB 3.x (of which min. 1 x type A or adapter solution to provide type A)	2 × USB 3.x (of which min. 1 x type A or adapter solution to provide type A)	If one of the USB type C ports is also used to charge the laptop, it is occupied during the charging process and cannot be used to connect other peripherals. Adapters to increase the number of USB ports are available on the market.
Display output	1 digital connecti-on for screens	1 digital connection for screens	The exact type should be specified (e.g. HDMI, Mini HDMI, USB-C, DisplayPort, Mini DisplayPort).
Audio	Audio in and audio out	Audio in and audio out	Input and output are provided by a combination interface on many devices.
Keyboard	German / English etc. keyboard layout	German / English keyboard layout, keyboard with backlight	Portable visual display units without separation between the screen and the external input device (especially units without a keyboard) may only be deplo-yed at workstations where the units are only used for a short period of time or where the work tasks cannot be performed using any other visual display units. Portable display screen devices with alternative input means must be operated appropriately for the work tasks and with the aim of providing optimum relief for employees.
Front camera	Resolution HD 720p HD	Resolution HD 720p and Hybrid Infrared (IR)	
Speaker	Stereo	Stereo (front-facing)	
Microphone	Mono	Mono	
Touchpad	Two-button function	Two-button function	
Operating system	e.g. Windows, ChromeOS, MacOS, Linux	e.g. Windows, ChromeOS, MacOS, Linux	
Graphics unit	Integrated into CPU	Integriert in CPU DirectX 12-fähig Support von zwei externen Displays	
Printers and multifunctional devices	Printer	Multifunctional device	Whether a printer or multifunctional device must be able to print only in black and white or also in colour depends on the type of activity and the frequency and variety of use. For further details on the individual requirements and other criteria, please refer to the guide »Tendering for multifunctional devices in a product-neutral manner«.
Max. format	DIN A4	DIN A4	
Working memory	256 MB	256 MB	
Paper output capacity (guide values)	100 sheets	125 sheets	
Scanning		600 x 600 dpi s/w	

Equipment	Functional	Optimal	Remarks / explanations
Authenticity of documents	PTS certificate	PTS certificate	
USB for client	Min. USB 2.0	Min. USB 2.0	
Network connection	RJ 45 Ethernet 10/100	RJ 45 Ethernet 10/100	
Wireless connection	WLAN infrastructure (according to IEEE 802.11x)	WLAN infrastructure (according to IEEE 802.11x)	
Print speed	Min. 20 ipm at DIN A4 according to ISO/IEC 24734	Min. 20 ipm at DIN A4 according to ISO/IEC 24734	
Certifications	GS mark Blue Angel	GS mark Blue Angel	

Table 3: Criteria for technical equipment

5.3 External hardware for audiovisual communication

An essential factor for communication in a home office is optimal audio and video quality, which can be supported by the use of external equipment.

Equipment	Functional	Optimal	Remarks / explanations
External headset			
Connection	Wired	Bluetooth	
Wearing comfort	Simple wearing comfort	Individual wearing comfort	Individual preferences: Stereo / mono, head mount (in-ear, over-ear, headband, neckband)
Volume control and muting	Via software	Via hardware switch on headset	
Microphone positioning	Flexible holder	Additional protection from breath and spit	
Sound quality	300-15000 hZ	Additional attachable noise cancellation	
External microphone			
Sound quality	300-15000 hZ	Additional attachable noise cancellation Stereo	
Directionality	Omnidirectional	Cardioid	
Connection	Wired	Bluetooth	
Sensitivity and muting	Via software	Via hardware switch on headset	

Equipment	Functional	Optimal	Remarks / explanations
Microphone positioning	Flexible holder	Additional protection from breath and spit	Decoupling from structure-borne sound, e.g. from the PC
External hands-free kit			
Connection	Wired	Bluetooth	
Volume sensitivity and muting	Via software	Via hardware switch on the unit	Touch operation is not barrier-free
Audio quality	Maximum echo decoupling	Additional elimination of noise for the incoming audio signal	
Microphone sensitivity	Single directional microphone	Microphone array with automatic speech direction detection (for multiple participants)	

Table 4: Criteria regarding external hardware for audio-visual communication

6 ITechnical support for working from a home office

When technical problems occur in a home office, it is particularly important that a support process has been defined beforehand and that the employees are aware of it (e.g. formalisation in a user manual or a support process map). Access to technical support should be as low-threshold and transparent as possible. For this purpose, ticket systems are recommended where support processes can be initiated via different channels (web access, mail, hotline). In addition, the organisation should regulate how a device can be replaced at short notice in the event of damage (e.g. collection / pickup).

A supplier's service portfolio does not need to be limited to the delivery of hardware and software, but can also include other services related to the delivery item, which can also be accessed from a home office.

Support / Helpdesk:

For instance, it would be conceivable to maintain and keep the delivered hardware and any software supplied up to date on the basis of a separate service contract or via a warranty extension. In this context, it must be clarified whether the equipment can be sent by post in the event of damage. Additional services such as troubleshooting or hotline services for general technical questions can also be agreed.

If necessary, the corresponding support should be agreed together with the specification of response times / repair times.

Standard market offers differ according to:

- Duration of the contract
- Response times (time between fault report and first response from support)
- Restoration time (time between fault report and restoration of the system to operational readiness)
- Spare parts logistics
- Additional technical services offered

Terminal management:

The commissioning of new devices usually involves expenditure that should not be underestimated. A device management system can help here. It must be clarified whether the device management is to be operated by the company's IT department or by an external service provider.

7 IT security

IT security in the home office depends on two factors in particular: The technology used in the home office environment and the people working in the home office environment. This is also true for work done in the office environment, but in a home office it is much more difficult for many organisations to ensure that employees behave according to the rules that have been set out. The shift to mobile working models thus places greater responsibility on employees. A rough overview of some potential cyber attack tactics as well as typical vulnerabilities in IT security infrastructures that are particularly common with mobile working:

- **Inadequately protected endpoints:** Many organisations do not actively manage endpoints in the home office because direct access to the devices is hampered by the remote work setting. In these cases, organisations often fail to regularly install updates or to comprehensively check anti-virus software. This lack of mobile device management (MDM) and patch management leads to security gaps that cybercriminals exploit for targeted attacks.

- **IT infrastructure:** If employees increasingly transfer work-related data from home or public networks via the protected infrastructure of companies, specific challenges can arise. Private access points are often less well secured and sometimes transmit data without encryption. Direct attacks on inadequately secured routers and WLAN networks are a very easy way for hackers to access sensitive data.

- **Organisational risks:** The majority of cyber attacks on organisations use employees as a gateway. Examples include phishing campaigns, which are designed to manipulate recipients and induce them to take dangerous actions. While employees can exchange information about possible attacks on their employer's premises and protect themselves in this way, they are often left to their own devices when working from home – which means that the attacks are less likely to be detected and, in turn, are more likely to be successful.

- **New tools and credential theft:** In home offices, digital collaboration tools are becoming more and more important. Chat messages, telephone calls and video conferences replace on-site meetings and enable continuous communication, even across teams. It is precisely these tools, which are being increasingly used in mobile working, that cybercriminals are focusing on when carrying out credential theft attacks, which aim to steal login data. Once the attackers have gained access to the systems, they not only have access to sensitive data; they also often aim to manipulate other employees. Using a stolen identity, they will send messages under a false name and can prompt people who think the attackers are colleagues to commit harmful act.

To combat this risk, organisations should implement concrete measures related to the afore-mentioned »technology« and »people« factors. In the area of technology, the aim should be to secure the transmission, processing and storage of data and information in a similar way to how this entire process is carried out in the context of the office and the protected corporate infrastructure (cf. chapters 7.1 and 7.2).

In addition, employers should also provide their employees with clear guidelines and rules regarding the protection of data and devices. The changeover to mobile working models should thus be accompanied by appropriate education and training measures, through which employees learn how they can minimise the risks described. Detailed recommendations for strengthening cyber security awareness as well as further measures can be found in the chapter »IT security in the home office and mobile work« of the Bitkom guide ↗ **»Mobile and hybrid work. Working in and after the Coronavirus pandemic«**.

7.1 Terminal security

Mobile devices can become the target of cyber attacks, data theft and data misuse. The devices are exposed to an increased risk potential especially if they are not only used in the home environment but also in mobile environments. Such attacks endanger the confidentiality, availability and integrity of the data processed and stored with the devices as well as the functionality of the devices themselves. Modern terminals can be equipped ex works with integrated security functions that can support compliance with security requirements. Data protection and data security can ultimately only be established through a combination of organisational measures, due diligence on the part of the device user and security functions inherent in the device.

No.	Criterion	Requirements	Comments / Explanations
1	**Mechanical anti-theft protection**	▪ Device to accommodate a mechanical anti-theft device ▪ Anchored in the inner laptop frame	Suitable locks etc. must be procured separately as accessories. May have an influence on the design / thickness / dimensions of the unit. For additional locking options, see docking functionality.
2	**Out-of-band management**	If available, delivered deactivated in the firmware; can only be activated with firmware password	Remote maintenance functions that can change the firmware and / or data independently of the operating system must be delivered deactivated, if they are available. Activation of the functions must be protected and must only be possible with a firmware password. When deactivated, the functions must neither establish nor accept network connections.
3	**BIOS / UEFI / coreboot tamper protection**	Detection of and protection against tampering, reliable notification of the owner or user.	The systems must have mechanisms that prevent manipulation of the firmware (e.g. by write protection) or detect manipulations (e.g. by signature verification) and reliably notify the owner or user if this occurs.
4	**Encryption**	Hardware-based drive encryption	Integrated hardware and firmware provide automated encryption of data (e.g. OPAL). No operating system support or separate software installation is required.
5	**Interface protection**	Interfaces in BIOS / UEFI / coreboot can be disabled	e.g. Ethernet, USB, WLAN, WWAN, Bluetooth, camera, microphone, fingerprint sensor, etc.
6	**User authentication**	Multifactor-authentication options	e.g. smart card, fingerprint, other biometric features, etc.
7	**Webcam cover**	Integrated or retrofitted physical webcam cover	
8	**Privacy filters**	Privacy filter (integrated or as an accessory)	Solution depends on system manufacturer.

Table 5: Security criteria and requirements

7.2 Infrastructure security (security and privacy)

The following security functionalities and configuration options should be evaluated depending on the specific configuration of the home office workstation's network connection.

VPN

For secure connection via the Internet, the devices should support VPN encryption technology. The highly secure IPSec VPN technology (according to the current IKEv2 standard), which is widely used by many end devices and remote stations, enables the convenient and flexible connection of external network users or entire locations and service providers.

Anti Spam, Anti Virus

In addition to security awareness measures, anti-spam and anti-virus applications support e-mail security. This protects the infrastructure used in the long term as well as ensuring short-term operability. Modern solutions are based on a two-step approach: first, they check potentially dangerous files locally (e.g. on a firewall) and then, in a second step, via sandboxing in the cloud. Sandboxing involves preventively isolating a suspicious file in a sealed-off environment in order to assess possible attacks. Among other things, machine learning ensures that the individual security mechanisms are up-to-date.[7]

Zero-trust security, anti-malware, intrusion detection / prevention, artificial intelligence

New attack vectors are emerging, particularly due to the diversity of terminals and the increasing number of devices used in the Internet of Things. This is particularly critical because these types of terminals can be compromised in various ways as soon as they are integrated into a network infrastructure and authorised in a security-compliant manner. For example, they can be used to exploit existing access privileges to read out data and transmit it to attackers or to cause damage or disruption. These more complex cyber attacks can be detected through behavioural analysis of terminals by analysing deviations from previous behaviour. Known attacks can be detected and thwarted with an intrusion detection and prevention system that tracks typical attack patterns. However, the key is to be able to detect, contain and prevent previously unknown attacks. These types of systems are based on artificial intelligence and help to detect and prevent such new attacks when behaviour changes, for instance when data is transmitted to previously non-existent targets or when the data transmission pattern changes. These mechanisms should be combined with a role-based network access control platform to exclude compromised devices from network access or at least quarantine them.

Role-based network access requires a policy manager to apply role-based access control and enforcement to all detected and profiled devices. This is done by setting up real-time policies that determine how users and devices are connected and what they can access. Traditional firewalls

7 ↗ Guidelines | ITK-Beschaffung

that use IP-based VLANs for control and only become active after a user or device is added to the network provide an opportunity for advanced attacks. However, a user and application firewall covers this vulnerability instead by using identity, traffic attributes and other security contexts to centrally control access rights at the time of initial connection. Filling this gap is important because every second an attacker is connected to the network, essentially thousands of malware packets can be released.

Wireless intrusion detection system

A network infrastructure can also be exposed to hardware-based attacks. This applies in particular to WLAN networks, as wireless signals can easily spread over greater distances and, in contrast to wired networks, there is no clear demarcation between the network and the outside world – which is why sources of interference can influence the radio network. Sources of interference can simply be other devices such as microwaves, which create interference on the same wireless frequencies as WLAN when they are in operation. However, they can also be attackers who deliberately paralyse a WLAN network or imitate a WLAN network in order to tap into the data of the terminals.

When selecting a WLAN solution, it therefore makes sense to ensure that it can detect, localise and ideally avoid such sources of interference. The functions for detecting malicious attackers fall into the area of wireless intrusion detection and prevention. As well as detecting sources of interference, the access points can thus recognise typical patterns of attacks that can be used to disrupt wireless communication. Spectrum monitoring and intelligent channel selection can also help to detect and avoid general interference to ensure trouble-free operation.

In addition to the implementation of these essential security functions in the network, security aspects should also be taken into account when choosing a manufacturer. The following things should be implemented by the manufacturer:

GDPR

The General Data Protection Regulation comes into effect in networks when services to be provided by the network process personal data (e.g. MAC addresses, IP addresses, login information, information about service use, e-mail addresses, etc.). This is the case, for example, with content filters or network access control and network management via cloud systems. Therefore, only solutions whose manufacturers enable GDPR-compliant use may be deployed.

Common Criteria / BSI certification

The Common Criteria or BSI certification ensures that the network components meet the tested security standard and thus contribute to the secure infrastructure in a comprehensible manner. The Common Criteria certification should be available for as many components as possible and should be up-to-date.[8]

8 For more detailed information on the subject of Common Criteria and further links, please refer to the glossary.

Processes for detecting and fixing security vulnerabilities

No software is error-free, which makes it even more important for every manufacturer to implement organisational processes that check the respective solution for vulnerabilities before release and then fix them. If vulnerabilities are found by third parties after release, they can be reported to the manufacturer. The manufacturer must make a Critical or Security Incident Response Team (CIRT or SIRT) available for this purpose. The IRT must process these vulnerabilities and fix them according to its own specifications.

Support organisation

The manufacturer should have its own service and support organisation. This is the only way to ensure that products are replaced in the event of hardware faults or that software updates are made available. Both of these are important for the longest possible, fully functional use of network products.

The manufacturer should offer different service levels that ensure short response times when needed.[9]

9 For more in-depth information on infrastructure security, see also Bitkom guide ↗ **»Tendering hardware in a product-neutral way for the school sector. Guidelines for Public IT Procurement«**.

8 Accessibility

Procurement of accessible hardware and software is required if a company employs people with disabilities (this applies equally to public and private employers). General accessibility requirements are laid down in law in Article 4 of the Disability Equality Act (BGG, see: https://www.gesetze-im-internet.de/bgg/BJNR146800002.html). In addition, there are other relevant standards and regulations such as Part 1 of the Barrier-Free Information Technology Ordinance BITV 2.0 (↗ **https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html**). For the legal basis and for further information on accessibility, see Annex B in this guide.

Procurement should refer to these or equivalent requirements (refer to Annex B.2). The provider submits a self-declaration laying out which accessibility requirement are met by the offered product and which cannot be met. DIN EN 301549:2020-02 Accessibility requirements for ICT products and services is to be used for this purpose. This is directly referenced in Article 3 (1) and (2) of the Information Technology Accessibility Ordinance BITV 2.0 (↗ **https://www.gesetze-im-internet.de/bitv_2_0/BJNR184300011.html**) to the German Disability Equality Act (BGG). As laid down in Article 31 (2) 1 of the Ordinance on the Award of Public Contracts (VgV), reference can be made to DIN EN 301549 in the technical specifications, in order to appropriately take the user needs of persons with disabilities into account. Templates for the self-declaration are provided in Table C.4 (page 56) of Technical Report CEN/CLC/ETSI TR 101 552 (2014-03, https://www.etsi.org/deliver/etsi_tr/101500_101599/101552/01.00.00_60/tr_101552v010000p.pdf). Equivalent standards such as the US ICT accessibility standard US Section 508 should also be accepted (refer also to Annex B.6: International self-declaration).

Further information on the accessibility of ICT products can be found in the Bitkom guides relating to product-neutral tenders for ↗ **laptops** und ↗ **thin clients**.

9 Procurement models

There are basically two different ways of procuring the requirements for a home office. Either the requirements are covered as part of the procurement of the respective components (e.g. mobile terminals, office furniture) or the supplies and services for the home office are handled via a separate procurement process. Both approaches have advantages and disadvantages.

	Procurement of the requirements via the normal procurement cycles	Procurement of the entire home office requirement in a separate transaction
Advantages	Lower-priced contracts can be concluded by combining the procurement processes. The variety of manufacturers and the associated administrative effort can be reduced. Under certain circumstances, more services can be offered to employees working from home.	More precise attention can be paid to the needs of employees working from home. More uniform equipment for home offices Processes can be aligned more precisely to home offices. Bidders can implement these processes more precisely.
Disadvantages	Ordering and service processes for home offices must be considered in the service descriptions. In some cases, requirements cannot be covered in such a targeted manner.	Higher processing and administration costs, as additional contracts have to be concluded. Procurement may be somewhat expensive compared to the other procurement process.

Table 6: Procurement models

Hardware can be procured by renting, buying or leasing it. In contrast to renting, leasing usually entitles the procurer to a purchase option for the leased item at the end of the contractual useful life. The approach selected by the procurer depends not least on whether it has a one-off budget or a budget covering several years.

Generally, one of the above-mentioned procurement models must be chosen in advance of the procurement measure in the context of an economic feasibility study. At the same time, it must also be decided whether the hardware and operating system are to be procured from one source on a uniform contractual basis (bundling) or from different suppliers. Software manufacturers sometimes offer special licensing models for software intended for use in public administration.

Another point to consider is how consumables can be ordered in a home office, especially for printers and multifunctional devices, and how other services (e.g. repairs) can be provided. The contract model under which these services are purchased also plays a major role here. Please refer to the corresponding product guides for this. These guides describe the possible contract models that are common for the respective products in the service area and which services they include. Corresponding processes need to be derived from these. In addition, procedures for how employees in the home office can order the office materials they need and where they are to be delivered must be defined. As the organisational requirements are quite different at this point, individual processes have to be developed here for each user.

Annex A: Legal basis of telework and mobile working

Definition of teleworkstation according to the Workplace Ordinance (ArbStättV)

Article 2 (7)

Teleworkstations are VDU workstations permanently set up by the employer in the private sphere of the employees, for which the employer has specified both a weekly working time, which has been agreed upon with employees, and the duration for which the workstation is to be set up.

A teleworkstation is only established by the employer when the employer and the employee have laid down the conditions of teleworking in an employment contract or in the context of an agreement, and the furniture and work equipment including communication equipment that the teleworkstation requires has been provided and installed by the employer or a person commissioned by the employer in the private area of the employee.

Scope of application of the Workplace Ordinance regarding teleworkstations

Article 1 (3)

For teleworkstations only:

1. Article 3 during the initial assessment of the working conditions and the workstation,

2. Article 6 and Annex No. 6,

insofar as the workstation differs from that in the establishment. The provisions referred to in sentence 1 shall apply insofar as requirements are applicable to teleworkstations, taking into account their specific nature.

Excerpt from the explanatory memorandum of the Bundesrat printed matter 506/ 16 of 23 September 2016. Paragraph 3 defines the scope of application for teleworkstations.

The lack of specifications and standards for setting up and operating teleworkstations has increasingly led to conflicts between employers and employees in practice in recent years. Today, both groups are faced with the question of which specific requirements apply to teleworkstations and how these workstations outside the company are to be designed to protect employees. Clarification with regard to workstations in the private sector is all the more urgent as this type and form of work organisation and work design will become even more important in the future as part of the reconciliation of family and work. [...]

Teleworkstations are mostly workstations of employees who alternate between working on site and in their private sphere (teleworkstations). […]

»Mobile working« (occasional working from home or while travelling, checking emails after work outside the company, working at home without a set-up VDU workstation, etc.) is not subject to the Workplace Ordinance; it is not telework in the sense of the Ordinance. Rather, mobile working is a working model that enables employees to work outside of regular working hours at home or on the road in addition to working in the office (permanent access to the company / business via means of communication). […]

Excerpt from the »SARS-CoV-2 Occupational Health and Safety Regulation« (version 07/05/2021)

2.2 Working from home as a form of mobile work

(1) Mobile work is a form of work which is not carried out at a workstation in accordance with Article 2 (1) of the Workplace Ordinance (ArbStättV) or at a fixed teleworkstation in accordance with Article 2 (7) of the ArbStättV in the private sphere of the employee, but in which the employees work at any other location (for example at the customer's premises, in means of transport, in a home).

(2) Electronic or non-electronic work equipment is used to perform mobile work.

(3) Working from home is a form of mobile working. It enables employees, after prior agreement with the employer, to work temporarily for the employer in their private sphere, for example using portable IT systems (e.g. laptops) or data carriers.

(4) Regulations on telework remain unaffected.

Annex B: Information on accessibility

B.1 Definition of accessibility

»Information processing systems are [...] defined as accessible [...] if people with disabilities

- can find, access and use them
- without it being exceptionally difficulty for them and
- without them requiring any third-party

assistance in general.

The use of special tools for disabilities is allowed« (BGG Article 4)Tools are devices such as special keyboards, alternative pointing devices, screen readers and screen magnifiers.

B.2 Relevant standards and regulation

When creating the performance specification for the procurement of notebooks, accessibility criteria must be considered, except for justified exceptions:

- Act to Modernise Procurement Law (Vergaberechtsmodernisierungs-Gesetz, VergRModG) (18/4/2016) (implementation of Directive 2014/24/EU and Directive 2014/25/EU) Article 121 Description of services, paragraph 2
- Equality for Persons with Disabilities Act (Behindertengleichstellungsgesetz, BGG), (10/7/2018) Article 12 Accessible information technology, paragraph 2.

Care should be exercised here to ensure that the requirements are aligned with user needs and are both technology-neutral and open to innovation.

In order to harmonise accessibility requirements in the procurement of information and communication technology products and services by public entities in Europe, the European Commission tasked the European Standards Organisations CEN, CENELEC and ETSI with the creation of a standard. The result of this assignment is European Standard EN 301549:2018-08 (↗ **https://www.etsi.org/deliver/etsi_en/301500_301599/301549/02.01.02_60/en_301549v020102p.pdf**), listed in the Official Journal of the European Union under Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies. This European standard was implemented with DIN EN 301 549:2020-02 Accessibility requirements for ICT products and services. Verification should be provided by means of a contractor self-declaration. Currently, there is no relevant certification option available, which is why certificates cannot be demanded as verification.

B.3 Standards on accessibility features

A comprehensive overview of accessibility features that must also be fulfilled by desktop PCs, laptops, tablets and smartphones is provided by ISO/IEC 20071-5 »Information technology – User interface component accessibility – Part 5: Accessible user interface for accessibility settings on information devices«. This standard is available as a draft and is expected to be published in 2021. The annex to the standard can serve as a checklist when drafting the offer. The accessibility features are listed in Chapter 4.2 of the standard.

B.4 Management system standards for accessibility

DIN EN 17161 »Design for All – Accessibility of products, goods and services in accordance with a »Design for All« approach – Extending the range of users« is a management system standard that helps organisations ensure accessibility in its processes. It is not mandatory to apply this standard, but doing so is helpful with regards to the self-declaration.

B.5 Outlook

An updated version of the standard is already available as EN 301 549 (2021-03,-, ↗ **https://www.etsi.org/deliver/etsi_en/301500_301599/301549/03.02.01_60/en_301549v030201p.pdf**) Its publication in the Official Journal of the EU, as well as its implementation as DIN EN 301549, is expected in 2021.

Article 2 »Scope« (1), »Products« and other provisions of EU Directive 2019/882/EU on accessibility requirements for products and services (European Accessibility Act, EAA) (↗ **https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019L0882&from=EN**) fdemand the accessibility of the following products if they are placed on the market after 28 June 2025:

»a) Hardware systems and operating systems intended for these hardware systems for all-purpose computers for consumers« [...]

c) Consumer terminals with interactive capabilities used for electronic communications services;

d) Consumer terminals with interactive capabilities used to access audiovisual media services; [...]«

In addition, the following services are also covered in Article 2 (2):

»a) Electronic communications services other than transmission services for the provision of machine-to-machine communications services;

b) Services providing access to audiovisual media services; [...]

f) Electronic commerce services [...]«

The EAA envisages accessibility to be part of the self-declaration as part of the CE marking process. The EAA is essentially implemented one-to-one in Germany through the Accessibility Enhancement Act (Barrierefreiheitsstärkungsgesetz, BFSG), which is expected to be passed before the end of summer 2021. For the additional accessibility requirements in the EAA, an extension of EN 301 549 is planned as a standardisation mandate.

B.6 International self-declaration

The following information might be helpful for internationally active ICT providers in creating their self-declaration: »The Information Technology Industry Council« (ITI) provides a free reporting tool – the Voluntary Product Accessibility Template (VPAT) – to help determine whether ICT products and services meet accessibility requirements, including the rules following US Rehabilitation Act Section 508. The ITI has published updated versions of the VPAT (2.4) that are based on the updated 508 rules of the US Access Board (VPAT 2.4 508). Additionally, versions for WCAG 2.1 (VPAT 2.4 WCAG) and EN 301 549 (VPAT 2.4 EU) are offered, as well as an additional version based on all three (VPAT 2.4 INT).
↗ https://www.itic.org/policy/accessibility/vpat

Annex C: Glossary

BYOD-Konzept	Concept for integrating private mobile devices such as laptops, tablets or smartphones into the networks of companies or schools, universities, libraries and other institutions (»bring your own device«).
Common Criteria	When selecting information technology components such as network and security solutions, attention should be paid to security certification. International certification according to »Common Criteria« (CC), which is also carried out by the Federal Office for Information Security (BSI), ensures the greatest possible variety of solutions with simultaneous application security. The BSI also recognises certificates already issued by other countries that are based on common protection profiles (cPP). The »Common Criteria Recognition Arrangement« agreement (CCRA) regulates mutual international recognition with the aim of avoiding multiple certifications. It is therefore important to ensure that the components used have CC certification from the BSI or equivalent from a certification body in accordance with the CCRA agreement. More information: BSI website: ↗ **https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/InternatAnerkennung/CCRA_Anerkennung.html** Search facility for CC certificates from different manufacturers: ↗ **https://www.niap-ccevs.org/** Common Criteria Portal: ↗ **https://www.commoncriteriaportal.org/**
Controllers and gateways	Controllers and gateways provide connectivity and security features, including VPN termination for remote workers for optimised Layer 3 roaming, scalability and redundancy for campus networks of any size. Ideally, controllers will have a firewall to enforce access rules, AI-based RF optimisation and automatic provisioning from the secure on-site infrastructure to remote elements such as remote access points or VPN clients.
Intrusion detection and prevention system	An intrusion detection or intrusion prevention system (IDS / IPS) is a security solution that monitors a network or a network component such as a server or a switch and seeks to detect rule violations and harmful incidents such as hacker attacks, and then to ward them off to some extent automatically.
Network Management System (NMS)	NMS is a general term for the software and / or hardware that performs network management. This includes all functions and components needed to monitor and control networks.
Policy enforcement firewall	A policy enforcement firewall is the underlying technology that enables automatic provisioning to simplify and secure wired and wireless networks. This feature extends to remote users and provides administrators with critical visibility, control and security enforcement capabilities.
Policy manager	Policy management platforms contain sets of rules that include access rights for users and terminals. This provides complete visibility and role-based access control for IoT, BYOD, and corporate devices, as well as employees, contractors and guests across all multi-vendor wired, wireless and VPN infrastructures. Access policies also apply to remote users connecting via VPN clients or remote access points (RAPs).
Remote access points (RAPs)	Remote access points (RAPs) establish a secure SSL / IPSec VPN connection to a central controller via private Internet access, including cellular, home DSL and cable networks with the simplicity of plug-and-play. RAPs should be secure by design and use a factory certificate with a TPM chip for the connection. This provides certificate-based authentication tied to each individual RAP. In addition, all traffic is encrypted to secure data in transit.

Sandboxing	Sandboxing is a term from the computer security field that refers to separating a programme from other programmes into a discrete environment so that, in the event of errors or security problems, these problems do not spread to other areas of the computer.
VPN client	Hybrid IPsec / SSL VPN clients are optimal, as they automatically scan and select the best and most secure connection for terminating corporate-bound traffic. Unlike traditional VPNs that require dedicated hardware, VPN services integrate directly with existing secure infrastructure in the office to simplify architecture and management. In this deployment model, mobile devices or desktop workstations can securely access networks that process controlled, unclassified, confidential and classified information.
Zero trust security	This term summarises the key elements for implementing complete visibility of what is on the network: Endpoint and user authentication, policy-based access authorisation, and attack detection and prevention. This is based on the assumption of trusting nothing and no one (zero trust), with the aim of establishing continuous and dynamic security. In addition to protecting against new attack vectors, zero trust security reduces operational complexity, enhances the user experience by automating monitoring in the background, and eliminates the need to configure networks by applying access rules, which in turn can lead to entirely new operational models.

Bitkom represents more than 2,700 companies of the digital economy, including 1,900 direct members. Through IT- and communication services alone, our members generate a domestic annual turnover of 190 billion Euros, including 50 billion Euros in exports. The members of Bitkom employ more than 2 million people in Germany. Among these members are 1,000 small and medium-sized businesses, over 500 startups and almost all global players. They offer a wide range of software technologies, IT-services, and telecommunications or internet services, produce hardware and consumer electronics, operate in the digital media sector or are in other ways affiliated with the digital economy. 80 percent of the members' headquarters are located in Germany with an additional 8 percent both in the EU and the USA, as well as 4 percent in other regions of the world. Bitkom promotes the digital transformation of the German economy, as well as of German society at large, enabling citizens to benefit from digitalisation. A strong European digital policy and a fully integrated digital single market are at the heart of Bitkom's concerns, as well as establishing Germany as a key driver of digital change in Europe and globally.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom