



KAUGTÖÖ TURVALINE KORRALDAMINE

29.04.2020

KES ME OLEME?



TRINITI ADVOKAADID



Karmen Turk

Vandeadvokaat ja partner



Maarja Pild

Advokaat



Maarja Lehemets

Jurist

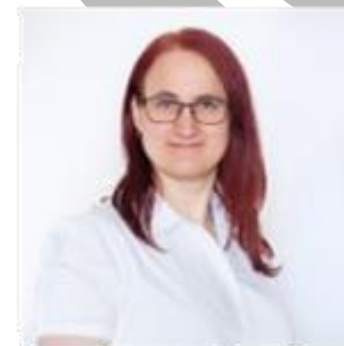


CYBERS INFOTURBESPETSIALISTID



Ats Onemar, CISA

CYBERS infoturbeanalüütik



Helena Jürgenson

CYBERS projektijuht



AJAPLAAN

30 minutit jagame enda kogemusi ja mõtteid

1. osa: terviseandmete kogumine
2. osa: kaugtöö reeglid
3. osa: turvalised lahendused koosolekuteks

30 minutit vastame teie küsimustele



Palun kirjuta enda **küsimused kohe** (vt ülal kollase ringikese juurde), kui need tekivad. Nii saame neile järjest vastata.

SISSEJUHATUS

Mis on tänaseks juhtunud?

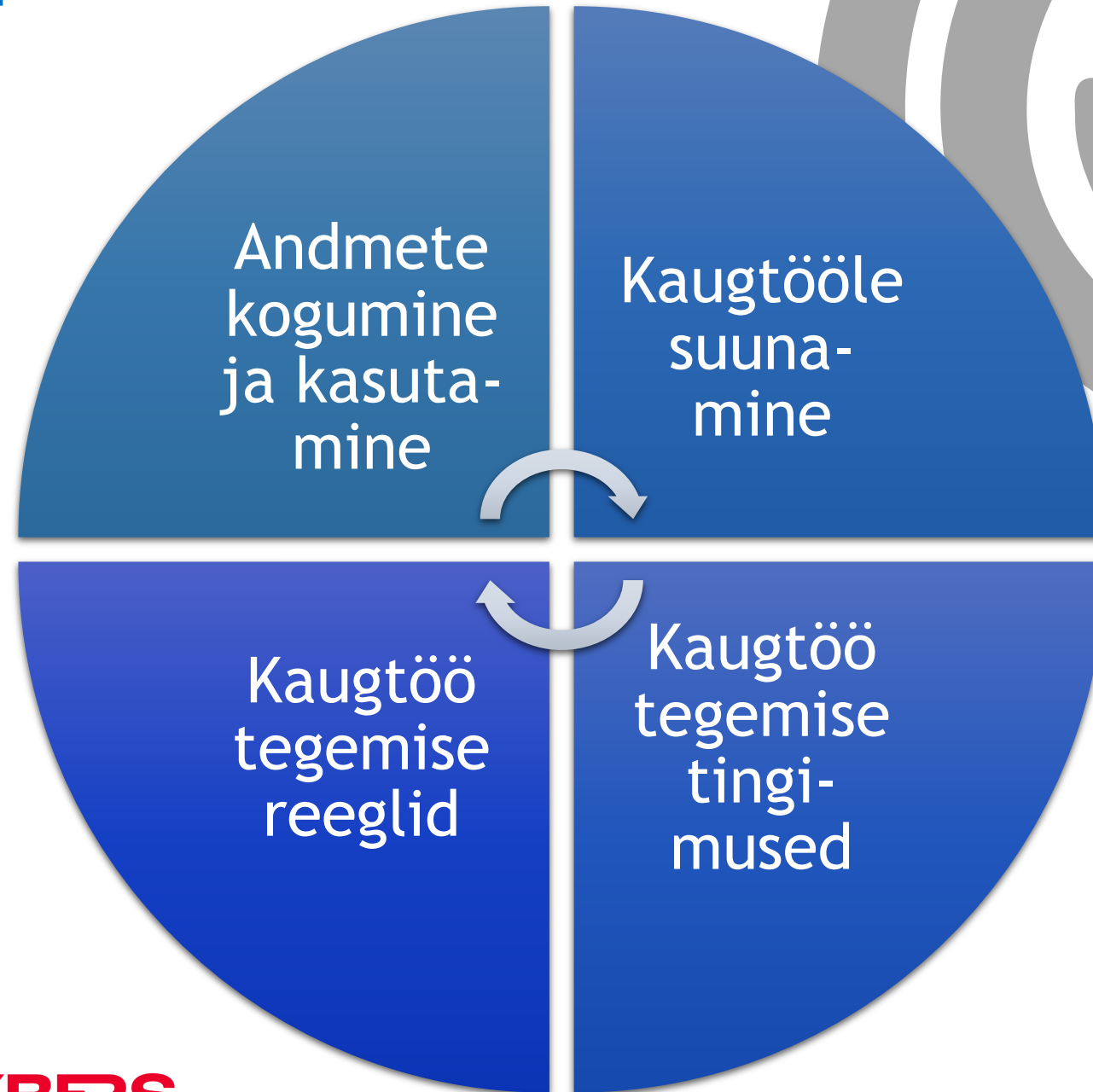


TÄNANE UUS REAALSUS



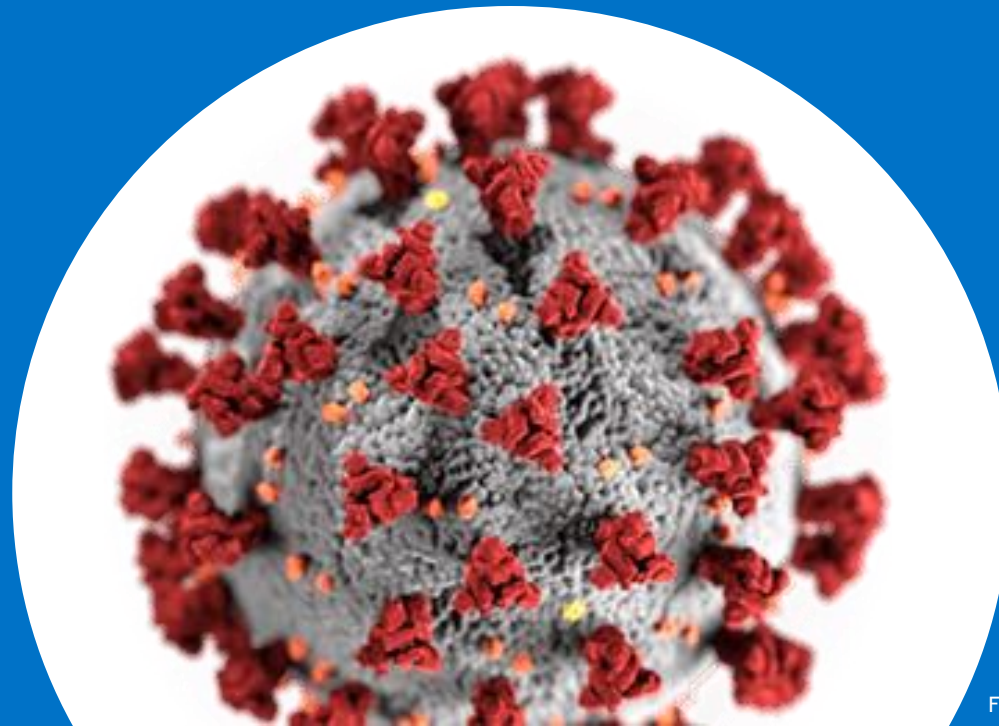
- ✓ KASUTAJA UUES OLUKORRAS
- ✓ KAUGTÖÖ PLATVORMID
TÄHELEPANU ALL
- ✓ INIMLIKUD VEAD

ÕIGUSLIKULT KERKINUD KÜSIMUSED



I OSA

Töötaja terviseandmete töötlemine



AKI kõrgendatud tähelepanu seoses terviseandmete töötlemisega



Andmekaitse Inspeksioon

20. märts · 🌐

AKI on saanud etteheiteid, et terviseandmete jagamisse suhtub asutus liiga rangelt, mis võib seada ohtu inimeste elu ja tervise. Oleme selles osas nõus, et suhtume rangelt, aga see on ennekõike sellepärast, et siseriiklik seadusandlus ei anna meile väga palju võimalusi seda teistmoodi teha.

Samas on koroonaviirus aga meie kõigi ühine mure, meie kõigi vastutus ja mitte ainult Eestis, vaid kogu maailmas. Tahame seda või mitte, aga terviseandmete töötlemist saab seaduslikuks lu... Vaata veel



TERVISEANDMETE TÖÖTLEMISEGA KAASNEV ÕIGUSLIK RISK

- Terviseandmeid kogu **võimalikult vähe** ja säilitada võimalikult **lühikest aega**
- Võimalusel kogu vaid **terviseandmetega seotud andmeid** (nt viirusekandjaga kokkupuutumine)



KAUGTÖÖ REEGLID TOP 10

1. Kes, millal, kelle juhisel?
2. Kus töötamine toimub?
3. Nõuded töötamise kohale
4. Nõuded seadmetele
5. Küberturbe meetmed



KAUGTÖÖ REEGLID TOP 10

JÄTK

6. Ärisaladuse kaitse
7. Tehniline abi
8. Kommunikatsiooni reeglid
9. Kontrollimise õigus



KAUGTÖÖ REEGLID TOP 10

JÄTK

10. Kaugtöö tegemise reeglite siduvus ja jõustamine

• Siduvus

- Töölepingulises suhtes
- Muus (nt käsundi-) suhtes

• Jõustamine

- Jälgimine
- Leppetrahv
- Kahju hüvitamine



KAUGTÖÖ REEGLITE KOKKUVÕTTED MEELDEJÄÄVAKS JA LIHTSAKS!

Fotode allikad:

- 1) https://www.thesagenext.com/blog/wp-content/uploads/2019/11/A_Preparatory_Timeline_Info.png
- 2) <https://venngage-wordpress.s3.amazonaws.com/uploads/2020/03/Employee-Remote-WFH-Policy-Guide-Infographic.png>
- 3) <https://pbs.twimg.com/media/ES29M00VAAEowqW.jpg>

5

WAYS HOW TO: KEEP YOUR DATA SECURE WHILE WORKING WITH A REMOTE TEAM



A vast majority of working people these days prefer a remote setup which allows them to utilize their skills, talents, and potential at their will. However, working with a remote team at times raises some security concerns. Hence comes the need to double-check your security measures.

Make Use of The Cloud



With cloud, you can easily connect with your team and work collaboratively without any location barriers. The cloud will provide you with round-the-clock accessibility and therefore, you can reach your data at any time.

Review Password Security

A password can make or break the entire security system for a firm. To ensure the tight security of the data, multi-factor authentication, anti-virus protection, and restricted access is recommended for firms. ****



Manage the Use of Public Wi-Fi



At times, your employees may need to access public Wi-Fi, restricting which may hamper productivity. Therefore, it is essential to follow some already constructed guidelines to avoid any unforeseen circumstances.

Conduct Training of Your Staff

To safeguard your critical data, it is important to provide proper training for cybersecurity to your employees. Training your remote team will help to deploy all the necessary security measures before your data is exposed to online threats.



Provide Remote Protection



If possible, devise your own remote protection software with the help of your IT department as it will help you to safeguard your precious data. You can share the software with the remote team and hence, can ensure that your data is safe.



TEKICON SOFTWARE Employee Remote WFH Policy & Guidelines

Tekicon Software's "Employee Remote Work Policy & Guidelines" outline our expectations and processes for employees who work from a location other than our offices. We want to ensure that both employees and our company will benefit from these arrangements.



Communication

- Check Online messages/emails frequently: Your notifications should not be on snooze, especially during critical release hours (pre-internal, post release etc).
- All meetings should use video conferencing (Google Hangouts): We suggest you turn on your video so everyone remains engaged.
- Make sure you have reliable WIFI: This is especially essential during meetings and release hours. If you won't be available online, let your team know in the online #WFH Slack Channel or add it in the Employee Time Off Google Calendar.



Take Home Your Work Equipment

- Please take your remote work station essentials: This includes your laptop, keyboard, mouse, headphones, additional monitors, and any other equipment. If you need any additional equipment, please email our HR Lead, Cynthia Morris at cynthia.morris@tekiconsoftware.com
- QA Team: Please ensure you have all the devices you need for testing purposes (iPhones, android phones, Mac laptops, PC laptops, chargers, etc.)



Mandatory / Circumstantial Scenarios

In circumstantial situations, if any of our offices or overall workplace is deemed unsafe to the health and safety of our employees and staff, then a mandatory work from home policy may be enforced and placed into effect.

Circumstantial scenarios can be a result of public health emergencies, structural construction that can cause risks/hazards, natural disasters, etc. The Human Resources team will provide updates and information to all employees and staff.



Maintain a Healthy Work/Life Balance

WFH does not mean you are expected to be available at all hours of the day. Set boundaries for yourself that allow you to unwind at the end of the work day. Get good sleeps. Take care of your health.



Confidential Information & Security

All remote employees and staff are responsible for maintaining the privacy and security of any company related documents, company data and other work-related materials confidential and secure in their remote location. All remote workers must comply with the guidelines of proper use of information technology as outlined in the Tekicon Software Employee Handbook.

For further inquiries or questions, please contact Cynthia Morris:
555-294-3374 ext. 225 or Cynthia.morris@tekiconsoftware.com

The National Cyber Security Alliance Recommends These Tips for Staying Safe Online While Working Remotely

1 CONNECT TO A SECURE NETWORK

and use a company-issued Virtual Private Network to access any work accounts. Home routers should be updated to the most current software and secured with a lengthy, unique passphrase. Employees should not be connecting to public WiFi to access work accounts unless using a VPN.



2 SEPARATE YOUR NETWORK

so your company devices are on their own WiFi network, and your personal devices are on their own.



3 KEEP DEVICES WITH YOU AT ALL TIMES

or stored in a secure location when not in use. Set auto log-out if you walk away from your computer and forget to log out.



4 LIMIT ACCESS TO THE DEVICE YOU USE FOR WORK

Only the approved user should use the device (family and friends should not use a work-issued device)



KASUTAJA TEADLIKKUS - MIDA TEHA

• Ole alalhoidlik

- 9 korda mõtle, 1 kord kliki

• Isikutuvastus

- Unikaalne, pikk ja keeruline parool
- Kasuta mitmetasemelist autentimist

• Seadme sihipärane kasutamine

- Tööandja vara kasuta vaid ise
- Andmeid töötle vaid ettenähtud keskkonnas
- Kasuta seadet kasutaja õigustega (mitte administraatori õigustega)

KASUTAJA TEADLIKKUS - MIDA TEHA

- Tööseade kodus
 - Jälgi füüsilist turvalisust
 - Lukusta ekraan!
- Tööine suhtlus
 - Kasuta kokkulepitud kanaleid
 - Krüpteerimine
- Sotsiaalmeedia
 - Firma grupid ja üritused
 - 9 korda mõtle, 1 kord postita :)



III OSA

Turvaline kaugtöö ja konverentskõned



VALIME TÖÖVAHENDID

- Koolita kasutajat
- IT toe olemasolu
- Kasutatavus vs turvalisus
- Töökindlus on osa turvalisusest
- Konfidentsiaalsus



ISIKUANDMETE TURVALISUSE TAGAMINE

- Identifitseerimise vajadused ja võimalused praktikas
- Kõnede, veebinaride jagamine





KÜSIMUSI? AITÄH



TRINITY@TRINITY.EE

INFO@CYBERS.EU



WWW.TRINITY.EE

WWW.CYBERS.EU

