OHJEITA TURVALLISTEN ETÄTYÖVÄLINEIDEN VALINTAAN

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

OHJEITA TURVALLISTEN ETÄTYÖVÄLINEIDEN VALINTAAN

www.huoltovarmuus.fi

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI

Huoltovarmuudella tarkoitetaan kykyä sellaisten yhteiskunnan taloudellisten perustoimintojen ylläpitämiseen, jotka ovat välttämättömiä väestön elinmahdollisuuksien, yhteiskunnan toimivuuden ja turvallisuuden sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi vakavissa häiriöissä ja poikkeusoloissa.

Huoltovarmuuskeskus (HVK) on työ- ja elinkeinoministeriön hallinnonalan laitos, jonka tehtävänä on maan huoltovarmuuden ylläpitämiseen liittyvä suunnittelu ja operatiivinen toiminta.

Julkaisija:
Huoltovarmuusorganisaatio

Selvityksen tekijä:
Tämä ohje tehtiin yhteistyössä F-Secure Oy:n, Cyber Security Services:n riippumattomien asiantuntijoiden kanssa.

- **Software Security Expert**
  Hiski Ruhanen F-Secure Consulting
- **Security Management Consultant**
  Ludvig Lund F-Secure Consulting
- **Technical Security Consultant**
  Antti Aitta F-Secure Consulting

Kuvat: Shutterstock

Taitto: Up-to-Point Oy

Julkaisuvuosi: 2020

ISBN: ISBN 978-952-5608-77-9

Sisältö

Johdanto **7**

Kuinka valita turvallinen työväline? **9**

Valitaanko pilvipalvelu vai paikallinen järjestelmä? **9**

Mitkä ovat työvälineen oletusasetukset ja ominaisuudet? **9**

Minkälaista tietoa työvälineessä halutaan käsitellä? **9**

Kuinka työvälineessä voi rajata tiedon käyttöoikeuksia? **9**

Onko työväline suunnattu ensisijaisesti kuluttajille vai yrityksille? **9**

Luovuttaako työväline tietoja kolmansille osapuolille? **9**

Ennen valintaa mieti käyttötapaukset **10**

Käytetäänkö työvälinettä organisaation ulkopuolisten kanssa viestimiseen tai julkisiin tapahtumiin? **10**

Käytetäänkö työvälinettä organisaation sisäiseen työskentelyyn? **10**

Käsitelläänkö tietoa, joka ei saa päätyä ulkopuolisten käsiin? **10**

Käsitelläänkö tietoa, johon pitää rajoittaa pääsyä organisaation sisällä? **10**

Millaiset lisenssi- tai käyttäjämäärävaatimukset työvälineessä on? **10**

Vastuu turvallisesta käytöstä on sekä organisaatiolla että käyttäjillä **10**

Yleisten pikaviestintä- ja etäkokoustyövälineiden tietoturvaominaisuuksia **12**

Yleisten ryhmätyöskentely- ja tiedostonjako-työvälineiden tietoturvaominaisuuksia **13**

Vertailumetodologia **14**

Käytettyjä lähteitä ja sovellusten käyttösuosituksia **15**

Asetusten kovennusohjeita **18**

JOHDANTO

Etätyöskentelyyn tarkoitettujen pikaviesti-, telekommunikaatio- ja ryhmätyövälineiden tarve on kasvanut merkittävästi. COVID-19-pandemian myötä tarve korostui nopean etätyösiirtymän myötä. Etätyöskentelyyn saatavilla olevien työvälineiden turvallisuuden taso vaihtelee kuitenkin merkittävästi ja moni kaipaa tukea tarvittavan työvälineiden turvallisuusominaisuuksien valinnassa: mitä huomioida ja miten eri työvälineiden ominaisuudet poikkeavat toisistaan?

Tämän oppaan tarkoitus on auttaa organisaatioita valitsemaan oikeanlaiset ja turvalliset työvälineet etätyöskentelyyn. Erityishuomiota näiden työvälineiden valintaan ja turvalliseen käyttöön tulee kiinnittää organisaatioissa, joissa käsitellään tietoturvaluokiteltua materiaalia. Opas on tarkoitettu erityisesti niille työntekijöille, jotka kokevat turvallisuuden huomioimisen etätyöskentelyssä tärkeäksi, mutta toivovat tueksi selkeytettyä materiaalia oikeiden ominaisuuksien huomioimiseksi. Sekä niiden tietoturvasta vastaavien työntekijöiden avuksi, jotka valitsevat ja asentavat organisaation etätyösovelluksia ja kaipaavat yksinkertaistettua vertailua etätyökalujen turvallisuusominaisuuksista. Parhaimmillaan oppaan myötä etätyövälineiden tietoturvallisten ominaisuuksien vaatiminen leviää yrityksissä oletusarvoiseksi käyttötavaksi.

Oppaassa käydään alkuun läpi kysymyksiä, jotka helpottavat oikeanlaisen etätyövälineen valintaa. Lisäksi on syytä huomioida käyttötapaukset, mihin työvälinettä ensisijaisesti on tarkoitus käyttää. Esimerkiksi julkisen tilaisuuden järjestämiseen tarvitaan erilaisia ominaisuuksia kuin pienen työryhmän sisäiseen keskusteluun. Taulukoissa vertaillaan eri etätyövälineiden tietoturvaominaisuuksia. Ominaisuuksia voi peilata omaan käyttötarpeeseen ja soveltaa etätyövälineiden valintaan myös muiden etätyövälineiden osalta. Loppuun on kerätty vertailtujen sovellusten tietoturvan parantavat oppaat eli kovennusohjeet sekä vertailussa käytettyjä lähteitä ja sovellusten käyttösuosituksia.

Oppaan laatimiseen on käytetty uusimpia lähteitä ominaisuuksien vertailuun ja käyttösuosituksiin. Lukijan on syytä huomioida, että ominaisuudet muuttuvat ja hyvä on tarkistaa, onko ohjeen jälkeen ilmestynyt tuoreempia ohjeita tai suosituksia. Oppaan myötä toivotaan tekojen ja valintojen kautta yrityskulttuurin muuttuvan entistä enemmän tietoturvaa suosivaksi. Yrityksistä lähtöisin oleva kysyntä lisää myös tarjolla olevia turvallisia ominaisuuksia.

”Mitä huomioida ja miten eri työvälineiden ominaisuudet poikkeavat toisistaan?”

KUINKA VALITA TURVALLINEN TYÖVÄLINE?

Tässä kappaleessa käydään läpi tärkeimpiä kysymyksiä, mitkä tulee pohtia tarkoituksenmukaista etätyöskentelysovellusta valittaessa.

Valitaanko pilvipalvelu vai paikallinen järjestelmä?

Suurten toimijoiden toimittamat pilvipalvelut ovat usein turvallisempi vaihtoehto kuin omaan konesaliin sijoitetut palvelut. Itse ylläpidettyä ratkaisua kannattaa kuitenkin harkita, mikäli vaihtoehtoiset pilvipalvelut eivät ole toimittajan pääliiketoimintaa tai palveluntarjoaja on pieni ja uusi yritys. Mikäli palvelulta vaaditaan korkeaa tietoturvatasoa, täytyy muistaa, että itse ylläpidetyn ratkaisun ylläpitoon ja tietoturvan hallintaan tulee varata riittävät resurssit.

Mitkä ovat työvälineen oletusasetukset ja ominaisuudet?

Usein työvälineen oletusasetukset eivät ole riittäviä, ja käyttöönottajan vastuulle jää turvamekanismien, kuten riittävän salauksen, kaksivaiheisen tunnistautumisen (Two Factor Authentication, 2FA) ja pääsyrajauksien asettaminen. Monelle työkalulle on julkaistu tietoturvaa parantavia asetusten kovennusoppaita tai listoja tärkeimmistä tietoturva-asetuksista. Ennen käyttöönottoa työvälineiden oletusasetukset tulisi aina käydä läpi ja varmistaa, että työkalussa on halutut tietoturvaominaisuudet käytössä.

Minkälaista tietoa työvälineessä halutaan käsitellä?

Työvälineille asetettavat tietoturvavaatimukset riippuvat siitä, käsitelläänkö työvälineellä liiketoiminnalle kriittistä tietoa vai viranomaisen määrittelemää luokiteltua tietoa. Organisaation on noudatettava lakia julkisen hallinnon tiedonhallinnasta (9.8.2019/906), jossa määritellään, kuinka eri turvallisuustasoista luokiteltua materiaalia käsitellään. Tässä ohjeessa on huomioitu lain mukainen turvallisuus luokka IV (TLIV).

Kuinka työvälineessä voi rajata tiedon käyttöoikeuksia?

Jos palvelussa on tarkoitus käsitellä liiketoiminnalle kriittistä tietoa, on tärkeää, että tiedon jakamista organisaation ulkopuolelle voidaan rajoittaa ja että pääsyä tietoon voidaan rajoittaa henkilö- tai ryhmäkohtaisesti.

Onko työväline suunnattu ensisijaisesti kuluttajille vai yrityksille?

Yrityksille suunnattujen työvälineiden tietoturvassa on usein toteutettu keskitetyn hallinnan sekä organisaation tarvitseman pääsynhallinnan ominaisuuksia. Kuluttajille suunnattujen palvelujen tai ilmaisversioiden tietoturvaominaisuudet eivät lähes koskaan riitä organisaation käyttötarkoituksiin.

Luovuttaako työväline tietoja kolmansille osapuolille?

Valittaessa työvälinettä kannattaa tarkastaa, että toimittajalla on selkeä tietosuojaseloste, jossa kerrotaan, mihin työvälineen tietoja käytetään ja kenelle niitä luovutetaan. Pilvipalveluissa on mahdollista, että paikallinen lainsäädäntö mahdollistaa ulkomaiden viranomaisten pääsyn tietoon, jolloin palvelua ei voida käyttää turvaluokitellun tiedon käsittelyyn.

ENNEN VALINTAA MIETI KÄYTTÖTAPAUKSET

Työvälineen tietoturvavaatimuksien tulee kattaa kaikki sen eri käyttötapaukset. Kattavasti laaditut käyttötapaukset kuvaavat tiedonkäytön monipuolisesti ja mahdollistavat uhka-arvioinnin tekemisen.

Käytetäänkö työvälinettä organisaation ulkopuolisten kanssa viestimiseen tai julkisiin tapahtumiin?

Kun viestitään organisaation ulkopuolisten kanssa, on tärkeää hallita kokousten osallistujia esimerkiksi odotushuoneita tai salasanaa käyttäen. Jos samaa työvälinettä käytetään myös organisaation sisäisesti, täytyy välineessä näkyä selvästi ero sisäisen ja ulkoisen tiedonvälityksen välillä.

Käytetäänkö työvälinettä organisaation sisäiseen työskentelyyn?

Sisäisen työskentelyn välineissä suurimmat riskit liittyvät usein käyttäjänhallintaan ja palveluiden turvaamiseen organisaatioverkon ulkopuolelta. Hyviä tapoja vähentää tietoturvariskejä ovat seuraavat ratkaisut: Kertakirjautumisella (Single Sign On, SSO) palvelun käyttäjänhallinnan yhdistäminen organisaation muihin järjestelmiin sekä pääsyn salliminen organisaation verkon ulkopuolelta vain kaksivaiheista tunnistautumista (2FA) käyttäen

Käsitelläänkö tietoa, joka ei saa päätyä ulkopuolisten käsiin?

Pilvipalveluissa on usein toiminnallisuuksia, jotka mahdollistavat sisällön jakamisen sähköpostilla tai jaetun linkin kautta. Organisaation tiedostojen ja sisällön jakaminen tulee aina oletuksena rajata vain sisäiseen käyttöön ja luoda erikseen säännöt julkisen materiaalin jakamiselle.

Käsitelläänkö tietoa, johon pitää rajoittaa pääsyä organisaation sisällä?

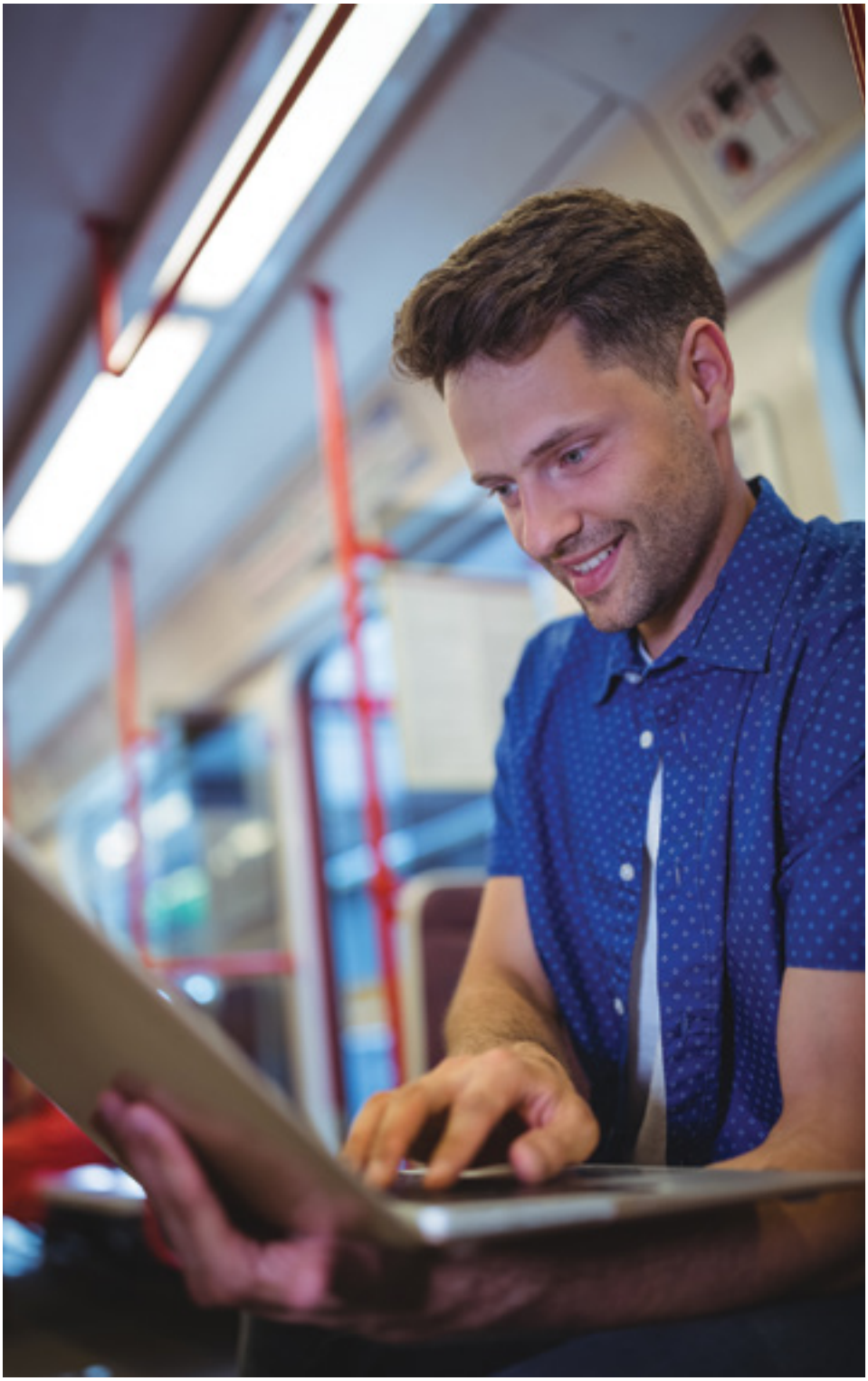
Sisäiseen käyttöön kannattaa usein valita työkalu, jossa tietoon pääsyä voi rajata eri ryhmille ja tarvittaessa myös yksittäisille käyttäjille.

Millaiset lisenssi- tai käyttäjämäärävaatimukset työvälineessä on?

Muista tarkastaa työvälineen tukemat ominaisuudet, käyttäjämäärät ja mahdolliset lisenssivaatimukset ennen lopullisen valinnan tekemistä, jotta työväline sopii kaikkiin haluttuihin käyttötarkoituksiin.

Vastuu turvallisesta käytöstä on sekä organisaatiolla että käyttäjillä

Turvallisen etätyöskentelyn toteutumiseksi käyttäjien tulee käyttää työvälineitä organisaation ohjeistusten mukaisesti ja organisaation tulee suunnitella työvälineiden turvallinen käyttö sekä ohjeistaa se käyttäjille. Mikään työväline ei ole tietoturvallinen, mikäli sitä käytetään turvattomasti.



Yleisten pikaviestintä- ja etäkoustyövälineiden tietoturvaominaisuuksia

TYÖKALU	Pika-viestintä	Etä-kokous	Paikal-linen palvelin	Pilvi-palvelu	Päästä päähän salaus	TLIV-luokitellun tiedon käsittely	Kerta-kirjautuminen	Kaksivaiheinen tunnistau-tuminen
Slack	✓	✓		☁			✓	✓
Mattermost Enterprise	✓	✓	⌂			✓	✓	✓
Teams	✓	✓		☁			✓	✓
Signal	✓			☁	✓		🔍	🔍
WhatsApp	✓			☁	✓			
Zoom Business		✓		☁	✓		✓	✓
Webex		✓	⌂	☁	ⓘ		✓	
BlueJeans		✓		☁	ⓘ		✓	✓
Click Meeting		✓		☁				

🔍 Signal tarjoaa osapuolien vahvan todentamisen ja tiedon paikallisen suojaamisen PIN-koodin avulla.

ⓘ Päästä päähän salaus ei toteudu etäkokouksissa, joihin osallistutaan puhelimitse tai jotka nauhoitetaan (Webex).

Yleisten ryhmätyöskentely- ja tiedostonjakotyövälineiden tietoturvaominaisuuksia

TYÖKALU	Ryhmätyö	Tiedostonjako	Paikallinen palvelin	Pilvipalvelu	Ulkopuolisille jakamisen rajoittaminen	TLIV-luokitellun tiedon käsittely	Kertakirjautuminen	Kaksivaiheinen tunnistautuminen
OneDrive, SharePoint (365)	✓	✓	⌂	☁	✓	🔍	✓	✓
Google Drive, Docs (G-Suite)	✓	✓		☁	✓		✓	✓
Dropbox Enterprise, Dropbox Paper	✓	✓		☁	✓		✓	✓
Dropbox Professional		✓		☁				✓
Collabora Online	✓		⌂		ⓘ	ⓘ	ⓘ	ⓘ

🔍 Palvelun tetoturvaominaisuudet voidaan toteuttaa sekä pilvipalvelussa että omassa konesalissa.

ⓘ Tietoturvaominaisuuksien toteutus Collabora Onlineen vaatii runsasta asennuksen mukautusta.

Taulukoissa käytettyjen termien selitykset

Paikallinen palvelin	*Palvelu on asennettuna organisaation omaan konesaliin omassa verkkoympäristössä.*
Pilvipalvelu	*Palvelua käytetään internetin yli, ja siihen liittyvät palvelimet ovat palveluntarjoajan hallinnassa.*
Päästä päähän salaus	*Tiedonsiirto on salattu keskustelun osanottajien välillä niin, ettei keskustelua välittävä osapuoli voi purkaa salausta.*
Ulkopuolisille jakamisen rajoittaminen	*Palvelussa voidaan rajoittaa tiedostojen jakamista muille anonyymien linkkien kautta vaatimalla vastaanottajien tunnistautumista palveluun.*
TLIV-luokitellun tiedon käsittely	*Palvelussa on tietoturvaominaisuudet, joita käyttämällä voidaan täyttää julkisen pilvipalvelulinjauksien ja VAHTI-ohjeen määrittelemät vaatimukset viranomaisen turvaluokitellun tiedon käsittelyyn turvallisuusluokan IV osalta.*
Kertakirjautuminen (Single Sign On, SSO)	*Palveluun kirjautuminen ja käyttäjien hallinta on yhdistetty organisaation omaan käyttäjänhallintaan, jolloin palveluun voidaan kirjautua organisaation omia tunnuksia käyttäen.*
Kaksivaiheinen tunnistautuminen (Two Factor Authentication, 2FA)	*Palveluun kirjautuessa voidaan tunnistaa käyttäjä vahvemmin käyttämällä tunnuksen ja salasanan lisäksi esimerkiksi tekstiviestillä lähetettävää kertakäyttöistä koodia.*

VERTAILUMETODOLOGIA

Vertaillut sovellukset valittiin Suomessa yleisesti tunnettujen ja laajalti käytössä olevien ratkaisuiden joukosta. Otokseen sisällytettiin myös ensisijaisesti kuluttajille tai pienyrityksille suunnattuja sovellusversioita, kuten Dropbox Professional, jotta erot suurille yrityksille kohdistettuihin ratkaisuihin kävisivät selviksi.

Sovelluksia tarkasteltiin yksitellen ottamatta huomioon, kuinka eri työkalujen yhteiset alustat tai niiden väliset yhdistämismahdollisuudet vaikuttavat työvälineen käyttöön tai tietoturvaan.

Vertailussa tarkasteltiin avoimia tietolähteitä. Työvälineiden julkaisijoiden omat selvitykset toimivat ensisijaisina lähteinä, sillä harvasta vertailussa mainitusta sovelluksesta löytyi riippumattomien tutkijoiden tekemiä julkaisuja.

Vertailuun käytetyt lähteet löytyvät omasta liitteestään. Sovellusten vertailuun ei tehty teknisiä tarkastuksia tässä yhteydessä.

Kaikki vertailuun käytetty aineisto oli uusinta mahdollista eli se oli julkaistu vuoden 2020 toukokuussa. Jokaisen organisaation on itse varmistuttava työkalujen sopivuudesta omaan ympäristöönsä ja tarkastaa ratkaisun tietoturva, mikäli tilanne muuttuu päivitysten tai uusien ominaisuuksien myötä.

KÄYTETTYJÄ LÄHTEITÄ JA SOVELLUSTEN KÄYTTÖSUOSITUKSIA

Ohjelmistojen ja palveluiden soveltuvuuden arvioinnissa hyödynnettiin julkisen hallinnon pilvipalvelulinjauksia[1] ja VAHTI-ohjetta[2]. Alla olevissa taulukoissa listataan vertailussa arvioituja ratkaisuita kuvauksineen, sekä viitteitä tietolähteisiin, joita arvioinnissa hyödynnettiin.

Ohjelmisto / Palvelu	Mattermost
Kuvaus ja käyttösuositus	Avoimen lähdekoodin keskitetty pikaviestintäsovellus, josta on saatavilla kaupallinen yritysversio. Mattermost soveltuu parhaiten organisaation sisäiseen ja tiimien väliseen viestintään.
Viite	*https://mattermost.com/security/*

Ohjelmisto / Palvelu	Slack
Kuvaus ja käyttösuositus	Kaupallinen keskitetty pikaviestintäsovellus puheluominaisuuksilla. Slack soveltuu organisaation sisäiseen ja tiimien väliseen viestintään.
Viite	*https://slack.com/intl/en-fi/security*

Ohjelmisto / Palvelu	Microsoft Teams
Kuvaus ja käyttösuositus	Microsoftin tarjoama kaupallinen pikaviestintä- ja etäkokoussovellus. Teams soveltuu hyvin organisaation ja tiimien sisäiseen sekä yhteistyökumppaneiden väliseen viestintään organisaatiorajojen yli.
Viite	*https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview*

Ohjelmisto / Palvelu	Signal
Kuvaus ja käyttösuositus	Avoimen lähdekoodin alustariippumaton pikaviestintä- ja puhelusovellus. Sovellusta voidaan käyttää yksityiseen viestinvälitykseen, kun halutaan salata viestit ja puhelut sekä varmistua toisen osapuolen henkilöllisyydestä. Signalin käyttö turvallisesti vaatii käyttäjiltä tavanomaista parempaa tietoturvaosaamista.
Viitteitä	*https://support.signal.org/hc/en-us/articles/360007059792-Signal-PINs* *https://signal.org/en/*

Ohjelmisto / Palvelu	WhatsApp
Kuvaus ja käyttösuositus	Facebookin omistama alustariippumaton pikaviestintä- ja puhelusovellus. Sovellusta voidaan käyttää julkisen tiedon käsittelyyn ja viestintään, mikäli tiedon luottamuksellisuuden vaarantumisesta ei aiheudu vakavia vaikutuksia.
Viite	*https://www.whatsapp.com/security/*

1) https://julkaisut.valtioneuvosto.fi/handle/10024/161294
2) https://www.vahtiohje.fi/web/guest/home

Ohjelmisto / Palvelu	Zoom
Kuvaus ja käyttösuositus	Kaupallinen videokokoussovellus. Sovellusta voidaan käyttää organisaation ja ulkopuolisten yksityishenkilöiden väliseen viestintään. Jos Zoomia halutaan käyttää organisaation sisäiseen viestintään tai luottamuksellisen tiedon välitykseen, on suositeltavaa käyttää Zoomin Business- tai Enterprise-versioita.
Viite	*https://zoom.us/docs/en-us/privacy-and-security.html*

Ohjelmisto / Palvelu	Cisco Webex
Kuvaus ja käyttösuositus	Ciscon tarjoama kaupallinen videokokoussovellus. Webexin Business-versio soveltuu parhaiten organisaation sisäiseen tai kumppanien väliseen viestintään. Webexin muissa versiossa ei ole kertakirjautumisominaisuutta, joka helpottaa organisaation käyttäjänhallintaa.
Viite	*https://www.cisco.com/c/dam/en/us/products/collateral/conferencing/webex-meeting-center/white-paper-c11-737588.pdf*

Ohjelmisto / Palvelu	BlueJeans
Kuvaus ja käyttösuositus	Kaupallinen video- ja etäkokoussovellus. BlueJeans soveltuu organisaation sisäiseen ja tiimien väliseen viestintään.
Viite	*https://www.bluejeans.com/products/secure-video-conferencing*

Ohjelmisto / Palvelu	ClickMeeting
Kuvaus ja käyttösuositus	Kaupallinen video- ja etäkokoussovellus. Sovellus soveltuu parhaiten julkisen tai vähemmän kriittisen tiedon käsittelyyn, sillä siitä puuttuu tietoturvaominaisuuksia, kuten kertakirjautuminen ja monivaiheinen tunnistautuminen.
Viite	*https://knowledge.clickmeeting.com/privacy-security/security-policy/*

Ohjelmisto / Palvelu	Microsoft OneDrive/SharePoint
Kuvaus ja käyttösuositus	Microsoftin tarjoama kaupallinen sovellus, joka on suunniteltu organisaation sisäiseen ja tiimien väliseen ryhmätyöskentelyyn ja tiedostonjakoon.
Viitteitä	*https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices* *https://support.office.com/en-us/article/set-up-your-microsoft-365-sign-in-for-multi-factor-authentication-ace1d096-61e5-449b-a875-58eb3d74de14* *https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off*

Ohjelmisto / Palvelu	Google G-Suite (Google Drive, Google Docs)
Kuvaus ja käyttösuositus	Googlen tarjoama kaupallinen sovellus, joka on suunniteltu organisaation sisäiseen ja tiimien väliseen ryhmätyöskentelyyn ja tiedostonjakoon.
Viite	*https://gsuite.google.com/security/*

Ohjelmisto / Palvelu	Dropbox Business / Enterprise
Kuvaus ja käyttösuositus	Dropboxin organisaatioille tarjoama sovellus, joka on suunniteltu organisaation sisäiseen ja tiimien väliseen tiedostonjakoon
Viite	*https://www.dropbox.com/business/trust/security/control-visibility*

Ohjelmisto / Palvelu	Dropbox Professional
Kuvaus ja käyttösuositus	Dropboxin tarjoama sovellus yksittäisille käyttäjille tiedostojen jakamiseen. Dropboxin Professional-, Basic- ja Plus-versioissa ei ole organisaation käyttöön tarkoitettua käyttäjänhallintaa tai tarvittavia tietoturvaominaisuuksia, kuten jakamisen estäminen organisaation ulkopuolelle, eikä niitä ole suositeltavaa käyttää organisaatiokäytössä tiedostojen jakamiseen.
Viite	*https://www.dropbox.com/security*

Ohjelmisto / Palvelu	Dropbox Paper
Kuvaus ja käyttösuositus	Dropboxin tarjoama reaaliaikaiseen ryhmätyöskentelyyn suunnattu sovellus. Sovellusta voi käyttää yhdessä Dropboxin tiedostonjakopalvelun kanssa, ja se soveltuu organisaation sisäiseen ja tiimien väliseen ryhmätyöskentelyyn.
Viite	*https://help.dropbox.com/files-folders/paper/admin-settings-business-teams*

Ohjelmisto / Palvelu	Collabora Online
Kuvaus ja käyttösuositus	Avoimen lähdekoodin reaaliaikaiseen ryhmätyöskentelyyn suunnattu sovellus. Mikäli sovellusta halutaan käyttää organisaatiossa, sen käyttöönotto vaatii huomattavaa asetusten mukauttamista ja mahdollisia lisäpalveluja, jotta siihen saadaan organisaatiolle tarvittavat tietoturvaominaisuudet.
Viite	h*ttps://www.collaboraoffice.com/collabora-online/*

ASETUSTEN KOVENNUSOHJEITA

Osa vertailuun valituista työvälineistä vaativat tuotteen ostoa, ennen asetusten kovennusohjeiden saamista työvälineen julkaisijalta. Kaikki tässä julkaisussa hyödynnetyt kovennusohjeet olivat ajantasaisia 15.5.2020.

Työvälineiden asetusten kovennusohjeita ja -vinkkejä:

Microsoft Teams:

https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview

https://docs.microsoft.com/en-us/microsoftteams/teams-security-guide

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-wide-setup-for-increased-security?view=o365-worldwide

Microsoft Sharepoint/OneDrive:

https://docs.microsoft.com/en-us/sharepoint/security-for-sharepoint-server/security-hardening

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-wide-setup-for-increased-security?view=o365-worldwide

Mattermost:

https://docs.mattermost.com/guides/administrator.html

Slack:

https://slack.com/intl/en-fi/help/articles/115004155306-Security-tips-to-protect-your-workspace

Zoom Business:

https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

Cisco Webex:

https://help.webex.com/en-us/8zi8tq/Cisco-Webex-Best-Practices-for-Secure-Meetings-Hosts

BlueJeans:

https://www.bluejeans.com/blog/bluejeans-best-practices-keeping-your-meetings-private

Google G-Suite (Google Drive):

https://support.google.com/a/answer/7587183?hl=en

Dropbox:

https://help.dropbox.com/accounts-billing/security

HUOLTOVARMUUSORGANISAATIO
DIGIPOOLI