Tietoturvakuvaus

10.11.2020
Julkinen

Versiohistoria

Päivämäärä	**Henkilö**	**Kuvaus**
10.11.2020	Sami Pussinen	Lisättiin lisätietoja kokouksista
20.10.2020	Sami Pussinen	Lisättiin kuvaukset tiedostosynkronoinnista
15.07.2020	Sami Pussinen	Lisättiin kuvaukset allekirjoituksista
5.6.2020	Sami Pussinen	Julkaistiin julkinen versio

Johdanto

Palvelun tietoturvallisuus on Viilulle ensiarvoisen tärkeää ja se on huomioitu kaiksessa yritykseme toiminnassa. Tässä asiakirjassa kuvataan Viilu Solutions Oy:n tietoturvaperiaatteet ja -käytännöt.

Asiakirjaa voidaan täydentää erillisillä tarkemmilla järjestelmä-, prosessi ja liiketoiminta-aluekohtaisin ohjein.

Kaikkien Viilun työntekijöiden on noudatettava tässä asiakirjassa esitettyä ohjeistusta.

Yleiset tietoturvaperiaatteet ja ohjeet

Viilun käsittelee tietoa sähköisesti ja hyvin vähäisissä määrin ei-sähköisesti. Esimerkki ei-sähköisestä käsittelystä on paperisen sopimuksen allekirjoittaminen mikäli asiakas ei pysty toteuttamaan allekirjoitusta sähköisessä muodossa. Palvelu tai Viilun henkilöstö ei käsittele mitään tietoa ei-sähköisesti normaaliolosuhteissa.

Viilun käsittelemä tieto jakautuu eri luottamusasteille. Esimerkiksi Viilun ja asiakkaan väliset sopimusasiat, henkilötiedot tai Viilun tekijänoikeudelliset seikat lukeutuvat luottamukselliseen tietoon. Tämäntyyppisiä tietoja käsiteltäessä on erityisen tärkeää noudattaa tämän asiakirjan ohjeistusta. Muihin tietoihin, kuten julkisiin tietoihin ja tietoihin, jotka eivät ole luottamuksellisia tulee soveltaa tämän asiakirjan ohjeita soveltuvin osin ja niin, ettei se kohtuuttomasti haittaa työtehtävän suorittamista. Epäselvissä tilanteissa työntekijä on velvoitettu kysymään ohjeistusta tietoturvavastaavalta.

Vastuut ja tietoturvan kehittämisprosessi

Viilu Solutions Oy:n tietoturvasta ja tietosuojasta vastaa toimitusjohtaja Sami Pussinen. Tietoturvavastaava vastaa myös tietoturvallisuuden toteutumisesta ja johtaa tietoturvaan liittyvää operatiivista toimintaa.

Tietosuojasta vastaa rekisterinpitäjä. Tietosuojavastaava seuraa ja valvoo, että tietosuoja-asetusta sekä muita lainsäädäntöjä noudatetaan. Tietoturvan- ja suojan toimeenpanoa ohjaa tietosuojavastaava.

Tietoturvan toteuttamisesta teknisissä järjestelmissä vastaa kehitysosasto. Kehitysosastolla tulee olla riittävä asiantuntemus teknisten ratkaisujen määrittelyyn ja toteuttamiseen sekä tietoverkkojen ja -järjestelmien tietoturvavalvontaan. Tietoturvavastaava koordinoi teknisen tietoturvan toteuttamista.

Esimiesten tehtävä on huolehtia, että heidän alaisensa tuntee tietoturvaperiaatteet ja -vastuut, että alainen on tutustunut tähän asiakirjaan ja saa tarvittavan koulutuksen.

Jokainen Viilun työntekijä, alihankkija ja Viilun tarjoamiin palveluihin käyttöoikeuden saanut henkilö on velvollinen noudattamaan annettuja ohjeita. Jokainen vastaa omalla toiminnallaan tietoturvan toteutumisesta ja edistää hyvän tietotuvakulttuurin kehittymistä.

Tietoturvaperiaatteiden ja -ohjeiden noudattaminen

Jokainen Viilun työntekijä on velvollinen noudattamaan tämän asiakirjan ja tätä asiakirjaa täydentäviä ohjeita. Ohjeiden laiminlyöminen tai niiden vastaisesti toimiminen katsotaan tietoturvarikkeeksi. Ohjeiden tarkoituksenmukainen laiminlyönti tai rikkominen voi johtaa seuraamuksiin rikkeen vakavuudesta riippuen.

Mikäli rikkeeseen liittyy rikosepäily, päättää toimitusjohtaja tutkintapyynnön tekemisestä poliisille. Rikosepäilyn tapauksessa Viilu voi sulkea käyttöoikeudet määräajaksi. Käyttöoikeudet voidaan sulkea myös, mikäli yhtiön tietoturva merkittävästi vaarantuu käyttäjän toiminnan takia.

Tietoturvapoikkeamien raportointi ja käsittely

Jokaisella Viilun työntekijällä on velvollisuus ilmoittaa havaitsemistaan tietoturvapoikkeamista ja -puutteista sekä epäilemistään väärinkäytöksistä tai tietoturvarikkomuksista tietoturvavastaavalle tietoturva@vii.lu tai omalle esimiehelleen. Havaittuja poikkeamia hyödynnetään tietoturvallisten toimintatapojen, prosessien ja teknisten ympäristöjen kehittämiseen.

Mikäli poikkeamiin liittyy rikosepäily päättää toimitusjohtaja tutkintapyynnön tekemisestä poliisille.

Palveluun tallennetut tiedot ja niiden käsittely

Kaikelle henkilötietojen ja luottamuksellisen tietojen keruulle on oltava pätevä peruste, joka pohjaa joko lainsäädäntöön tai liiketoiminnan tarpeisiin. Liiketoiminnan peruste ei voi olla ristiriidassa lainsäädännön, oikeushenkilöiden tai yksityishenkilöiden oikeuksien kanssa. Tiedot tallennetaan rekistereihin ja jokaisesta rekisteristä tuotetaan seloste tietosuojaselosteeseen.

Tietoja säilytetään palvelussa niin kauan kun niitä tarvitaan asiakkaan palvelemiseen, kunnes asiakas poistaa tiedot tai pyytää Viilua poistamaan tiedot. Tarkemmat aikamääreet näet tietosuojaselosteesta.

Henkilötiedot (Personally identifiable Information)

Yksityishenkilöitä koskevia tietoja säännöstelee Euroopan tietosuoja-asetus (GDPR). Yksityishenkilön on pystyttävä pyytämään Viilua poistamaan kaikki heitä koskevat tiedot tai pyytämään kooste kaikesta häntä koskevasta tiedosta.

Viilu tallentaa rekistereihinsä vain välttämättömät henkilötiedot. Viilu ei koskaan tallenna rekistereihin tietoja kuten henkilötunnus tai syntymäaika. Vahvaan tunnistautumiseen käytetään tunnistusvälittäjää Telia Oyj.

Henkilötiedot näkee palvelusta vain tunnistautuneet käyttäjät, joille on annettu käyttöoikeus käyttäjänhallintaan (Esim. isännöitsijä).

Taloyhtiöiden asukkaat/osakkaat ja isännöintiyritysten henkilöstö sijaitsevat eri rekistereissä ja ovat hallinnoitavissa erikseen.

Tunnukset ja salasanat

Tunnuksien hallinta ja kirjautuminen on ulkoistettu tunnistautumisvälittäjille kaikissa tunnistautumistavoissa. Viilun henkilöstöllä tai järjestelmillä ei ole pääsyä käyttäjien tunnuksiin tai salasanoihin. Näitä tietoja ei tallenneta Viilun rekistereihin.

Asiakirjat

Asiakkaat voivat tallentaa palveluun asiakirjoja ja tiedostoja. Asiakirjoihin on pääsy vain henkilöillä, jotka ovat kirjautuneet sisään palveluun ja omaavat käyttöoikeudet kyseisiin asiakirjoihin. Poikkeus tähän on kokousten aineistot, mikäli kokous on määritelty avoimeksi ilman kirjautumista. Tässäkin tapauksessa käyttäjällä tulee olla hänelle jaettu yksilöllinen linkki asiakirjoihin käsiksi päästäkseen.

Kokoukset

Palveluun tallennetaan tietoja kokousten järjestämiseksi. Tietoihin sisältyy asiakkaan syöttämät tiedot, kuten paikka, aika ja kutsutut osallistujat. Näihin tietoihin pääsee käsiksi vain kirjautunut käyttäjä, joka omaa tarvittavat käyttöoikeudet (esimerkiksi hallituksen jäsen).

Kokous voidaan myös määritellä toimimaan ilman tunnistautumista, jolloin osallistujille lähetetään kokouksen yksilöllinen linkki sähköpostitse tai tekstiviestitse.

Allekirjoitukset

Palvelun kautta on mahdollista allekirjoittaa asiakirjoja sähköisesti. Tarjolla on kaksi tunnistautumistapaa; tunnistautuminen Viilu-tunnuksella tai vahva tunnistautuminen. Käytämme vahvaan tunnistautumiseen tunnistusvälityspalvelua. Tallennamme tietokantaan allekirjoitusten tilan, mutta emme koskaan henkilötunnusta tai muuta vastaavaa arkaluontoista tietoa.

Keskustelut

Palvelun kautta on mahdollista viestitellä ja keskustella, mikäli tämä ominaisuus on otettu osaksi palvelukokonaisuutta. Viestikanavien ja viestien näkyvyyttä voidaan hallinnoida

käyttöoikeustasojen perusteella. Keskustelut ovat nähtävissä vain tunnistautuneille käyttäjille, joille on annettu käyttöoikeus.

Tiedotteet

Palvelun kautta on mahdollista lähettää erinäisiä tiedotteita, mikäli tämä ominaisuus on otettu osaksi palvelukokonaisuutta. Tiedotteiden näkyvyyttä voidaan hallinnoida käyttöoikeustasojen perusteella. Tiedotteet ovat nähtävissä vain tunnistautuneille käyttäjille, joille on annettu käyttöoikeus.

Asiakaskäyttöliittymän tietoturva

Yhteyksien salaus

Kaikki palvelussa tapahtuva asiointi tapahtuu TLS-tekniikalla salattua HTTPS-yhteyttä pitkin riippumatta siitä käytetäänkö web-käyttöliittymää tai sovelluksia. Kaikki palvelussa oleva tieto siirretään salattua yhteyttä pitkin, eikä palvelua ole mahdollista käyttää ilman salausta.

Palvelun ja kaikkien Viilun sivustojen salaus perustuu 2048-bittisellä RSA-avaimella luotuihin varmenteisiin. Varmenteen avulla selainohjelmat ja sovellukset varmentavat että salattu yhteys muodostetaan Viilun aitoihin palvelimiin. Mahdollisessa hyökkäystilanteessa selainohjelma estää palveluun pääsyn ja varoittaa viallisesta sertifikaatista. Sovellukset eivät suostu etenemään viallisen sertifikaatin kanssa.

Kaikki video ja ääniyhteydet ovat salattuja. On myös mahdollista asettaa päälle end-to-end salaus, jolloin video- ja äänipaketteja ei pureta edes Viilun palvelimilla. Tämä vaatii jaetun salausavaimen käyttöä.

Kahden laitteen välinen kokous hyödyntää mahdollisuuksien mukaan P2P teknologioita. Näin video- ja kuvayhteyden ohittavat Viilun palvelimet kokonaan ja yhteys muodostetaan vain näiden kahden laitteen välille.

Huijaus-yrityksiltä suojautuminen

Ulkopuoliset hyökkääjät saattavat yrittää tuottaa harhautus-sivustoja, jotka näyttävät Viilun hallinnoimilta, mutta eivät tätä tosiasiallisesti ole. Suosittelemme asiakkaitamme olemaan aina valppaina verkkotunnuksen suhteen. Käytämme aina vii.lu verkkotunnusta tai sen alitunnuksia, kuten app.vii.lu.

Jotkin selainlisäosat saattavat muokata verkkosivujen ulkoasua tai sisältöä. Suosittelemme asiakkaitamme olemaan tietoisia selaimensa lisäosista ja niiden luottamuksen tasosta. Asennetuilla lisäosilla on aina täysi pääsy vierailemillesi verkkosivuille. Viilu ei koskaan esitä mainoksia varkkosivuillaan tai palvelussaan.

Emme ole vielä saaneet tietoomme yhtään huijausyritystä, mutta kehotamme asiakkaita olemaan aina valppaana ja raportoimaan epäilyksistään meille.

Näkymien jaottelu asiakasryhmittäin

Palvelu on pääasiallisesti jaoteltu kahteen osaan; Talosivut ja Isännöintinäkymä. Talosivut sisältävät kaiken yksittäiseen taloyhtiöön liittyvät tiedot ja toiminnallisuudet. Henkilöiden käyttöoikeuksia hallinnoidaan käyttäjänhallinnan kautta. Vastaavasti isännöintinäkymä sisältää kaiken isännöintitoimiston laajuiset tiedot ja toiminnallisuudet. Isännöintinäkymän näkee vain isännöintitoimiston henkilöstö. Henkilöstön käyttöoikeudet ovat hallinnoitavissa isännöintitoimiston Master-tasoisten tunnusten kautta.

Tiedostosynkronoinnin tietoturva

Tarjoamme isännöintitoimistoille erillispalveluna tiedostosynkronointisovellusta, joka asennetaan isännöintitoimiston henkilöstön työasemille. Työpöytäsovellus luo työasemalle Viilu-verkkolevyn, joka synkronoituu automaattisesti konfiguroitujen taloyhtiöiden talosivuille. Verkkolevyllä on myös mahdollista säilyttää isännöintitoimiston sisäisiä asiakirjoja jakamatta niitä taloyhtiöille.

Työpöytäsovellus synkronoi tiedostoja vain paikallisen “Viilu”-levyn ja palvelun välillä. Kaikki liikenne on salattua ja vaatii tunnistautumisen isännöintitoimiston henkilöstöltä.

Ohjelmistokehityksen tietoturva

Tietoturva huomioidaan läpi koko ohjelmistokehityksen elinkaaren.

Ohjelmistokehityksen tietoturvaperiaatteet

Kaikille Viilun ohjelmistokehittäjille pidetään seuraavat koulutukset sekä työsuhteen alussa että vuosittain:

1. Yrityksen tietoturvaohjeet ja -käytännöt
2. Tietosuoja ja henkilötietojen käsittely
3. Tietoturvallinen ohjelmistokehitys (OWASP)

Ennen tuotantoon siirtämistä jokaiselle ohjelmistokomponentille toteutetaan tietoturvakatselmointi. Tämän yhteydessä tehdään myös mahdolliset päivitykset tietosuojaselosteeseen.

Käytettyjen ohjelmistokomponenttien tietoturvallisuuden varmistaminen

Kaikista käytetyistä ohjelmistokomponenteista pidetään kirjaa olivat ne sitten sisäisiä tai kolmannen osapuolen komponentteja. Ennen uuden ohjelmistokomponentin käyttöönottoa tuotantoympäristössä sille tehdään tietoturvakatselmus. Mahdolliset avoimen lähdekoodin kirjastot katselmoidaan havoittuvuuksien varalta. Uuden komponentin käyttöönotto vaatii vähintään kahden kehittäjän hyväksynnän.

Käytettyjen kolmannen osapuolen komponenttien ja palveluiden tietoturvatiedotteita seurataan aktiivisesti.

Lähdekoodin suojaus

Kaikki lähdekoodi säilytettään GIT-versionhallintajärjestelmässä. Kaikista muutoksista ja muokkaajista jää pysyvä merkintä versiohistoriaan. Kaikki muutokset vaativat vähintään yhden toisen kehittäjän hyväksynnän.

Pääsy versionhallintaan ja siten lähdekoodiin on suojattu henkilökohtaisilla käyttäjätunnuksilla, joissa on kaksivaiheinen tunnistus käytössä.

Lähdekoodia ei saa ladata tai lähettää laittelle, jotka eivät ole Viilu Solutions Oy:n hallinnoimia.

Lähdekoodin ja konfiguraation tietoturvakatselmukset

Jokainen muutos lähdekoodiin vaatii katselmuksen vähintään yhdeltä toiselta kehittäjältä. Tuotantoympäristöön viemisen edellytyksenä on myös tietoturvakatselmointi tietoturvavastaavan toimesta.

Konfiguraatiolla ei kontrolloida tietoturvaan liittyviä seikkoja. Konfiguraatiomuutokset vaativat vähintään yhden toisen kehittäjän hyäksymisen ja näistä jää aina auditoitava jälki.

Palvelun testaus

Palvelua testataan kehityksen aikana sekä ennen uuden tuotantoversion julkaisemista sekä manuaalisilla että automatisoiduilla testitapauksilla. Tuotantoympäristöön ei voida viedä lähdekoodia, joka ei läpäise kaikkia testejä.

Käyttöoikeudet

Taloyhtiön asukkaiden, osakkaiden ja hallitusten käyttöoikeudet

Pääsyä taloyhtiökohtaiseen tietooj ja toiminnallisuuksiin hallinnoidaan kohteen talosivujen käyttäjänhallinnan kautta. Henkilöitä voidaan kutsua käyttäjiksi ja asettaa heille roolit, joiden kautta he saavat luku ja/tai kirjoitusoikeudet erinäisiin tietoihin ja toiminnallisuuksiin.

Käyttäjänhallintaa voidaan hyödyntää vaikka käytettäisiin vain osaa palvelusta. Esimerkiksi isännöintitoimisto, joka käyttää vain Viilun kokouspalveluita voi silti kutsua taloyhtiön hallituksen jäsenet palveluun, jolloin he pystyvät hyödyntämään kokoustyökaluja täysin.

Kokouskohtaisesti voidaan määritellä vaatiiko kokoukseen osallistuminen tunnistautumista vai ei. Tunnistautumattomilla käyttäjillä on rajalliset käyttöoikeudet vain kyseiseen kokoukseen, johon heidät on kutsuttu.

Isännöintitoimiston henkilöstön käyttöoikeudet

Isännöintitoimiston henkilöstö saa automaattisesti käyttöoikeudet kaikkien isännöimiensä taloyhtiöiden talosivuille. Isännöitsijän tunnukset vastaavat käyttöoikeuksiltaan hallituslaisen tunnuksia, mutta sallivat myös isännöintitoimiston tietojen hyödyntämisen, kuten kokouksen esityslistan lataamisen isännöintitoimiston tallennetusta pohjasta.

Isännöintitoimiston henkilöstön käyttöoikeudet jaetaan kahteen ryhmään; Isännöitsijät ja Masterit. Isännöitsijät pystyvät hallinnoimaan isännöimiään taloyhtiöitä palvelun kautta. Master-roolin omaava tunnus pystyy tämän lisäksi muokkaamaan isännöintitoimiston henkilöstöä ja toimistokohtaisia asetuksia.

Viilun henkilöstön käyttöoikeudet

Oletusarvoisesti Viilun henkilöstöllä ei ole pääsyä asiakkaiden tietoihin, kuten asiakirjoihin tai talosivuille. Asiakkaan pyynnöstä asiakaspalvelu voi ottaa oikeudet käyttöön palvellakseen asiakasta. Tästä jää aina jälki lokitiedostoihin.

Kehittäjille myönnetään luku ja/tai kirjoitusoikeuksia tuotantoympäristöön tapauskohtaisesti ja mahdollisimman rajatusti, mikäli heillä on työtehtäviensä suorittamisen vuosi tarve saada väliaikainen käyttöoikeus.

Fyysinen tietoturva

Tietotekniset laitteet

Viilun tarjoamat tietotekniset laitteet on konfiguroitu käyttämään ajantasaista virustorjuntaa. Laitteita saa käyttää vain työkäyttöön, eikä laitteille saa asentaa työhön liittymättömiä ohjelmistoja. Laitteet ovat keskitetysti hallinnoitavissa.

Toimitilojen tietoturva

Viilun toimitiloissa on kulunvalvonta ja käytössä henkilökohtaiset avainkortit. Toimitiloissa ei säilytetä palvelimia tai laitteita, jotka olisivat yhteydessä tuotantoympäristöön.

Fyysiset rekisterit

Viilu ei ylläpidä fyysisiä rekistereitä.

Käyttäjän manipulaatio (social engineering)

Viilun työntekijöille pidetään työsuhteen alussa koulutus sekä fyysisestä tietoturvasta, että manipulaatioyrityksien tunnistamisesta.

Infrastruktuurin tietoturva

Konesalin sijainti ja palveluntarjoaja

Palvelun tuottamiseen käytämme seuraavia konesalipalveluntarjoajia:

Nimi	**Osoite**	**Konesalien sijainti**	**Alihankkijat**
Google Cloud, Google Ireland	Gordon House Barrow Street Dublin 4, Ireland	Suomi, Belgia	https://cloud.google.com/terms/subprocessors

Kaikissa konesaleissa on kahdennetut palvelinlaitteet ja automaattinen valvonta seuraa palveluiden saatavuutta jatkuvasti.

Konesaleissa on ympärivuorokautinen päivystys, elektroninen kulunvalvonta, kahdennettu jäähdytys, Internet-yhteys ja sähkönsyöttö.

Kaikki käytetyt palvelinkeskukset sijaitsevat EU-alueella.
Kaikkien konesalipalveluiden tietoturva on ISO 27001 -sertifioitu.

Tuotantoympäristön tietoturva

Kaikki tuotantoympäristön palvelinympäristöt ovat Googlen hallinnoimia (managed). Ostamme Googlelta palveluna tietoturvalliset, kovennetut ympäristöt, joka sisältää esimerkiksi:

- Tietoturvapäivitykset asennetaan automaattisesti päivittäin
- Virtuaalikoneilla ei ole ajossa mitään muuta koodia/palveluita lähdekoodimme lisäksi
- Palvelimet ovat täysin Google-managed, eli tuotantoympäristöön ei ole olemassa SSH avaimia tai muita tunnuksia, jolla me tai ulkopuolinen tunkeutuja pääsisi tuotantopalvelimiin käsiksi.

Suojaus haittaohjelmilta

Palvelun lähdekoodi ja ulkopuoliset riippuvuudet tarkistetaan ajantasaisen virustorjuntaohjelmiston avulla ennen tuotantoon siirtymistä.

Tällä hetkellä asiakkaiden asiakirjoille ei tehdä mitään operaatioita, kuten virustorjuntaa.

Ohjelmistojen haavoittuvuuksien ja tietoturvariskien hallinnointi

Kaikki pelvelimet ovat Googlen hallinnoimia ja tietoturvapäivitykset asennetaan automaattiseti päivittäin.

Palvelun ylläpito ja kehitystiimi seuraavat jatkuvasti haavoittuvuustiedotteita. Kaikki käytössä olevat ohjelmistokomponentit ja palveluntarjoajat on luetteloitu, joka mahdollistaa haavoittuvuuden nopean tunnistamisen. Haavoittuvuuden löytyessä käynnistetään tietoturvapoikkeamaprosessi ja ryhdytään välittämiin toimenpiteisiin.

Lokitiedostot

Palvelun lokitiedostot ja kolmannen osapuolen riippuvuuksien lokitiedostot kerätään keskitetyyn paikkaan, josta lokitiedostoja on mahdollista auditoida. Lokitiedostot ovat saatavilla vaikka alkuperäinen palvelin ei olisikaan saatavilla.

Palvelinyhteyksien salaus

Kaikki asiakkaan ja palvelun palvelimien välinen tietoliikenne on salattu perustuen 2048-bittisellä RSA-avaimella luotuihin varmenteisiin. Myös kaikki Viilun palvelimien välinen tietoliikenne on salattua.

Asiakirjojen salaus

Palveluun tallennetut asiakirjat tallennetaan Google Cloud Storage-palveluun. Tiedostot tallennetaan Suomessa sijaitsevaan Googlen palvelinkeskukseen. Ennen tallennusta levylle Google salaa tiedoston käyttäen AES-256 salausalgoritmia ja Googlen hallinnoimaa tiedostokohtaista salausavainta. Kun tiedosto poistetaan, myös tiedostokohtainen salausavain poistetaan.

Kaikki asiakirjojen siirtämiseen käytetyt yhteydet ovat salattuja.

Varmuuskopiot

Kaikesta palvelun sisällöstä otetaan varmuuskopiot päivittäin.

Sekä taloyhtiökohtaiset että isännöinnin asiakirjat varmuuskopioidan päivittäin. Asiakirjat ovat katastrofitilanteessa palautettavissa vaikka joku olisikin vahingossa poistanut kaikki asiakirjat.

Viestinnän tietoturva

Sähköposti-ilmoitukset

Palvelu lähettää käyttäjille häntä koskettavista asioista ilmoituksia sähköpostitse. Käyttäjä voi myös poistaa sähköposti-ilmoitukset käytöstä.

Sähköpostit lähetetään käyttäen TLS-salattua yhteyttä, mikäli vastaanottajan sähköpostipalvelin tukee TLS-salausta. Emme kuitenkaan voi tietää tukeeko vastaanottajan sähköpostipalvelin TLS-salausta, joten emme voi taata, että kaikki viestit lähetetään salattua yhteyttä pitkin.

Sähköpostissa ei välitetä luottamuksellisia tietoja, vaan tiedot/asiakirjat ovat saatavilla palvelusta vasta tunnistautumisen jälkeen, ellei tietoja/asiakirjoja ole säädetty avattavaksi ilman tunnistautumista.

Palvelun lähettämät sähköpostit hyödyntävät SPF- ja DKIM-tietueita. Näiden avulla vastaanottajan sähköpostiohjelma voi varmistua siitä, että lähettäjä on tosiasiassa Viilu. Mikäli tietueet eivät täsmää vastaanottajan sähköpostiohjelmisto tiedottaa vastaanottajalle, että sähköposti saattaa olla väärennetty. On kuitenkin aina tärkeä varmistaa, että sähköpostin linkit osoittavat vii.lu verkkotunnukseen, jotta ei vahingossa ohjauduta hyökkääjän harhautus-sivulle.

Kolmannet osapuolet

Käytämme palvelun tuottamiseksi joitakin kolmannen osapuolten palveluita. Näihin lukeutuvat erinäiset viestioperaattorit ja tunnistautumisvälittäjät.

Tarkastamme aina kumppaniemme tietoturvan tason ja seuraamme sen kehitystä.

Analytiikan tietoturva

Käytämme verkkosivuillamme ja palvelussa analytiikkatyökaluja, joiden kautta saamme anonyymiä käyttödataa. Voimme käyttää tätä dataa palvelun kehittämiseen. Analytiikkadataa ei voi henkilöidä käyttäjään. Analytiikkadatan säilytysajan löydät tietosuojaselosteestamme.

Käytämme automaattiseen virheraportointiin kolmannen osapuolen palvelua. Virheraportti syntyy automaattisesti mikäli palvelu tai sovellus kaatuu käytössä kriittiseen virheeseen. Virheraportti sisältää yksilöivän tunnisteen, jonka ylläpitomme voi yhdistää henkilön käyttäjäprofiiliin. Tämän avulla voimme ottaa käyttäjään yhteyttä ja auttaa ratkaisemaan ongelman, joka heillä ilmeni.

Palvelun jatkuvuuden hallinta

Käytämme palvelun tuottamiseen ensisijaisesti Suomessa sijaitsevaa Googlen konesalia. Palvelinkeskus on jaettu vyöhykkeisiin, joissa on erillinen infrastruktuuri. Tämä tarkoittaa sitä, että palvelumme pysyvät käytettävissä vaikka konesalissa olisi isompaakin ongelmaa. Katastrofitilanteessa, jossa koko konesali häviää kartalta voimme siirtää palvelumme toiseen Googlen EU:n konesaliin muutamassa tunnissa.

Työntekijöiden roolit on määritelty ja jaettu siten, että mikään yrityksen toiminto ei ole riippuvainen yksittäisestä työntekijästä. Pyydämme ilmoittamaan palvelussa olevista ongelmista ensisijaisesti sähköpostitse osoitteeseen asiakaspalvelu@vii.lu, jolloin pyyntö välittyy tukijärjestelmän kautta työvuorossa oleville henkilöille.

Mitkään henkilöstön tehtävät eivät ole sidottuja yrityksen toimitiloihin, jolloin toimintaa voidaan jatkaa vaikka toimitilat eivät poikkeustilanteen takia ole käytettävissä. Koko henkilöstöllä on valmius suorittaa kaikki työtehtävät tarvittaessa toisesta toimistotiloista tai kotoa etätyöskentelynä.

Palvelun mahdollisista häiriötilanteista julkaistaan tietoa osoitteessa https://status.vii.lu. Sivuston kautta häiriö- ja huoltotiedotteet voi tilata itselleen sähköpostilla.