Lyytin tietoturva

Tietoturvan korkean tason ylläpitäminen on tärkein prioriteettimme. Kun uskot tapahtumatietosi Lyytiin, voit olla varma sen turvallisuudesta. Olemme 100-prosenttisesti sitoutuneet noudattamaan tiukkoja turvallisuusstandardeja useiden suojakerrosten avulla.

Lyytin avulla sinulla on kaikki tarvittavat työkalut osallistujatietojen turvalliseen hallintaan.

Lyytin tietoturvan hallintajärjestelmä (ISMS) on ISO/IEC 27001 -standardin mukainen ja sisältää kattavan valikoiman turvatoimia. Näihin toimenpiteisiin kuuluvat tarkastukset, käytännöt, ohjeet, suunnitelmat ja menettelyt, jotka kaikki on suunniteltu turvaamaan toimintamme kaikki osa-alueet.

Lyyti käsittelee tietoja yksinomaan EU:n alueella noudattaen tarkasti GDPR:ää (2016/679). Lyytin tilat on suunniteltu ja varusteltu tiukkoja turvallisuusmääräyksiä noudattaen. Toimintatiimi valvoo jatkuvasti Lyytin toimivuutta. Ryhmä palvelee 24/7, vuoden jokaisena päivänä.
Seuraamme jatkuvasti Lyyti-ympäristöjä tunnistaaksemme ja korjataksemme mahdolliset haavoittuvuudet ripeästi.

Kaikki Lyytin aliprosessorit on valittu huolellisesti täyttämään tiukat turvallisuusstandardimme. Jokainen alikäsittelijä auditoidaan vuosittain vaatimustenmukaisuuden varmistamiseksi, ja luettelo kumppaneista on saatavilla Lyytin verkkosivuilla.
Lyytin varmuuskopiointijärjestelmä on vankka, ja se sisältää neljä erillistä toimintatasoa, jotka on maantieteellisesti erotettu turvallisuuden parantamiseksi.

Henkilöstön turvallisuusohjelmamme velvoittaa kaikki työntekijät suorittamaan vuosittaisen tietoturva- ja tietosuojakoulutuksen, mikä varmistaa, että tiimimme on hyvin perehtynyt korkeimpien tietoturvastandardien ylläpitämiseen.

Lyytin Tietoturvaohjelma

Lyytin tietoturvaohjelma kattaa yrityksen toiminnan kaikki alueet. Tietoturvan hallinnalla suojataan Lyytin ydinarvot, kuten henkilöstö, tiedot, maine, omaisuus, resurssit ja ympäristö. Lyytin tietoturvan tavoite on parantaa yrityksen kilpailukykyä varmistamalla kaiken käsitellyn tiedon luottamuksellisuus, eheys sekä saatavuus, kaikissa tiedon käsittelyn eri vaiheissa.

Lyytin tietoturvan hallintajärjestelmä (ISMS)

Lyytin tietoturvan hallintajärjestelmä (ISMS) pohjautuu ISO/IEC 27001 -standardiin ja se sisältää erilaisia tietoturvan hallinnan toimenpiteitä. Näihin sisältyy esim. hallintakeinot, politiikat, ohjeet, suunnitelmat ja parhaat käytännöt, ja ne on suunniteltu turvaamaan toimintamme kaikki osa-alueet.

Fyysinen turvallisuus

Lyytin toimisto on varustettu elektronisilla lukitusjärjestelmällä, kameravalvonnalla sekä moderneilla murtohälytysjärjestelmillä. Ulkopuolinen turvapalveluyritys valvoo tiloja ympäri vuorokauden, vuoden jokaisena päivänä. Jokaisella työntekijällä on henkilökohtainen elektroninen avain ja kaikki kulkutapahtumat kirjataan ja niitä voidaan tarvittaessa tutkia.

Lyytin hosting-palveluntarjoaja noudattaa useita alan tunnettuja turvallisuusstandardeja, kuten ISO 9001, SOC 1 Type II, SOC 2 Type II, ISO 27001, ISO 22301 sekä PCI-DSS. Palveluntarjoajan kaikki voimassa olevat sertifikaatit löytyvät osoitteesta: https://upcloud.com/data-centres.

Tietojen luokittelu

Lyyti käyttää kolmiportaista tietojen luokittelumallia. Kriteerit tietojen luokittelulle sekä tietojen käsittelyohjeet jokaiselle tasolle on kuvattu politiikoissa. Työntekijöille annetaan säännöllistä koulutusta näistä menettelyistä oikean tietojen käsittelyn varmistamiseksi.

Päätelaitteiden turvallisuus

Kaikki yrityksen tietoja käsittelevät laitteet ovat yrityksen omistamia, ja ne on kovennettu dokumentoidusti. Laitteet on suojattu erilaisia hyökkäyksiä vastaan ympäri vuorokauden

valvotulla XDR-ratkaisulla. Päätelaitteiden hallintaan käytetään MDM-ratkaisua, jolla varmistetaan että kaikki laitteet ovat vaatimustenmukaisia ja salattuja. Käyttäjien on ilmoitettava kaikista laitteiden käytön aikana havaitsemistaan poikkeavuuksista.

Lyytin Acceptance Use Policy määrittelee yrityksen IT-resurssien ja yrityksen omistamien laitteiden käytön säännöt sekä menettelyt sääntöjen mahdollisissa laiminlyönneissä.

Turvallisuuskoulutukset

Uusien työntekijöiden on suoritettava tietoturva- ja tietosuojakoulutus sekä läpäistävä siihen liittyvä testi ensimmäisenä työpäivänään. Koulutusten sisältöä päivitetään säännöllisesti ja ne suoritetaan jatkossa vähintään vuosittain. Koulutusten suorittamista valvotaan.

Ohjelmistokehittäjät koulutetaan vähintään vuosittain lisäksi turvallisen ohjelmistokehityksen parhaisiin käytäntöihin.

Salauskäytännöt

Kaikki yrityksen omistamat laitteet on salattu. Asiakkaiden tiedot käsitellään aina salatussa muodossa, sekä lepotilassa (at rest) että siirron aikana (in transit).

Lyytin tietoturvavastuut

Kaikki Lyytin tietoturvaan liittyvät keskeiset roolit ja sijaiset on kuvattu yrityksen sisäisessä dokumentinhallintajärjestelmässä. Yrityksen viestintäkanavat sisältävät vastuuhenkilöiden yhteystiedot.

Tietoturvapolitiikat

Lyytin tietoturvadokumentaatio koostuu useista hallituista politiikkadokumenteista ja ohjeista, joilla jokaisella on vastuuhenkilö. Dokumentit katselmoidaan vuosittain tai aina, kun sisältöön tehdään muuten merkittäviä muutoksia. Näin varmistaan, että politiikat ja ohjeet pysyvät ajan tasalla ja ovat linjassa organisaation tavoitteiden, päämäärien sekä lakisääteisten vaatimusten kanssa.

Tietomurrot ja häiriönhallinta

Lyyti ylläpitää dokumentoitua järjestelmää tietoturvaloukkausten valvontaan ja hallintaan. Työntekijöiden on viipymättä ilmoitettava havaitsemistaan tai epäilemistään tietoturvapolitiikan rikkomuksista, murtoyrityksistä, tietomurroista, laitteiden varkaudesta tai katoamisesta sekä muista tietoturvaan liittyvistä poikkeamista.

Lyytin häiriönhallinnan dokumentaatiot tarkastetaan vuosittain ja se on kaikkien työntekijöiden saatavilla. Dokumentaatio sisältää kommunikointiohjeet ja korostaa nopean reagoinnin merkitystä Lyytin palveluiden ja tietojen suojaamiseksi.

Riskienhallinta

Riskienhallinta on olennainen osa Lyytin toimintaa. Se auttaa yritystä saavuttamaan tavoitteensa varmistamalla, että riskit ovat suhteessa riskien sietokykyyn.

Lyyti ylläpitää riskirekisteriä tunnistetuista riskeistä. Riskit on luokiteltu ja analysoitu, ja niille laaditaan vuosittain toimintasuunnitelmat niiden hallitsemiseksi. Riskienhallintapolitiikan ja riskien arvioinnin laadinnasta vastaa CTO yhdessä CEO:n ja yrityksen Compliance-tiimin kanssa. Johtoryhmä hyväksyy riskienhallintapolitiikan ja tarkistaa prosessin vuosittain.

Jatkuvuussuunnittelu

Lyytillä on liiketoiminnan jatkuvuussuunnitelma (BCP), jota tukee kattavat palautussuunnitelmat (DRP). Näiden avulla varmistetaan kriittisten toimintojen jatkuvuus kriisitilanteen aikana ja sen jälkeen. Palautumissuunnitelman ensisijainen tavoite on minimoida järjestelmän käyttökatkot ja tietojen häviäminen. Dokumentteja tarkastellaan säännöllisesti niiden ajantasaisuuden varmistamiseksi.

Haavoittuvuuksien hallinta ja valvonta

Lyytin IT-infrastruktuuria valvotaan ympäri vuorokauden, mukaan lukien pilvipalvelut, verkot , päätelaitteet sekä toimistotilat. Kaikki havaitut poikkeamat luokitellaan, dokumentoidaan ja käsitellään olemassaolevien politiikkojen ja ohjeiden mukaisesti.

Ympäristöt skannataan haavoittuvuuksien varalta, järjestelmästä riippuen, joko reaaliaikaisesti, päivittäin tai viikoittain.

Penetraatiotestaukset

Riippumaton ulkopuolinen yritys suorittaa järjestelmän penetraatiotestauksen vähintään kerran vuodessa. Kaikki havainnot dokumentoidaan ja käsitellään asianmukaisesti.

Viimeisin penetraatiotestaus on suoritettu 03/2024. Fraktalin yhteenveto testistä.

Päivitysprosessit

Lyytin tuotantojärjestelmiä valvotaan jatkuvasti mahdollisten haavoittuvuuksien varalta. CVSS v3.0-luokitusjärjestelmän mukaan "kriittisiksi" tai "korkeiksi" luokitellut haavoittuvuudet paikataan välittömästi, ja "keskitasoiset" ja sitä matalammat haavoittuvuudet korjataan kuukauden kuluessa päivityksen julkaisusta.

Työntekijöiden ja alihankkijoiden turvallisuuskäytännöt

Lyyti on sitoutunut noudattamaan parhaita tietoturvakäytäntöjä, sisältäen myös työntekijöiden ja alihankkijoiden rekrytointi- ja perehdytysprosessit. Rekrytoimme ainoastaan luotettavia ja vastuullisia työntekijöitä, ja kaikki sopimukset sisältävät myös salassapitolausekkeen.

Tietoturvan varmistamiseksi henkilöstö ja alihankkijat käyvät läpi koulutuksen ja suorittavat testit ennen käyttöoikeuksien myöntämistä. Pääsyoikeuksia tarkastellaan työnkuvien mukaan, jolla varmistetaan vain välttämätön pääsy yrityksen tietoihin.

Työntekijän offboarding

Työntekijän työsuhteen päättyessä, noudatetaan dokumentoitua yksityiskohtaista offboarding-prosessia, jolla varmistetaan mm. käyttäjätilien lopettaminen ja yrityksen omistamien IT-laitteiden palautuminen. Kaikki Lyytin omistamat IT-laitteet on kirjattu omaisuusrekisteriin ja niitä hallinnoidaan dokumentoitujen käytäntöjen mukaisesti.

Datan sijainti ja alikäsittely

Kaikki Lyytin käsittelemä tieto, mukaanlukien alihankintakäsittely, käsitellään ainoastaan EU-alueella. Lista Lyytin käyttämistä alihankkijoista löytyy osoitteesta https://www.lyyti.com/en/subprocessors, ja kaikki alihankkijat arvioidaan vuosittain osana Lyytin riskienhallintaprosesseja.