liana

Tietoturvaohjeistus

Sisältö

Johdanto

Liana Technologies yrityksenä

Liana Technologies on eurooppalainen ohjelmistoyritys, joka on perustettu vuonna 2005. Olemme erikoistuneet digitaalisen markkinoinnin ja viestinnän ohjelmistoihin. Liana Technologiesin markkinointiteknologiaa käyttää yli 3 500 asiakasta maailmanlaajuisesti, mukaan lukien yritykset kuten Hertz, Toyota, Ikea ja Starbucks. Missiomme on auttaa asiakkaitamme saavuttamaan tavoitteensa ja saamaan tuloksia markkinointi- ja PR-teknologiamme avulla. Tavoitteenamme on kasvaa Pohjoismaiden suurimmaksi markkinointiteknologian tarjoajaksi.

Dokumentin tarkoitus

Tämän Tietoturvaohjeistuksen tarkoituksena on tarjota asiakkaillemme kattava kuva siitä, miten me Lianalla lähestymme ja toteutamme tietoturvatoimenpiteitä kaikissa digitaalisen markkinoinnin ja viestinnän tuotteissamme. Haluamme osoittaa olevamme sitoutuneita asiakkaidemme tietojen luottamuksellisuuden, eheyden ja saatavuuden säilyttämiseen kaikissa Lianan palveluissa.

Tämän dokumentin avulla pyrimme:

- Avaamaan tietoturvallisuuskäytäntöjämme: Kerromme yksityiskohtaisesti lähestymistapamme tietoturvaan, mukaan lukien käytännöt, menettelyt ja kehykset, joita käytetään arkaluonteisten tietojen suojaamiseen.
- Vakuuttamaan vaatimustenmukaisuudesta ja standardeista: Korostamme sitoutumistamme alan standardeihin, lakisääteisiin vaatimuksiin ja sertifiointeihin edistääksemme asiakkaidemme luottamusta.
- Helpottaa asiakkaiden päätöksentekoa: Tarjoamme arvokasta tietoa asiakkaillemme, jotta he voivat arvioida käytössä olevia tietoturvatoimenpiteitä ja tehdä tietoon perustuvia päätöksiä yhteistyöstä Lianan kanssa.
- Helpottamaan yhteistyötä: Jakamalla tietoturvallisuusperiaatteitamme haluamme luoda luottamuksen ja yhteistyön ilmapiirin.

Tämä dokumentti korostaa sitoutumisemme tietoturvaan ja toimii referenssinä asiakkaillemme, jotka haluavat varmistua palveluihimme sisällytetyistä suojaustoimenpiteistä. Asiakkaidemme suojaamiseksi emme julkaise matalan tason turvallisuusmäärityksiä.

Liana pidättää oikeuden päivittää tätä Tietoturvaohjeistusta ja voi tehdä siihen muutoksia tarvittaessa.

Kehittäjädokumentaatio

Työntekijämme ovat tietoturvan ytimessä. Koska keskitymme SaaS-ohjelmistojen kehittämiseen ja ylläpitoon, kiinnitämme erityistä huomiota järjestelmien turvallisuuteen. Ohjelmistokehitysala kehittyy todella nopeasti. Jotta kehitystiimimme keskittyisivät oikeisiin asioihin, ylläpidämme Lianan DevOps-käsikirjaa, joka sisältää ajantasaiset ohjeet, erityisesti tietoturvallisuusnäkökohdat. Käsikirja sisältää tietoa esimerkiksi:

- Hyväksytyt turvallisuuskäytännöt / sovelluskehityksen kohdealueet
- Tekninen perusta tuotteidemme turvallisuuden ja liiketoiminnan jatkuvuuden varmistamiseksi
- Elinkaaren lopun (EOL) toimenpiteet, joita seurataan

Vaatimustenmukaisuus ja tietoturvan hallinta

Lakisääteinen vaatimustenmukaisuus

Liana Technologiesissa asetamme etusijalle kaikkien sovellettavien lakien ja asetusten noudattamisen, jotka koskevat tietoturvaa, yksityisyyttä ja tiedonhallintaa. Sitoumuksemme ulottuu alueellisten, kansallisten ja kansainvälisten standardien noudattamisen varmistamiseen, asiakkaidemme tietojen suojaamiseen ja heidän luottamuksensa ylläpitämiseen.

Lähestymistapamme lakisääteiseen vaatimustenmukaisuuteen kattaa:

- Tietosuojasäännökset: Varmistamme yhdenmukaisuuden soveltuvien tietosuojasäännösten, kuten GDPR:n, CCPA:n ja muiden alueellisten säädösten kanssa.

- Yksityisyysstandardit: Toteutamme toimenpiteitä, jotka ovat yhdenmukaisia globaalien yksityisyysstandardien kanssa tietosuojan varmistamiseksi.

Seuraamme jatkuvasti kehittyvää lainsäädäntöä mukauttaaksemme käytäntöjämme ja menettelyjämme, jotta voimme varmistaa jatkuvan vaatimustenmukaisuuden uusien vaatimusten kanssa.

Tietoturvan hallintorakenne

Lianalla tietoturvan hallintamme perustuu vankkaan kolmikkoon, joka koostuu toimitusjohtajasta (CEO), teknologiajohtajasta (CTO) ja tietosuojavastaavasta (DPO). Tämä kolmikko muodostaa tietoturvallisuuspäätöksentekoprosessimme kulmakiven varmistaen kokonaisvaltaisen ja strategisen lähestymistavan tietoturvan hallintaan.

Tietoturvan hallintamme keskeisiä näkökohtia ovat:

- Johdon osallistuminen: Toimitusjohtajamme ja teknologiajohtajamme osallistuvat aktiivisesti tietoturvallisuusstrategioiden määrittelyyn ja valvontaan.

- Tietosuojavastaava (DPO) vastaa vaatimustenmukaisuuden valvonnasta, tietosuoja-aloitteiden ohjaamisesta ja yhdenmukaisuuden varmistamisesta lakisääteisten vaatimusten kanssa.

- Tietoturvatietoisuus ja -koulutus: Tavoittelemme säännöllisten koulutusten, työpajojen ja koulutusohjelmien avulla korkean tietoturvatietoisuuden ylläpitämistä työntekijöiden keskuudessa. Tämä varmistaa, että kaikilla työntekijöillä on tarvittava tieto ja taito edistää tietoturvaamme.

Hallintorakenteemme on suunniteltu edistämään tietoturvallisuustietoisuuden kulttuuria organisaation kaikilla tasoilla ja edistämään ennakoivia toimenpiteitä riskien lieventämiseksi ja asiakkaidemme tietojen eheyden ylläpitämiseksi. Tietoturvamme perustana on tietoturvahenkinen kulttuuri sekä kehitystiimeissä että koko organisaatiossa.

Standardit ja sertifioinnit

Liana on sitoutunut tarjoamaan turvallisen ympäristön asiakkaidensa datalle. Vaikka meillä ei ole vielä virallisia alan sertifiointeja, noudatamme johtavien sertifiointien, kuten ISO/IEC 27001, periaatteita ja käytäntöjä ympäristöjemme suojaamiseksi. Olemme käynnistäneet ISO 27001 sertifiointiprosessin

vuoden 2025 alusta. Tavoitteemme on saada sertifikaatti vuoden 2025 loppuun mennessä.

Pääsynhallinta

Vähimmäisoikeuksien periaate ja roolipohjainen käyttövaltuushallinta

Lianalla kaikkien järjestelmien ja tietojen käyttöoikeudet noudattavat vähimmäisoikeuksien periaatetta. Tämä periaate varmistaa, että henkilöillä on pääsy vain niihin tietoihin, jotka ovat tarpeen heidän rooliensa ja vastuualueidensa kannalta.

Roolipohjaiset käyttöoikeudet. Käyttöoikeudet myönnetään ennalta määriteltyjen roolien, kuten työroolien, perusteella.

Sitoutumisemme tiukkoihin pääsynhallintamekanismeihin varmistaa asiakkaidemme tietojen luottamuksellisuuden ja eheyden ja pienentää luvattoman pääsyn tai tietomurtojen riskiä.

Järjestelmien omistajuus ja hallinta

Jokaisella Lianan järjestelmällä, riippumatta siitä, onko se sisäisesti kehitetty järjestelmä vai kolmannen osapuolen palvelu, on Lianan nimeämä omistaja ja hallinnoija. Tämä lähestymistapa varmistaa vastuun ja valvonnan kunkin järjestelmän turvallisuuden ja toimivuuden osalta. Omistaja huolehtii, että hänen järjestelmäänsä käyttävät vain oikeutetut henkilöt.

Tuotantojärjestelmät ja tietojen käyttöoikeus. Pääsy tuotantojärjestelmiin, erityisesti asiakastietojen tallennuspaikkoihin, on rajoitettu nimetylle henkilöstölle, jolla on valtuudet käsitellä ja ylläpitää näitä järjestelmiä. Käyttöoikeuksia hallitaan tiukasti ja niitä tarkistetaan säännöllisesti turvallisuusprotokollien ja lakisääteisten vaatimusten noudattamisen varmistamiseksi. Tuotantotietoihin pääsyoikeuksien omaavien henkilöiden määrä pidetään mahdollisimman pienenä mahdollistaen järjestelmiemme luotettavan ylläpidon ja kehittämisen.

Tietosuoja

Tietojen eriyttäminen

Liana Technologiesissa noudatamme eriyttämisen periaatetta omien tietojemme (Lianan) ja asiakkaidemme tietojen välillä. Järjestelmämme on suunniteltu varmistamaan, että eri asiakkaiden tiedot on osastoitu eikä niitä sekoiteta. Tällä säilytämme kunkin asiakkaan tietojen yksityisyyden ja eheyden. Vaikka käytämme multi tenant -palveluita kaikille asiakkaillemme, ylläpidämme tietojen eristämistä estääksemme tietojen sekoittumisen eri asiakkaiden välillä.

Salaus liikenteessä ja levossa

Kaikki järjestelmissämme siirrettävät tiedot salataan, jotta tietojen luottamuksellisuus ja turvallisuus varmistetaan siirron aikana. Lisäksi kaikki varmuuskopiot, mukaan lukien pisteestä pisteeseen -varmuuskopiot, salataan, mikä suojaa varmuuskopioitujen tietojen eheyttä. Asiaankuuluvissa yhteyksissä tiedot salataan myös lepotilassa.

Jatkuvuuden varmistaminen

Lianan jatkuvuusriskien mitigointitoimenpiteet on räätälöity käytössä olevien järjestelmien arvon ja liiketoimintavaikutusten perusteella. Käytämme erilaisia menetelmiä pienentääksemme riskiä tietojen menetyksestä ja varmistaaksemme tietojen kestävyyden ja saatavuuden. Käytetyt toimet määritetään aina liiketoiminnan tarpeiden perusteella:

- Varmuuskopiot. Säännöllisiä varmuuskopioita (vähintään päivittäin) tehdään kaikista järjestelmistä tietojen menetyksen estämiseksi odottamattomien tapahtumien tai järjestelmävikojen sattuessa. Varmuuskopiot on fyysisesti eristetty muista järjestelmistä.

- Tietokantojen kerrostaminen. Tietokantojen monistaminen toimii lisäsuojakerroksena, joka parantaa redundanssia ja minimoi tietojen menetyksen riskiä.

- Jatkuva varmuuskopiointi. Joissakin tapauksissa teemme myös point in time -varmuuskopiointia tarkan palautuksen mahdollistamiseksi.

Näiden toimenpiteiden tarkoituksena on vahvistaa järjestelmissämme olevien tietojen turvallisuutta ja eheyttä varmistaen jatkuvan saatavuuden ja suojan mahdollisia tietojen menetystilanteita vastaan.

Monitorointi ja auditointi

Järjestelmän saatavuuden valvonta ja lokitus

Lianalla asetamme etusijalle järjestelmiemme jatkuvan saatavuuden. Käytämme seurantamekanismeja järjestelmän suorituskyvyn, saatavuuden ja turvallisuuteen liittyvien toimintojen seuraamiseen:

- Saatavuuden seuranta. Järjestelmiämme seurataan jatkuvasti korkean saatavuuden varmistamiseksi ja mahdollisten ongelmien nopeaksi tunnistamiseksi.

- Lokituskäytännöt. Lokitamme kaikki asiaankuuluvat toiminnot järjestelmissämme ylläpitääksemme tarkastusketjua ja tallentaaksemme tärkeitä tietoja analyysia ja turvallisuuspoikkeamien tutkimuksia varten. Emme kuitenkaan lokita mitään, joille meillä ei ole ennalta määriteltyä käyttötarkoitusta.

Lokien, metriikoiden ja hälytysten eristetty hallinta

Seurantakäytäntöjemme eheyden ylläpitämiseksi lokeja, metriikoita ja hälytyksiä hallinnoidaan järjestelmässä, joka on erillään niistä järjestelmistä, joita ne seuraavat. Tämä erottelu varmistaa, että seurantatiedot pysyvät turvallisina ja suojattuna tahallisilta muutoksilta. Kyseiseen järjestelmään on käyttöoikeudet rajatulla henkilöstöllä, ja järjestelmän tietovaraston muokkausoikeudet ovat rajatut.

Auditoinnit

Suoritamme säännöllisesti auditointeja, joissa arvioidaan järjestelmiämme, prosessejamme ja kontrollejamme. Auditoinneilla varmistamme vaatimustenmukaisuuden vakiintuneiden turvallisuusstandardien kanssa ja tunnistaaksemme kehityskohteita. Arvioimme auditointien kulloisenkin kohteen riskiperusteisesti.

Jatkuvuus ja palautuminen

Liana Technologiesissa sitoutumisemme tietoturvaan, lakisääteiseen vaatimustenmukaisuuteen, pääsynhallintaan, tietosuojaan, seurantaan ja tarkastukseen perustuu liiketoiminnan jatkuvuuden ja kriisitilanteista palautumisen kehykseen. Harjoittelemme säännöllisesti erilaisista kriisitilanteista palautumista.

Tuki ja Saatavuus

Pyrimme varmistamaan järjestelmiemme jatkuvan tuen ja saatavuuden päivystystiimin avulla. Päivystystiimi on nimetty vastaamaan kriittisten ongelmatilanteiden ratkaisemiseksi, tavoitteena varmistaa tehokas ratkaisu ja minimoida palvelun toimintaan kohdistuvat häiriöt.

Automatisoidut järjestelmäpäivitykset ja konfiguroinnit

Liiketoiminnan jatkuvuus varmistetaan automatisoitujen infrastruktuurien käyttöönotto- ja ohjelmiston käyttöönottoprosessiemme avulla. Nämä kehittyneet järjestelmät mahdollistavat ympäristöjen uudelleenrakentamisen kriittisten vikojen sattuessa.

Kriittisten vikojen sattuessa käyttöönottoprosessimme hyödyntävät tietoja fyysisesti eristetyistä varmuuskopioista. Nämä varmuuskopiot toimivat lähteenä, jonka avulla voimme palauttaa järjestelmät tehokkaasti.

Yhteenveto

Lianalla järjestelmiemme ja tietojesi turvallisuus ja eheys ovat ensiarvoisen tärkeitä. Tämä tietoturvaohjeistus edustaa sitoutumistamme läpinäkyvyyteen, vaatimustenmukaisuuteen ja ennakoiviin toimenpiteisiin asiakkaidemme tietojen suojaamiseksi.

Vaikka tämä dokumentti toimii yleiskatsauksena turvallisuuskäytännöistämme ja -protokollista, ymmärrämme räätälöityjen tietojen tärkeyden asiakkaillemme. Kannustamme tiedusteluihin lisätietoja, syvällisempää ymmärrystä tai selvennyksien saamiseksi mistä tahansa tässä ohjeistuksessa käsitellyn asian osalta.

Kiitos, että luotat Liana Technologiesiin liiketoimintatarpeidesi kanssa. Odotamme innolla yhteistyömme jatkamista pyrkimyksienne turvallisuuden ja menestyksen varmistamiseksi.