Fastroin tietopaketti - ISO 27001 -sertifikaatti

Julkaistu 29. huhtikuuta 2020

fastroi

Sisällysluettelo

Vastuuvapauslauseke

Tämän dokumentin tarkoituksena on esitellä ISO 27001 -standardin avainkäsitteet ja tarjota tietoa Fastroin asiakkaille, jotta he voivat tarkastella miten Fastroi toimii standardin vaatimusten mukaisesti.

Tämän dokumentin tietojen tarkoituksena ei ole korvata oikeudellista neuvontaa. Saadaksesi oikeudellista neuvontaa asemaasi tai velvollisuuksiisi liittyen, tulee sinun kääntyä lakimiehen puoleen.

Mikäli sinulla on tähän asiakirjaan (Fastroin ISO 27001 -tietopaketti) tai Fastroi Oy:n ISO 27001 -standardin vaatimusten mukaisuuteen liittyen kysyttävää, voit ottaa yhteyttä tietoturva- ja tietosuojatiimiin lähettämällä sähköpostia osoitteeseen privacy@fastroi.fi.

1 Fastroin ISO 27001 -sertifikaatti

Fastroi Oy:lle myönnettiin ISO 27001 -sertifikaatti marraskuussa 2019. Tämä tarkoittaa sitä, että Fastroin toiminta täyttää kansainvälisen tietoturvallisuuden standardin vaatimukset.

Fastroi yrityksenä ymmärtää tietoturvallisuuden ja yksityisyyden suojan olevan olennainen osa tietohallinnon parhaita käytäntöjä ja yrityksen toiminnan kulmakiviä.

Fastroille tietoturva ja yksityisyyden suoja ovat avainasemassa menestystekijöinä ja takaavat parhaan palvelutason asiakkaillemme. Fastroin tietoturvan hallintajärjestelmä (ISMS) on rakennettu täyttämään ISO 27001 -standardin vaatimukset:

- Riskienhallinta
- Omaisuuden hallinta
- Henkilöstöturvallisuus
- Pääsynhallinta ja fyysisten tilojen turvaaminen
- Ohjelmistokehitys ja ylläpito
- Tietoturva- ja tietosuoja poikkeamien hallinta
- Viestinnän hallinta
- Operatiivinen johtaminen
- Toimittajan tietoturvan hallinta
- Toiminnan jatkuvuuden hallinta
- Toiminnan jatkuvuuden suunnitelma
- Vaatimustenmukaisuus

Fastroi on määritellyt tietoturvapolitiikan mukaiset asiakirjat, jotka ovat pyynnöstä asiakkaidemme saatavilla.

Voit lukea lisätietoja matkastamme kohti sertifiointia blogistamme.

2 ISO 27001 -standardi ja -sertifikaatti

ISO 27001:2013 on tietoturvallisuuden hallintajärjestelmä -standardi, joka määrittelee tietoturvan parhaat käytännöt ja tietoturvan hallintakeinot parhaita käytäntöjä noudattaen. Standardi on laajalti tunnustettu kansainvälinen tietoturvastandardi, jota kohtaan Fastroin asiakkaat ovat osoittaneet kiinnostusta.

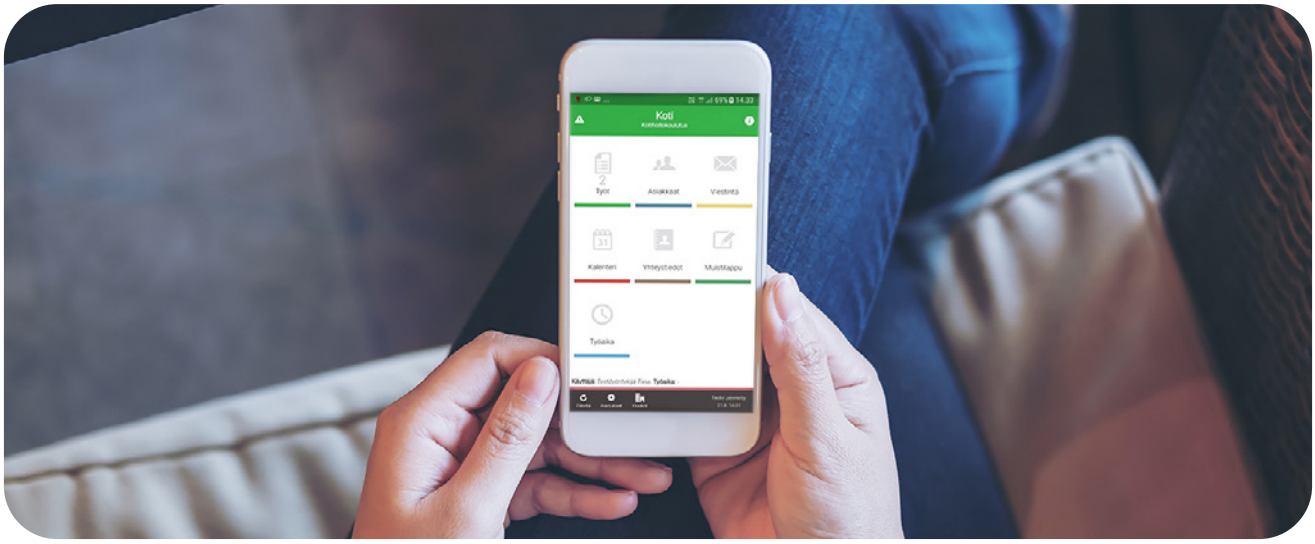
Standardi vaatii meitä jatkuvasti:

- Arvioimaan systemaattisesti tietoturvariskit huomioiden uhkien ja haavoittuvuuksien vaikutukset.
- Suunnittelemaan ja toteuttamaan kattavasti tietoturvan hallintakeinot ja muut riskienhallintatavat yrityksen ja sen arkkitehtuuria koskevien tietoturvariskien torjumiseksi.
- Laatimaan kattavan hallintaprosessin sen varmistamiseksi, että tietoturvan hallintakeinot vastaavat tietoturvatarpeisiimme.

Avain tämän standardin mukaiseen sertifiointiin oli ja on edelleen tiukka tietoturvallisuuden hallintaohjelma. Tämän standardin mukainen tietoturvan hallintajärjestelmä (ISMS) määrittelee kuinka hallitsemme jatkuvasti tietoturvaa kokonaisvaltaisella tavalla.

ISO 27001 -sertifikaatti on keskittynyt erityisesti tietoturvan hallintajärjestelmään (ISMS) ja se mittaa kuinka sisäiset prosessimme noudattavat ISO -standardia. DNV GL on riippumattomana tarkastajana suorittanut yrityksemme prosessien ja hallintakeinojen arvioinnin ja myöntänyt sertifioinnin sen merkiksi, että toimimme jatkuvasti yhdenmukaisesti ISO 27001 -standardin kanssa.

Toisin kuin aikaisemmissa ISO 27001 -standardin versioissa, vuoden 2013 versio täydentää liiketoimintakeskeistä lähestymistapaa korostamalla entistä enemmän johdon tukea tietoturvan hallintajärjestelmän (ISMS) osalta, riskienhallinnan merkitystä ja ISMS:n tehokkuuden parantamista.



3 Fastroin tietohallintajärjestelmän (ISMS) perusta

3.1 Tuoteturvallisuus

Meille on ensiarvoisen tärkeää varmistaa, että asiakkaillemme tarjoamamme ohjelmistotuotteet ovat turvallisia. Tämä tarkoittaa sitä, että ohjelmistotuotteidemme turvallisuudesta huolehtiminen ja ohjelmistotuotteiden sujuva käyttö ovat meille tärkeitä. Ohjelmistokehitysprosessin aikana suoritamme ohjelmistotuotteillemme sekä sisäistä että ulkoista testausta. Varmistaaksemme, että mitään ei jää huomioimatta sisäisen testauksen aikana, toteutamme sisäistä testausta useassa eri vaiheessa.

3.2 Tietosuoja

Fastroi on sitoutunut huolehtimaan käsittelemämme henkilötietojen ensiluokkaisesta tietosuojasta ja noudattamaan tietosuojalainsäädäntöä. Suojaamme tiedot työaseman ja kohteen välillä käyttämällä Transport Layer Security (TLS 1.2) -salausprotokollaa. Olemme myös toteuttaneet kattavan tietosuojaohjelman, josta voit lukea lisää GDPR-tietopaketistamme.

3.3 Fyysinen turvallisuus

Yrityksen tietovarat ja IT-omaisuus on suojattava riittävästi kaikissa käyttöolosuhteissa. Useasti tietoturva on fyysisen turvallisuuden osalta rakennettu vanhentuneille ratkaisuille. Ilman asianmukaisia yrityksen toimitilojen ja niissä sijaitsevien laitteiden suojaamista, yrityksen tietovarat voivat olla vaarassa. ISO 27001 asettaa fyysiselle turvallisuudelle hallintakeinot, joiden on täytettävä tietyt turvallisuusvaatimukset. Fastroin tilojen ja ympäristön osalta hallintakeinot on toteutettu riskienhallinnan määrittelemän tason mukaisesti.

4 Yleinen tietosuoja-asetus (GDPR) ja ISO 27001

Euroopan unionin yleinen tietosuoja-asetus (GDPR) tuli sovellettavaksi 25.5.2018 alkaen. Asetus toi uusia velvollisuuksia sekä rekisterinpitäjälle että tietojen käsittelijöille. Tietosuojaohjelmamme on toteutettu yleisen tietosuoja-asetuksen (GDPR) vaatimusten mukaisesti. Tietosuojalla ja ISO 27001 -standardilla on päällekkäisiä osa-alueita ja ISO 27001 -standardin noudattaminen auttoi meitä myös täyttämään yleisen tietosuoja-asetuksen vaatimuksia, joista osa on lueteltu alla.

4.1 Riskienhallinta

Yleisen tietosuoja-asetuksen noudattamatta jättäminen voi johtaa merkittäviin seuraamuksiin ja sakon suuruus voi tiettyjen rikkomusten kohdalla olla jopa 20 miljoonaa euroa tai 4 prosenttia yrityksen liikevaihdosta. Seuraamuksella on merkittävää taloudellista vaikutusta missä tahansa organisaatiossa. ISO 27001 -standardin mukaisesti tieto-omaisuuden osalta on tehtävä riskienarviointi, jossa on huomioitava myös henkilötietojen käsittelyyn liittyvät riskit ja niiden vaikutukset. Riskienarviointi suoritetaan määräajoin riskien tunnistamiseksi ja vaikutusten minimoimiseksi.

4.2 Yleisen tietosuoja-asetuksen noudattaminen

EU:n yleinen tietosuoja-asetus (GDPR) tuli voimaan 25.5.2018, johon mennessä organisaatioiden oli otettava huomioon tietosuoja-asetuksen vaatimukset. ISO 27001 -standardi edellyttää, että meillä on luettelo kaikista asiaan kuuluvista säädöksistä, määräyksistä ja sopimuksellisista vaatimuksista ja että noudatamme niitä.

4.3 Tietojen luokittelu

Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus. ISO 27001 vaatii meitä varmistamaan, että tietoja käsitellään aina tarvittavan suojaustason mukaisesti.

4.4 Tietosuojaloukkauksesta ilmoittaminen

Yleisen tietosuoja-asetuksen (GDPR) mukaisesti tietosuojaloukkauksesta on tehtävä ilmoitus valvontaviranomaisille mahdollisuuksien mukaan 72 tunnin kuluessa. ISO 27001 edellyttää toimivaa poikkeamien hallintaprosessia, jonka mukaisesti tietoturvaloukkauksesta on ilmoitettava mahdollisimman nopeasti sovittujen menettelytapojen mukaisesti.

4.5 Yhteistyö valvontaviranomaisten kanssa

Yleinen tietosuoja-asetus velvoittaa tietosuoja-asioissa yhteistyöhön valvontaviranomaisten kanssa. ISO 27001 edellyttää, että organisaatio pitää jatkuvasti yhteyttä asiankuuluviien viranomaisiin. ISO 27001 -sertifiointiprosessimme aikana vaatimus otettiin huomioon määriteltäessä organisaatiomme tietoturva- ja tietosuojavastaavien vastuita.

4.6 Omaisuuden hallinta

Yleinen tietosuoja-asetus vaatii yrityksiä kiinnittämään enemmän huomiota tietosuojaan. Asetuksen mukaisesti yrityksen on määriteltävä mitä henkilötietoja se käsittelee, miten henkilötiedot kerätään, miten ja kuinka kauan tietoja säilytetään sekä mitkä ovat henkilötietoja käsittelevien henkilöiden roolit. ISO 27001 -standardin mukaisesti meidän on tunnistettava organisaatiomme omaisuus ja määriteltävä asianmukaiset vastuut näiden suojaamiseksi. Fastroi on määritellyt yrityksen omaisuuserät ja luonut näille omaisuuserille hallinnointiprosessin.

4.7 Privacy by design

Yleinen tietosuoja-asetus asettaa velvollisuuden sisäänrakennetusta tietosuojasta (Privacy by design), mikä tarkoittaa sitä, että asetus edellyttää yksityisyyden suojan huomioon ottamista osana tuotteen tai palvelun kehitysprosessia. Olemme huomioineet sisäänrakennetun tietosuojan vaatimukset tuotteidemme kehitysprosessissa.

4.8 Toimittajat ja palveluntarjoajat

Yleinen tietosuoja-asetus koskee myös toimittajia ja palveluntarjoajia, jotka toimeksiannosta käsittelevät henkilötietoja. Toimittajan ja palveluntarjoajan kanssa on tehtävä sopimus henkilötietojen käsittelystä. ISO 27001 -standardin mukaisesti organisaation on suojattava omaisuus, johon toimittajalla tai palveluntarjoajalla on pääsy sekä valvottava tietoturvallisuuden toteutumista hankittavan palvelun osalta. Vaadimme toimittajiltamme ja palveluntarjoajiltamme, että heidän toimittamansa palvelut täyttävät tietoturvallisuuden vaatimukset.

4.9 Dokumentaatio

Yleinen tietosuoja-asetus edellyttää, että henkilötietojen käsittelyä koskeva dokumentointi ja sisäinen ohjeistus on kunnossa. Henkilötietojen käsittelyn osalta on esimerkiksi kuvattava mitä henkilötietoja kerätään, käsiteltävät henkilötietoryhmät ja tietosisältö. ISO 27001 -standardin vaatimuksena on dokumentaation ylläpito tietoturvallisuuden osalta.

5 ISO 27001 tarjoaa strategisen hallintatavan

Tietoturva ulottuu pidemmälle kuin asiakkaidemme henkilötietojen suojaamiseen. Tietoturvan hallintajärjestelmän (ISMS) käyttöönotto Fastroissa oli strateginen päätös ja käyttöönotossa otettiin huomioon myös muut yritykselle arvokkaat tiedot, kuten immateriaalioikeudet ja kaupallisesti arkaluontoiset tiedot.

ISO 27001 myötä Fastroi hallinnoi tieto-omaisuuttaan järjestelmällisesti, mikä helpottaa tietoturvallisuuden jatkuvaa parantamista ja mukautumista muuttuviin olosuhteisiin.

Standardi tarjoaa mallin tietoturvallisuuden hallintajärjestelmän rakentamiseen ja hallintaan, riskienarviointiin sekä erilaisten turvamekanismien ja valvontatavoitteiden valitsemiseen. Standardin noudattaminen auttaa meitä ylläpitämään ja parantamaan asiakkaidemme, liikekumppaniemme ja sidosryhmiemme luottamusta yritykseemme ja liiketoimintamme kestävyyteen.

6 Yhteenveto ISO 27001 -sertifikaatti

ISO 27001 -sertifiointi osoittaa, että olemme sitoutuneita noudattamaan tietoturvan ja tietosuojan vaatimuksia. ISO/IEC 27001 on kansainvälinen standardi, joka kuvaa tietoturvan hallintajärjestelmän perustamisen, toteuttamisen ja ylläpidon sekä järjestelmän jatkuvan parantamisen. ISO/IEC 27001 mukaisesti tietoturvallisuutta tarkastellaan riskienhallinnan kautta ja se on osa organisaation rakennetta ja toimintaa. ISO/IEC 27001 tarjoaa kattavat hallintakeinot, jotka auttavat organisaatioita suojaamaan henkilöstöä, prosesseja ja teknologiaa.

ISO/IEC 27001 standardin avulla varmistetaan organisaation tietojen luottamuksellisuus, eheys ja saatavuus. Organisaatiot voivat standardin avulla suunnitella tietoturvaohjelman, joka auttaa suojaamaan, valvomaan ja parantamaan koko yrityksen turvallisuutta ja kattaa toimialakohtaisten tietoturvavaatimusten ja -määräysten noudattamisen.

fastroi

— Caring together —

Fastroi Oy | www.fastroi.fi | sales@fastroi.fi