

Tietoturvaperiaatteet kumppaneille

Johdanto

Tietoturvaperiaatteissa määritellään käytännön toimintatavat tietoturvan toteuttamiseen. Tietoturvaperiaatteet velvoittavat Kuusakoskelle sopimussuhteessa olevia alihankkijoita. Tietoturvaperiaatteet ovat voimassa toistaiseksi ja se on Kuusakosken IT Managerin hyväksymä.

Tietoturvapoikkeamat

Jokainen kumppani on velvollinen raportoimaan havaitsemistaan tietoturvaan liittyvistä uhkista ja poikkeamista Kuusakosken yhteyshenkilölle. Tietoturva- tai tietosuojalainsäädäntöä ja tietoturva- ja tietosuojapolitiikkaa sekä sen perusteella annettuja ohjeita vastaan havaitut rikkomukset tiedotetaan aina Kuusakosken yhteyshenkilölle.

Tietoturvarikkomuksesta voi seurata yhteistyön päättäminen. Mikäli rikkomuksesta aiheutuu taloudellisia menetyksiä, voidaan päätyä vahingonkorvausvaatimukseen. Tietojen väärinkäyttö tai tahallinen ohjeiden vastainen toiminta voi johtaa rikosoikeudellisiin seuraamuksiin.

Tietoturvtiimillä ja tietohallinnolla on ylimmän johdon antama valtuutus ja velvollisuus tehdä tietojärjestelmien ja tietojen käsittelyn tietoturvallisuuden sekä tietosuojan seuranta ja valvontaa sekä tarvittaessa ryhtyä toimenpiteisiin ongelmatilanteiden selvittämiseksi ja havaittujen riskien korjaamiseksi. Tapauksista raportoidaan tarvittaessa konsernin johdolle.

Kumppanien henkilöturvallisuus

Kumppanien henkilöturvallisuudella tarkoitetaan henkilöstön toimista aiheutuvien ja heihin kohdistuvien tietoturvaohjeiden hallintaa. Tavoitteena on luotettava kumppaniverkosto, joka tuntee heille asetetut tietoturvaohjeet sekä velvollisuudet sopimussuhteen alkaessa, aikana ja päättyessä.

Periaatteet:

- Henkilöstön perehdytykseen kuuluu tietoturva- ja tietosuojaohjeiston läpikäynti. Kumppani vastaa siitä, että heidän työntekijöillään on selvillä yrityksen ja Kuusakosken tietoturva- ja tietosuojavaatimukset ja -käytännöt.
- Työntekijöille järjestetään tarvittaessa tietoturvakoulutusta henkilöstön tietämyksen ylläpitämiseksi.
- Jokaisella on tietoturvariskien ja -poikkeamien havainnointi ja ilmoitusvelvollisuus.
- Työsuhteen päättymiseen liittyvät järjestelyt toteutetaan siten, että pääsy Kuusakosken tietojärjestelmiin sekä tiloihin päättyvät työtehtävän päättyessä. Kuusakoskea on tiedotettava ajoissa, ennen työsuhteen päättymistä.

Fyysinen tietoturva

Fyysisellä tietoturvallisuudella tarkoitetaan toimitilojen, tietotyövälineiden, sekä muiden arkaluontoista tietoa sisältävien laitteiden tai muun materiaalin suojaamista.

Periaatteet:

- Asiaton pääsy yrityksen tai palveluntuottajan tiloihin, joissa on tietojärjestelmäympäristö tai arkaluonteista materiaalia tulee estää pääsynvalvonnalla.
- Henkilökortin käyttöä edellytetään Kuusakosken alihankkijoilta Kuusakosken toimitiloissa, ellei henkilöä tunnusteta muutoin.
- Tietoteknisten laitteiden tai tärkeää tietoa sisältävien arkistojen sijoittelussa tulee huomioida vesi-, lämpö-, ja tulivahingon riski. Sähkönsyötössä tulee varautua katkoksiin huomioiden laitteistojen kriittisyys.

Kuusakosken IT-palveluiden ja tietojärjestelmien turvallisuus

IT-palveluiden ja – tietojärjestelmien turvallisuus käsittää tietojärjestelmät, IT-palvelut, tukipalvelut, kapasiteettipalvelut sekä ohjelmistokehityskumppanit. Tavoitteena on Kuusakosken tarpeita parhaiten vastaavat tietoturvalliset tietojärjestelmät ja palvelut sekä niitä toimittavat kumppanit, jotka ovat sitoutuneet noudattamaan Kuusakosken tietoturvapolitiikan mukaista toimintaa sekä edelleen kehittämään sitä.

Periaatteet Kuusakosken järjestelmissä:

- Tietojärjestelmien ja IT- palveluiden hankinnat tehdään keskitetysti Kuusakosken tietohallinnosta käsin. Hankinnan edellytys on toiminnallinen ja tekninen soveltuvuus yrityksen IT-palveluarkkitehtuuriin.
- Uusien ohjelmistojen käyttöönoton edellytys on, että ohjelmisto on testattu ja että myös tietoturvatestaus on hyväksytysti suoritettu.
- IT-palveluiden kumppaneilta edellytetään salassapitosopimukset, jos palvelussa käsitellään yrityksen kannalta salassa pidettävää tai tietosuojasetuksen mukaisesti henkilötiedoksi luokiteltavaa tietoa.
- IT-palveluntarjoajilta edellytetään myös omassa toiminnassaan tietoturva- ja tietosuojalainsäädännön mukaista toimintaa.

Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan päätelaitteita, palvelimia, verkkolaitteita sekä muita tiedon käsittelyssä tarvittavia laitteita. Käytettävien laitteistojen tulee mahdollistaa tietoturvallisuusperiaatteiden mukainen toiminta.

Periaatteet:

- Laitteiden asennukset suoritetaan hyväksytyjen standardien mukaisesti ja asennuksessa huolehditaan, että tarvittavat tietoturvaohjelmistot asennetaan sekä asetukset muokataan tietoturvaohjeiston mukaisesti.
- Kuusakosken omistamia tietoja ei tallenneta tai siirretä ulkopuolisille laitteille ilman Kuusakosken kirjallista lupaa.

Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan häiriötöntä ja turvallista tietoliikenneyhteyksien käytettävyyttä, suojausta ja salausta, käyttäjien tunnistusta, tietoliikenteen varmistamista ja verkkoliikenteen havainnointikyvyn mahdollistamista. Tietoliikenneturvallisuustyön tulos on turvatut ja toimintavarmat tiedonsiirtoyhteydet.

Periaatteet:

- Tietoverkot ja järjestelmät, joissa Kuusakosken tietoja käsitellään, tulee suojata asianmukaisesti.
- Havaittuihin poikkeamiin tulee reagoida riittävin toimenpitein ja Kuusakoskeen liittyvistä tapahtumista tulee ilmoittaa viivytyksettä.
- Sähköpostien salausta käytetään kaikissa luottamuksellisissa sähköpostiviesteissä.