

Nykytila-analyysi Vihdin kuntakonsernin organisaatiourvallisuudesta sekä turvallisuuteen liittyvät asiantuntijapalvelut

Liite 2.1 Tietoturva-vaatimukset

Tässä dokumentissa asetetut vaatimukset kohdistuvat hankinnan kohteena olevaan palveluun. Toimittajan tulee täyttää kaikki tässä dokumentissa asetetut vaatimukset palvelua tuottaessaan.

Valitun toimittajan tulee pyydettyä toimittaa selvitys, jonka perusteella voidaan todentaa tässä dokumentissa asetettujen vaatimusten täyttyminen. Asiakkaalla on myös oikeus tarkastaa näiden tietoturva-vaatimusten täyttyminen hankintasopimuksen luvun "Tarkastusoikeus" mukaisesti. Vihdin kunnalla on oikeus tarkastaa näiden tietoturva-vaatimusten täyttyminen Sopimuksen luvun "Tarkastusoikeus" mukaisesti.

Hallinnollisen turvallisuuden vaatimukset

Vaatus nro	Nimi	Vaatus
H1	Periaatteet	Toimittajalla on kirjallinen tietoturvapoliittika, joka kuvaa miten Toimittaja on järjestänyt tietoturvallisuuden varmistamisen organisaatiossaan. Tietoturvapoliittika kuvaa Toimittajan tietoturvaluustoimenpiteiden kytkeytymisen Toimittajan toimintaan. Tietoturvapoliittika on tietojen suojaamisen kannalta kattava ja tarkoituksenmukainen.
H2	Tehtävät ja vastuut	Toimittaja on määritellyt ja dokumentoinut vähintään seuraavat vastuut hankinnan kohde huomioiden: a) turvallisuusjohtaminen b) fyysinen turvallisuus c) tekninen turvallisuus d) varautuminen ja jatkuvuudenhallinta e) tietosuojat f) riskienhallinta g) turvallisuuden kokonaisvastuu
H3	Resurssit	Toimittajalla on käytössään riittävät resurssit ja asiantuntemus tietoturvallisuuden varmistamiseksi huomioiden toiminnan jatkuvuus myös normaaliolojen häiriötilanteissa ja poikkeusoloissa.
H4	Suojattavat kohteet	Toimittaja tunnistaa ja dokumentoi liiketoimintaansa ja hankinnan kohteeseen liittyvät suojattavat kohteet. Suojattavia kohteita ovat esimerkiksi tiedot, tietojärjestelmät, tietojenkäsittelyprosessit, tilat sekä muut organisaation tietoturvallisuuteen vaikuttavat kohteet.
H5	Suojattavat kohteet - käsittely	Toimittajan tulee käsitellä Tilaaajan antamia tietoja Tilaaajan antamien ohjeiden mukaisesti.
H6	Seuranta ja valvonta - tietojen käyttö ja luovutukset	Toimittaja on tunnistanut lokitietojen keräämiseen liittyvät vaatimukset ja varmistanut niiden perusteella lokitietojen keräämisen ja seurannan riittävyyden. Toimittajalla tulee olla riittävät lokitiedot, joista se pystyy todentamaan muun muassa sen, kuka on käsitellyt Asiakkaan tietoja.
H7	Häiriöiden hallinta	Toimittajalla on tietoturvaluusuhäiriöiden ja poikkeamatilanteiden käsittelyyn määritellyt prosessit ja ohjeet. Toimittaja reagoi hankinnan kohteeseen liittyviin tietoturvapoiikkeamiin viivytyksettä, ryhtyy niiden johdosta asianmukaisiin toimenpiteisiin.
H8	Salassapito- ja vaihtovelvollisuus	Toimittaja varmistaa, että sen henkilöstö noudattaa Tilaaajan antamia, tietojen suojaamista ja asiakirjojen käsittelyä koskevia vaatimuksia.
H9	Koulutukset	Toimittaja varmistaa ohjeistuksilla, koulutuksilla ja viestinnällä, että palvelua tuottava henkilöstö on tietoinen tietoturvaluusuutta koskevista vaatimuksista.
H10	Käyttö- ja käsittelyoikeudet	Toimittaja varmistaa, että hankinnan kohteeseen liittyvien tietojärjestelmien käyttöoikeudet ja tietojen käsittelyoikeudet määritellään tehtäviin liittyvien tarpeiden mukaan sekä pidetään ajantasaisina. Vaatus koskee myös laitteita, joita Toimittaja käyttää tuottaessaan hankinnan kohteen mukaista palvelua.
H11	Käyttö- ja käsittelyoikeudet - päättyminen	Toimittaja palauttaa Asiakkaan pyynnöstä ja viimeistään hankintasopimuksen perusteella tuotetun Palvelun päätyttyä kaikki Asiakkaan palvelun suorittamista varten saamansa alkuperäisen lähdeaineiston ja sen kopiot, jolleivät sopijapuolet siitä erikseen toisin sovi. Toimittaja varmistaa, että työntekijä palauttaa hallussaan olevat Tilaaajan tiedot käyttö- ja käsittelyoikeuden päättyessä.
H12	Tietojen käsittely	Toimittaja varmistaa, että Asiakkaan tietoja käsitellään ja säilytetään siten, ettei sivullisilla ole niihin pääsyä.