VATAJANKOSKEN SÄHKÖN TIETOTURVAPOLITIIKKA

1 TAVOITE

Tietojenkäsittely tukee Vatajankosken Sähkön (VSO) palvelujen tuottamista ja palvelujen tehokkuus riippuu osaltaan tietojenkäsittelystä. Tietoaineistot sisältävät asiakkaisiin, työntekijöihin ja toimintaan liittyvää tietoa, joka on lainsäädännön perusteella suojattava. Tietojenkäsittelyn on oltava tehokasta, virheetöntä ja varmaa.

Tietoturvapolitiikka määrittelee ne periaatteet, vastuut, toimintatavat sekä seurannan ja valvonnan, joita yhtiössämme noudatetaan tietoturvan toteuttamisessa ja kehittämisessä. Tietoturvapolitiikkaa täydentävät toimintajärjestelmän ohjeistukset.

2 LAAJUUS

Tämä yhtiömme hallituksen vahvistama tietoturvapolitiikka kattaa kaikkeen toimintaamme liittyvät tietojen käsittelyn tehtävät.

3 VASTUU

Jokaisen yhtiömme henkilöstöön kuuluvan työntekijän ja luottamushenkilön, sekä muiden VSO:n tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietoturvapolitiikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä, sekä kansallisia normeja ja ohjeita.

4 TOIMINNON KUVAUS

4.1 Tietoturva

Tietoturva tarkoittaa tietojen käsittelyn ja arkistoinnin turvaamista. Tietoturva rakentuu tiedon luottamuksellisuudesta, eheydestä, saatavuudesta, käytettävyydestä ja kiistämättömyydestä sekä tietojen käsittelyn valvonnasta.

Tietoturvaan kuuluvat tietojen käsittelijöiden toimintatavat, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet.

Hyväksytyn tietoturvapolitiikan mukainen tietoturva tulee sisällyttää luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa yrityksen yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

4.2 Tietoturvatyö

Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tietoturvatyön päämäärä on turvata yrityksen toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Yritys vastaa osana tietoturvatyötä myös asiakkaiden asiakirjojen ja asiakastietoja sisältävien muiden asiakirjojen suojaamiseen liittyvästä tietoturvatyön suunnittelusta ja toteuttamisesta.

4.3 Organisointi ja vastuut

Tietoturvaa johtaa ja valvoo toimitusjohtajan asettama tietoturvaryhmä, johon osallistuvat merkittävimpien ohjelmistojen pääkäyttäjät sekä ylimmän johdon edustus. Tietoturvaryhmän vetäjänä ja kokoonkutsujana toimii toimintajärjestelmävastaava. Toimitusjohtaja päättää yrityksen kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista.

Tietoturvaryhmä vastaa yrityksen tietoturvatyön kokonaisuudesta johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa. Ryhmä vastaa myös tietoturva-asioista tiedottamisesta yrityksen ulkopuolelle ja yrityksessä yleisellä tasolla. Ryhmä vastaa myös yrityksen henkilötietoja sisältävien henkilörekistereiden suojaamisesta ja valvonnasta.

Tietoturvaryhmä käsittelee tietoturvan linjaukset ja ohjeet ennen kuin ne esitellään toimitusjohtajalle hyväksyttäväksi.

Jokaisella tietojärjestelmällä on omistajayksikkö ja vastuuhenkilö eli pääkäyttäjä. Tietojärjestelmän vastuuhenkilön velvollisuuksiin kuuluu tietojärjestelmän toimintaan ja turvallisuuteen asetettavien vaatimusten (esim. kriittisyyden, jatkuvuussuunnittelun ja varmuuskopiointimenettelyn) määrittely sekä käyttöoikeuksien myöntäminen ja valvonta.

Tietoturva-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaa toiminnon esimies.

Jokainen yrityksen työntekijä, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan toteuttamisesta sekä tietoturvaohjeiden noudattamisesta. Jokainen henkilö on velvollinen tietoturvaan liittyvien uhkien ja poikkeamien raportoimisesta esimiehelleen tai tietoturvaryhmälle.

4.4 Tietoturvan toteutus

Tietoturvan toteuttamisen perusta on tämä yrityksen hallituksen hyväksymä kirjallinen tietoturvapolitiikka, joka annetaan tiedoksi jokaiselle yrityksen työntekijälle ja tietojärjestelmien käyttäjälle.

Yrityksen tietoturvaperiaatteet perustuvat kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaa, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin.

Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon yrityksen tietoturvan kehittämisessä.

Tietoturvan toteuttaminen ja ylläpito kuvataan yksityiskohtaisesti tietoturvapolitiikkaa täydentävissä toimintajärjestelmän ohjeistuksissa. Tietoturvan toteutuksen tulee perustua niihin vaatimuksiin, joita toiminta ja palvelut sekä kunkin tiedon ja tietojärjestelmän turvallisuusluokka asettavat tietojenkäsittelyn varmuudelle, käytettävyydelle, salassapidolle, laadulle ja toiminnan jatkuvuudelle sekä toimintaan kohdistuvien riskien arvioinnille. Vaatimusten selvittäminen, riskien arvioiminen ja niiden perusteella turvallisuustoimenpiteiden määritteleminen tapahtuu säännöllisesti suoritettavilla turvallisuusanalyyseillä.

Tietoturvan tavoitteiden saavuttaminen on jatkuva prosessi, joka tapahtuu hallinnollisten ja teknisten ratkaisujen avulla.

Käyttäjien toimintaa ohjataan ohjeistuksiin sisältyvillä käyttösäännöillä sekä vahvistetuilla ja saatavilla olevilla toimintaohjeilla sekä tietoturvakoulutuksella. Jokainen käyttäjä allekirjoittaa käyttäjän tietosuojasitoumuksen saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien ja tietoaineistojen käyttöön.

4.5 Tietoturvan seuranta ja valvonta

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta esimiehelleen tai tietoturvaryhmälle.

Yksikön esimiehen tehtävänä on valvoa tietoturvan toteutumista omassa yksikössään.

Tietoturvaryhmän tehtävänä on seurata ja valvoa tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.