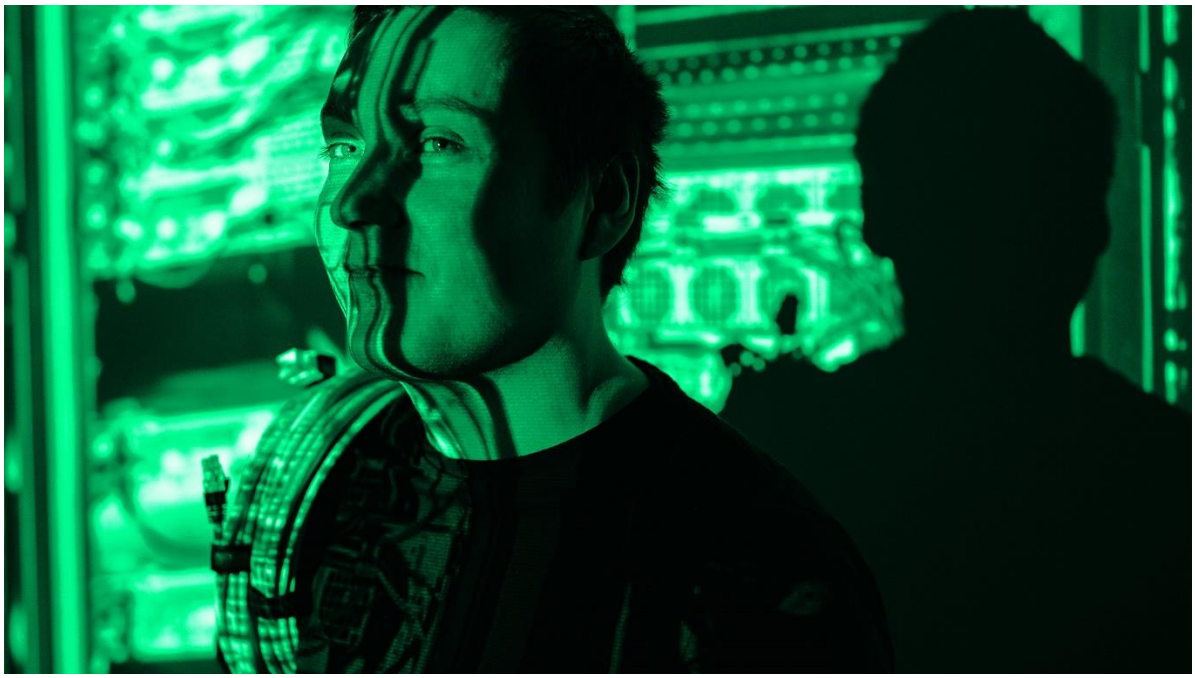
prog·it

TIETOTURVAOPAS PK-YRITYKSELLE

Tietoturvasuunnitelman laatiminen ja toimeenpano



TIETOTURVA-UHAT *ovat merkittävä riski kaikille organisaatioille organisaation koosta, tunnettuudesta ja sijainnista riippumatta. Liiketoiminnan keskeytyminen, merkittävät taloudelliset menetykset, mainehaitat ja jopa toiminnan loppuminen ovat pahimpia, mutta todellisuudessa varsin realistisia seuraamuksia tietoturvariskin toteutumisesta.*

Tietoturvauhat monipuolistuvat ja uudistuvat. Tämän vuoksi on tärkeää, että organisaatioissa luodaan käytännöt, joilla riskejä tunnistetaan ja arvioidaan säännöllisesti. Tietoturvaa varmistavien toimintamallien ja ohjeistuksen tulee olla ajantasaista. Kaikista varotoimenpiteistä huolimatta riskit voivat silti toteutua ja siksi myös häiriötilanteita varten tulee laatia ennalta suunnitelma.

TÄMÄ OPAS *sisältää keskeiset tietoturvan suunnittelussa, kehittämisessä ja ylläpitämisessä huomioitavat asiat sekä tarjoaa käytännönläheisiä ohjeita PK-yrityksen liiketoimintajohdolle ja IT-asioista vastaaville.*

TOP 3 UHAT VUONNA 2020

1) Päivittäinen tietojenkalastelu ja huijaukset jatkuvat. Kuka tahansa voi päätyä huijausten ja tietojenkalastelun kohteeksi.

2) Uusia haavoittuvuuksia hyödynnetään nopeasti ja siksi perinteiset torjuntakeinot eivät enää riitä. Tietojärjestelmiä ja sovelluksia on päivitettävä yhä nopeammin

3) Palveluja ostetaan suunnittelemattomasti ja vastuita ei määritellä selkeästi. Rikolliset hyödyntävät kumppaneita tai alihankkijoita pyrkiessään sisään varsinaisen kohteensa tietojärjestelmiin.

LÄHDE: Kyberturvallisuuskeskus

Tietoturvan perusasiat

TIETOTURVA kattaa kaiken sen, mikä liittyy tietojen saatavuuteen, oikeellisuuteen sekä tietojen luottamuksellisuuden säilymiseen käsittelyn, säilytyksen ja tiedonsiirron aikana.

TIETOSUOJALLA tarkoitetaan henkilötietojen sekä henkilökohtaiseen toimintaan liittyvien tietojen keräämisen ja käsittelyn rajoittamista niin, ettei henkilön yksityisyys turhaan vaarannu.

TIETOTURVAN PERUSPERIAATTEITA ovat:

- Saatavuus tai käytettävyys: tiedot ja järjestelmät ovat niihin oikeutettujen henkilöiden käytettävissä haluttuna aikana
- Luottamuksellisuus: tiedot ja järjestelmät ovat vain niiden henkilöiden käytettävissä, joilla on tähän oikeus
- Eheys: tietojen ja järjestelmien tulee olla luotettavia, oikeita ja ajantasaisia. Ne eivät muutu tai ole muutettavissa laitteisto- tai ohjelmistovikojen, luonnontapahtumien tai inhimillisen toiminnan seurauksena.

Tietoturvan osa-alueita ovat:

HALLINNOLLINEN TIETOTURVA: tietoturvapolitiikka, tietoturvaa koskevat linjaukset ja ohjeistukset, organisointi

FYYSINEN TIETOTURVA: toimitilojen, laitteiden ja asiakirjojen suojaaminen mm. ilkivallalta, varkaudelta sekä inhimillisiltä vahingoilta kuten sähkö- ja vesivahingolta.

HENKILÖSTÖTURVALLISUUS: henkilöstöriippuvaisten riskien hallinta, henkilöstön ohjeistus ja koulutus erilaisten tilanteiden varalle ja tiedon käsittelyssä.

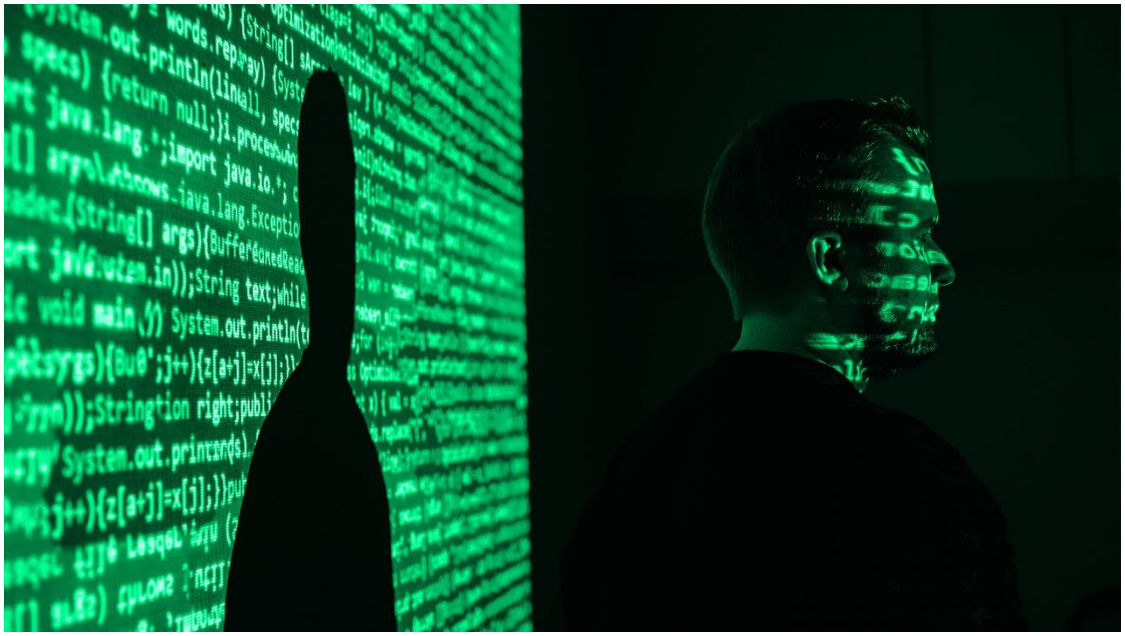
KÄYTTÖTURVALLISUUS: päivittäisten toimintojen ja rutiinien turvaaminen, tietotekniikan käyttöön, IT-ympäristöön ja tietojenkäsittelyyn liittyvä tuki-, ylläpito-, kehittämis- ja huoltotoimintojen turvallisuus.

LAITTEISTOTURVALLISUUS: tietojenkäsittely- ja tietoliikennelaitteiden käytettävyys, toiminta, kokoonpano, kunnossapito ja laadunvarmistus.

OHJELMISTOTURVALLISUUS: käyttöjärjestelmät, ohjelmistot sekä sovellus- ja tietoliikenneohjelmat, tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, lokimenettelyt, ohjelmistojen laadunvarmistus, turvallisuustoimet.

TIETOAINEISTOTURVALLISUUS: tiedostojen ja muiden tietoaineistojen käytettävyys, eheys ja luottamuksellisuus; tietoaineistojen luokitus ja luettelointi sekä asianmukainen hallinta, käsittely, säilytys ja hävittäminen.

TIETOLIIKENNETURVALLISUUS: varmistetaan tietojen turvallisuus, käytettävyys ja eheys, kun tieto liikkuu järjestelmien sisällä tai organisaatioiden välillä.



Tyypillisimpiä tietoturvariskejä

Tietoturvan suunnittelua varten on ensin tunnistettava merkittävimmät riskit. Kriittisimpiä osa-alueita ovat yleensä ne, joiden vahingoittuminen tavalla tai toisella aiheuttaa merkittäviä suoria tai välillisiä kustannuksia tai mainevahinkoja tai pahimmillaan jopa tekevät yrityksen toiminnan jatkamisen mahdottomaksi.

Tietoturvariskien tunnistaminen on osa liiketoiminnan riskien hallintaa ja jatkuvuuden suunnittelua. Riskien tunnistaminen tulee ulottaa kaikille edellä mainituille turvallisuuden osa-alueille. Riskien tunnistamisessa kannattaa hyödyntää eri toimintoja edustavien henkilöiden ryhmää, jotta eri näkökulmat tulevat katettua. Näin saadaan esille myös inhimilliseen käyttäytymiseen liittyviä riskejä, jotka voivat olla erittäin olennaisia tietoturvan kannalta.

Lisäksi riskiarviointi tulee ulottaa myös mahdollisten palvelutoimittajien hallinnassa oleviin asioihin ja heidän käytäntöihinsä.

Seuraavassa riskianalyysin tueksi lueteltuna muutamia varsin yleisiä riskejä:

- Päivityksiä laiminlyödään ja/tai ne tehdään vain osittain organisaatiossa (käyttäjä voi esimerkiksi siirtää kriittistä päivitystä itse myöhempään ajankohtaan)
- Liiketoimintakriittistä tietoa on varmistamattomassa muodossa
- Laitteet rikkoontuvat, niitä varastetaan tai ne katoavat
- Laitehallinta on puutteellista ja/tai keskitettyä laitehallintaa ei ole. Esimerkiksi hallinnan ulottumattomissa olevaa mobiililaitetta ei pystytä tyhjentämään sen kadotessa.
- Yhteiskäytössä olevien koneiden suojaus on puutteellinen
- Salasanat ovat heikkolaatuisia ja/tai salasanojen hallinnassa on puutteita. Samoja salasanoja käytetään sekä yleisissä palveluissa että yrityksen järjestelmissä.
- Käyttäjä ei kirjaudu ulos poistuessaan työpisteestään
- Vahvaa tunnistautumista ei ole käytössä
- Liiketoimintakriittistä tietoa tai henkilötietoa sisältävät asiakirjat ovat pöydillä, tulostimilla, avoimissa kaapeissa
- Yhteisten dokumenttien käyttöoikeudet eivät ole ajan tasalla
- Lähtevien henkilöiden laitteiden käsittelyyn, oikeuksien poistamiseen, asiakirjojen ja henkilötietojen käsittelyyn ym. ei ole yhdenmukaista toimintatapaa
- Käytettyjä tietokoneita lojuu (käsittelemättöminä) ”varakoneina” ja/tai käytettyjen laitteiden turvalliseen käytöstä poistoon ei ole toimintatapaa
- Työtä tehdään erilaisissa (huonosti suojatuissa) ympäristöissä etänä – kotona, autossa, kahvilassa.

- Kalasteluviestejä ei tunnisteta tai niiden aiheuttamaa riskiä ei ymmärretä (kalasteluviestit kehittyvät jatkuvasti)
- Sijaisia ei ohjeisteta riittävästi tietoturvanäkökulmasta (mm. kalasteluviestien kulta-aikaa on kesälomakausi)
- Henkilöstöä ei ole ohjeistettu ja koulutettu tietoturva-asioissa riittävästi tai ohjeet eivät ole ajan tasalla.
- Henkilöstöllä ei ole tietoa, miten tulee toimia epäillessään tietoturvauhkaa tai uhan jo toteuduttua.
- Henkilötietoja käsitellään ja säilytetään erilaisissa epävirallisissa henkilörekistereissä sähköisesti tai paperiversioina ilman tietosuoja-asetuksen mukaista käyttötarkoitusta
- Yrityksen asiakirjoja ja/tai järjestelmiä käytetään yksityisiltä koneilta, jotka eivät ole vaatimusten mukaisia
- Muistitikkuja tai muita siirrettäviä muistilaitteita säilytetään ja käytetään huolettomasti tai niille tallennetaan arkaluonteista materiaalia

Tietoturvapolitiikka, -suunnitelma ja -ohjeet

TIETOTURVAPOLITIIKKA on ylin organisaation tietoturvaa koskeva dokumentti. Se perustuu liiketoimintastrategiaan, noudatettaviin lakeihin ja asetuksiin sekä organisaatiossa tunnistettuihin tietoturvariskeihin. Tietoturvapolitiikka määrittelee ytimekkäästi tietoturvaa koskevat keskeiset linjaukset ja tavoitteet, organisoitumisen ja roolit sekä tietoturvan hallinnan ja valvonnan keskeiset periaatteet. Tietoturvapolitiikasta on esimerkki liitteessä 1.

Tietoturvapolitiikkaa toteutetaan tietoturvaa koskevan tietoturvasuunnitelman ja ohjeistuksen avulla. Seuraavassa kohdassa esitetty tietoturvasuunnitelman runko on tehty ISO27001-tietoturvastandardia mukaillen. Tietoturvasuunnitelman runkoa kannattaa hyödyntää jo riskikartoitusvaiheessa.

TIETOTURVASUUNNITELMA

Osa-alue	Sisältö
1. Tieto-turvallisuu-den organi-sointi	• Tietoturvavastuiden määrittely: nimetty tietoturvasta vastaava, johdon rooli, käyttäjien roolit • Tietoturvallisuusvastuut ja käytännöt yhteistyökumppanien ja pal-velutoimittajien kanssa • Tietoturvallisuuskäytännöt liikkuvassa työssä ja etätyössä
2. Henkilöstö-turvallisuus	• Tietoturvakäytännöt työsuhteen alussa ja työsuhteen päättyessä • Tietoturvakäytännöt vuokratyöntekijöitä tai muita väliaikaistyön-tekijöitä käytettäessä • Tietoturvaohjeistus henkilöstölle • Tietoturvakoulutus henkilöstölle
3. Suojattavan omaisuuden hallinta	• Suojattavan omaisuuden tunnistaminen, luettelointi, hallinta ja luovutuskäytännöt esim. työsuhteen päättyessä. • Tiedon luokittelu, eri luokkiin kuuluvan tiedon hallinnan ja käytön periaatteet • Tietovälineiden hallinta ja suojaaminen
4. Pääsynhal-linta ja salaus	• Pääsyoikeuksien hallinnan käytännöt: käyttäjien rekisteröinti ja oi-keuksien jakaminen ja muuttaminen, tunnistautumistietojen hal-linta • Turvalliset kirjautumiskäytännöt, salasanojen hallinta, salauskäy-tännöt
5. Fyysinen turvallisuus	• Arkaluonteisia ja liiketoimintakriittisiä tietoja sisältävien alueiden, tilojen ja palveluiden fyysinen turvaaminen ja varmistaminen • Kulunvalvonta • Laitteiden sijoitus, suojaus, huolto ja käytöstä poisto • Suojaus sähkökatkoilta • Kaapeloinnin suojaus • Toimitilan ulkopuolelle vietävien laitteiden ja tietojen suojaus
6. Käyttö-turvallisuus	• Ajan tasalla olevat ohjeet • Kapasiteetinhallinta • Kehitys-, testaus- ja tuotantoympäristöjen erottaminen • Haittaohjelmilta suojautuminen • Tietojen varmuuskopiointi • Tapahtuma- ja pääkäyttäjälokit ja niiden suojaaminen • Haavoittuvuuksien hallinta • Ohjelmien asentamisen rajoittaminen
7. Viestintä-turvallisuus	• Verkon hallinta ja valvonta • Verkkopalvelujen turvaaminen

	• Sähköisen viestinnän turvaaminen • Salassapito- ja vaitiolosopimukset
8. Järjestelmien hankkiminen, kehittäminen ja ylläpito	• Tietoturvavaatimusten huomiointi järjestelmävaatimuksissa sekä järjestelmien suunnittelussa, testauksessa ja käyttöönotossa • Sovelluspalveluiden suojaaminen julkisessa verkossa • Sovelluspalvelutapahtumien suojaaminen • Järjestelmämuutosten hallinta
9. Suhteet toimittajiin	• Toimittajasopimukset ja tietoturvakäytännöt • Toimittajien palveluihin tulevien muutosten hallinta
10. Tietoturva-häiriöiden hallinta	• Käytännöt tietoturvauhkien ja -tapahtumien tunnistamiseen, raportointiin ja hallintaan
11. Liiketoiminnan jatkuvuuden hallinta	• Käytännöt jatkuvaan riskienhallintaan ja tietoturvakäytäntöjen päivitykseen tarvittaessa • Liiketoimintakriittisten tietojenkäsittelypalveluiden saatavuuden varmistaminen
12. Vaatimustenmukaisuus	• Lakien, viranomaisten määräysten ja sopimuksien velvoitteiden mukaisen toiminnan ohjeistaminen • Immateriaalioikeuksista huolehtiminen • Tallenteiden suojaaminen • Tietosuoja ja henkilötietojen suojaaminen

HYVÄ LÄHTÖKOHTA tietoturvasuunnitelman toimeenpanoon on seuraavista asioiden ohjeistaminen ja kuntoon saattaminen:

- Tietoturvan vastuumatriisin laatiminen huomioiden myös kolmannet osapuolet ja mahdollisten sopimusvastuissa olevien epäkohtien korjaaminen
- Tiedon luokittelu esimerkiksi kolmeen luokkaan (liiketoimintakriittinen tieto, yksityisyyden suojan piirissä oleva tieto, muu tieto) sekä turvallisuuden varmistaminen ensisijaisesti liiketoimintakriittisen ja yksityisyyden suojan piirissä olevan tiedon osalta
- Muistilistat työsuhteen alkuun ja päättymiseen, tarvittaessa muutamalle eri roolille (esim. johto/esimiesrooli, työntekijärooli, väliaikainen tehtävä) sekä ohjeet oikeuksien hallintaan
- Ohjeistus käyttäjille siirrettävien tietovälineiden (kannettavat, mobiililaitteet, muistitikut ja laitteet) ja muiden fyysisten tietovälineiden suojaamiseen, käyttöön ja käytöstä poistoon
- Ohjeistus käyttäjille kirjautumis-, salasana- ja salauskäytäntöihin
- Ohjeistus ja varautumissuunnitelma häiriötilanteisiin (ks. lisää asiasta seuraavassa luvussa ”Toiminta häiriötilanteissa”)
- Fyysisen ympäristön turvaaminen, kuten
    - Arkistotilojen turvallisuus
    - Palvelintilojen turvallisuus
    - Työasemat, joista on pääsy liiketoimintakriittisiin tai arkaluonteisiin tietoihin
    - Työpisteiden suunnittelu (esim. näyttöjen sijoittelu)
- Henkilötietojen käsittelyä koskevien vaatimusten huomioiminen ja toteuttaminen (ks. lisää luvussa ”Tietosuoja”)

Esimerkki käyttäjäohjeistuksesta on liitteessä 2. Toimintaa häiriötilanteissa sekä tietosuojaa on käsitelty erikseen seuraavissa luvuissa.

Toiminta häiriötilanteissa

Häiriötilanteita varten on syytä olla toimintasuunnitelma valmiina, sillä yleensä tilanne vaatii nopeita toimia. Suunnitelmassa tulee minimissään määritellä:

- Vastuut poikkeamatilanteessa (tietoturvavastaava, johdon rooli, viestintävastaava, poikkeaman kohteena olevan palvelun vastaava)
- Tietoturvapoikkeamasta ilmoittaminen
- Poikkeamaan liittyvän tiedon kerääminen ja analysointi
- Käsittely
    - Eristämistoimenpiteet
    - Lähteen selvittäminen
    - Tapahtuminen kirjaaminen ja todistusaineiston kirjaaminen
    - Viestintä eri vaiheissa

Tietoturvapoikkeamatilanteessa (tai kun uhka sellaiselle on havaittu) otetaan yleensä ensimmäiseksi yhteyttä organisaation tietoturva-asioista vastaavaan henkilöön. Tietoturvapoikkeamista ilmoitetaan myös Viestintäviraston Kyberturvallisuuskeskukseen. Kyberturvallisuuskeskus ohjeistaa poikkeaman vahinkojen rajoittamisessa, lakisääteisten velvoitteiden täyttämisessä ja mahdollisen rikosilmoituksen tekemisessä sekä auttaa tarvittaessa tietoturvaloukkauksen analysoinnissa ja jatkotoimenpiteissä.

Julkaisussa mainittuja esimerkkejä tyypillisistä poikkeamatilanteista ja niihin reagoinnista ovat:

- Epäilyttävää tiedonsiirtoa ulkopuoliseen kohteeseen
- Palvelunestohyökkäys
- Tunkeutuja järjestelmässä
- Kohdistetut hyökkäykset
- Haittaohjelmatilanteet
- Pääsynhallinnan kriittinen poikkeama
- Arkaluonteisen tai liiketoimintakriittisen tiedon väärä käsittely
- Tietojen kalastelu (phishing)

Havaintoja tietoturvapoikkeamatilanteista voidaan saada esimerkiksi seuraavista lähteistä:

- Tietoturvaohjelmistojen hälytykset
- Verkko- ja tietojärjestelmäkohtaiset hyökkäyksen havaitsemisjärjestelmät
- Virustorjuntaohjelmistot

- Palveluiden käytettävyyden mittausohjelmistot
- Käyttöjärjestelmän, palveluiden ja sovellusten lokitiedostot
- Verkkolaitteiden lokitiedostot
- Julkisesti saatavilla olevat tietolähteet (esim. haavoittuvuustiedotteet), media, erilaiset keskusteluryhmät
- Käyttäjien yhteydenotot poikkeavasta toiminnasta.

Liitteessä 3 on malli sidosryhmäviestistä sähköpostipalveluun kohdistuneessa hyökkäyksessä. Tämän kaltaisia valmiita viestipohjia kannattaa sisällyttää valmiiksi varautumissuunnitelmaan.

LÄHDE JA LISÄTIETOJA:

Toimintasuunnitelmamalleja ja tarkempia ohjeistuksia löytyy mm. Valtiovarainministeriön julkaisusta 8/2017: Tietoturvapoikkeamien hallinta

Tietosuoja

Vuonna 2018 voimaan tullut EU:n yleinen tietosuoja-asetus ja kansallinen tietosuojalaki (2019) määrittelevät henkilötietojen käsittelyä koskevia velvoitteita ja toimintatapoja. Asetuksen ja lainsäädännön myötä esimerkiksi asiakkaista ja työntekijöistä kerättyjä henkilötietoja on käsiteltävä aiempaa huolellisemmin ja henkilötietojen käsittelystä on informoitava selkeästi läpinäkyvyyden periaatteita noudattaen. Henkilötietoja käsittelevän organisaation yritys on pystyttävä osoittamaan noudattavansa sääntelyä. Käytännössä tämä edellyttää henkilötietojen käsittelyä koskevaa dokumentointia ja sisäistä ohjeistusta.

Keskeiset noudatettavat periaatteet ovat

- KÄYTTÖTARKOITUSSIDONNAISUUS: henkilötietoja voidaan kerätä vain tiettyjä nimenomaisia laillisia käyttötarkoituksia varten
- TIETOJEN MINIMOINTI: henkilötietojen on oltava asianmukaisia, olennaisia ja rajoittua siihen, mikä on tarpeellista em. käyttötarkoitusta varten
- SÄILYTYKSEN RAJOITTAMINEN: henkilötiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen käyttötarkoitusta varten. Ei-tarpeelliset henkilötiedot on poistettava.
- TÄSMÄLLISYYS: rekisterinpitäjän käsittelemien henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä.
- LAINMUKAISUUS, KOHTUULLISUUS JA LÄPINÄKYVYYS: henkilötietojen käsittelyyn on oltava lailliset perusteet, joita voivat olla esimerkiksi rekisterinpitäjän oikeutettu etu, rekisteröidyn antama suostumus tai lakisääteinen tehtävä. Läpinäkyvyys edellyttää sitä, että rekisteröityjä informoidaan ymmärrettävällä tavalla henkilötietojen käsittelystä.
- EHEYS JA LUOTTAMUKSELLISUUS: henkilötietojen käsittelyn turvallisuus ja tietojen suojaaminen on varmistettava asianmukaisilla teknisillä ja hallinnollisilla toimilla.

Rekisterinpitäjän velvollisuuksia ovat edellä mainittujen periaatteiden noudattamisen lisäksi

- Osoitusvelvollisuus: on pystyttävä osoittamaan, että henkilötietojen käsittelyä koskevia periaatteita ja asetuksen muuta sääntelyä toteutetaan
- Riskien arviointi: toimia henkilötietojen suojaamiseksi suhteutetaan henkilötietojen käsittelystä rekisteröityjen oikeuksille ja vapauksille aiheutuvaan riskiin
- Henkilötietojen käsittelyä koskevan selosteen ylläpito (tietosuojaseloste)

- Tietosuojaa koskeva vaikutusten arviointi (kun rekisteröityjen oikeuksille ja vapauksille aiheutuu korkea riski henkilötietojen käsittelystä)
- Käsittelyn turvallisuus
- Henkilötietojen tietoturvaloukkauksista ilmoittaminen tietosuojavaltuutetulle ja rekisteröidyille
- Tietosuojavastaavan nimittäminen (koskee vain tiettyjä yhteisöjä)
- Henkilötietojen käsittelyn ulkoistaminen: rekisterinpitäjän ja henkilötietojen käsittelijän tulee laatia kirjallinen sopimus ulkoistettavasta henkilötietojen käsittelystä

Rekisteröidyllä on oikeus saada informaatiota henkilötietojen käsittelystä. Kun esimerkiksi yrityksen verkkosivuilla pyydetään jossakin palvelussa antamaan henkilötietoja, on samalla informoitava mahdollisuudesta tutustua yrityksen tietosuojakäytänteeseen tai tietosuojaselosteeseen. Esimerkki tietosuojaselosteesta on liitteessä 4.

Rekisteröidyllä on oikeus saada tietää, mitä häntä koskevia tietoja henkilörekisteriin on tallennettu sekä tietyin edellytyksin oikeus pyytää poistamaan häntä koskevia tietoja tai rajoittaa tietojen käsittelyä.

Tietosuoja-asetuksessa on esitetty perusteet, jolloin henkilötietoja voidaan siirtää käsiteltäväksi EU:n ulkopuolelle. Muissa tilanteissa henkilötietojen siirtäminen EU:n ulkopuolelle ei ole sallittua.

TIETOSUOJAA KOSKEVAT LÄHTEET JA LISÄTIETOJA:

- EK:n tietopaketti yrityksille EU:n yleisestä tietosuoja-asetuksesta ja tietosuojalaista
- Tietosuojavaltuutetun toimiston mallipohja rekisterinpitäjälle: Rekisteriseloste käsittelytoimista
- Tietosuojavaltuutetun toimiston mallipohja henkilötietojen käsittelystä: Henkilötietojen käsittelijän seloste käsittelytoimista - Tietosuojavaltuutetun toimisto
- TEM esitteet 4/2019: Työelämän tietosuojalaki

LIITE 1 ESIMERKKI TIETOTURVAPOLITIIKASTA

1. JOHDANTO

Tietotekniikka ja tietojenkäsittely ovat keskeinen osa Yritys Oy:n palvelujen tuottamista ja palvelulupauksen laadukas toimittaminen on riippuvainen tietojenkäsittelystä. Liiketoiminnan kannalta tärkeät sovellukset 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 yhtiöissä noudatetaan tietoturvan toteuttamisessa ja kehittämisessä. Tietoturvapolitiikkaa täydentävät Tietosuojaseloste omasta toiminnasta sekä yksityiskohtaiset määräykset ja ohjeet Intranetissa.

2. KATTAVUUS

Yritys Oy:n johtoryhmän vahvistama tietoturvapolitiikka kattaa kaikkeen toimintaan liittyvät tietojen käsittelyn tehtävät. Jokaisen työntekijän ja läheisessä yhteistyössä toimivien yritysten henkilökunnan sekä muiden tietojen ja tietojärjestelmien käyttäjän on tunnettava tämä tietoturvapolitiikka ja noudatettava sen perusteella annettuja ohjeita ja määräyksiä. Kumppaneiden, toimittajien ja muiden ulkopuolisten tahojen tulee myös sitoutua noudattamaan tätä tietoturvapolitiikkaa, kansallisia normeja sekä ohjeita ehtona tehtäviensä mukaiselle pääsylle yhtiöiden tietojärjestelmiin ja niiden sisältämiin tietoihin.

3. TIETOTURVA

Tietoturva tarkoittaa tietojen käsittelyn ja arkistoinnin turvaamista. Tietoturva rakentuu tiedon luottamuksellisuudesta, eheydestä, käytettävyydestä ja kiistämättömyydestä sekä tietojen käsittelyn valvonnasta. Tietoturvatyö on tietoturvan saavuttamiseksi tehtävien toimenpiteiden suunnittelua ja toteuttamista. Tietoturvaan kuuluvat tietoturvaryhmä, tietojen turvaamisen menetelmät, välineet ja toimenpiteet, työhön osoitetut resurssit sekä välineistön ja tilojen tietoturvaominaisuudet.

4. TIETOTURVAN TAVOITTEET

Yritys Oy:n tietoturvatyön päämäärä on turvata 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. Hyväksytyn tietoturvapolitiikan mukainen tietoturva tulee sisällyttää luonnollisena osana kaikkeen toimintaan. Tietoturvan kehittäminen ja ylläpito ovat osa yhtiöiden yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa.

5. ORGANISOINTI JA VASTUUT

Tietoturvaa johtaa ja valvoo johtoryhmä hallituksen valtuuttamana. Johtoryhmä päättää kokonaisturvallisuuden eri osa-alueiden kehittämistoiminnan tavoitteista, organisoinnista, resursseista ja toimintavaltuuksista sekä nimeää tietoturvavastaavan. Tietoturvan kehittämisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvallisesta toimintatavasta yrityksessä ja sen ostamissa palveluissa sekä raportoinnista vastaa saamiensa resurssien ja toimintavaltuuksien puitteissa tietoturvavastaava. Hän vastaa myös tietoturva-asioista tiedottamisesta yhtiöiden ulkopuolelle yleisellä tasolla. Tietoturvan kehittämisen suunnittelua ja toimeenpanon valmistelua varten yrityksessä toimii tietoturvaryhmä. Ryhmän jäsenten tehtävät kuvataan tarkemmin tiimin sisäisessä ohjeistuksessa.

Jokaisella tietojärjestelmällä on vastuuhenkilö. 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 liiketoimintayksikön vetäjä. Jokainen 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 tietoturvavastaavalle.

6. TIETOTURVAN TOTEUTUS

Tietoturvan toteuttamisen perusta on tämä johtoryhmän hyväksymä kirjallinen tietoturvapolitiikka, joka annetaan tiedoksi jokaiselle yhtiöiden työntekijälle ja tietojärjestelmien käyttäjälle. Tietoturva perustuu kansallisiin tietoturvaa, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin. Lainsäädännön ja ohjeistuksen muutokset otetaan huomioon tietoturvan kehittämisessä. Tietoturvan toteuttaminen ja ylläpito kuvataan Tietosuojaselosteessa.

Tietoturvan toteutus perustuu niihin vaatimuksiin, joita toiminta ja palvelut sekä kunkin tiedon ja tietojärjestelmän kriittisyysaste 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. Ne kuvataan tietosuojamallissa. Keskeiset kehittämistoimet toteutetaan hankkeina, joista tehdään hankesuunnitelma. Käyttäjien toimintaa ohjataan tietosuojamalliin sisältyvillä käyttösäännöillä sekä vahvistetuilla ja saatavilla olevilla

toimintaohjeilla sekä tietoturvakoulutuksella. Jokainen käyttäjä allekirjoittaa käyttäjän tietosuojaohjeen ja sitoumuksen saadessaan oikeuden tehtäviensä mukaiseen tietojärjestelmien käyttöön.

7. TIETOTURVAN SEURANTA JA VALVONTA

Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta tietoturvavastaavalle. Yksikön esimiehen tehtävänä on valvoa tietoturvan toteutumista omassa yksikössään. Tietoturvavastaavan tehtävänä on seurata ja valvoa tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.

LIITE 2: ESIMERKKI KÄYTTÄJIEN OHJEISTUKSESTA

1. OHJEEN TARKOITUS

Tätä ohjetta käytetään varmistamaan tietoturvaa Yritys Oy:n toiminnassa.

2. TIETOSUOJA

Noudata yrityksen kulloinkin voimassa olevia tietosuoja- ja tietoturvaohjeita.

Käsittele kaikkea henkilötietoja erityisen huolellisesti. Älä koskaan luovuta henkilötietoja kenellekään ulkopuoliselle taholle.

Älä kopioi tai tallenna ohjelmistoissa säilytettyä dataa omalle tietokoneelle, ulkoiselle muistille tai matkapuhelimeen. Tieto on yleensä parhaassa suojassa sille tarkoitetussa ohjelmassa.

Älä tulosta ohjelmistoissa tai muissa tallennuspaikoissa olevaa dataa. Jos joudut tulostamaan, niin huolehdi paperien turvallisesta käsittelystä ja hävittämisestä.

Älä kerää tai tallenna asiakkaiden tai muidenkaan henkilötietoja ilman selkeää käyttötarkoitusta, jonka yritys on hyväksynyt.

Kaikki tietopyyntöihin tai tietosuojaan liittyvät kysymykset pyydetään aina kirjallisena tieturvavastaavalle. Yksittäisen työntekijän ei tule ottaa asioihin kantaa vaan ohjata aina kyselyt yllä mainittuun osoitteeseen.

Tietosuojaan liittyen, jokaisen työntekijän tulee kiinnittää erityistä huomiota, yrityksen alueella ja tiloissa liikkuviin henkilöihin sekä estää ulkopuolisten pääsyä kiellettyihin paikkoihin.

Tietoturvaloukkaukset ja mahdolliset tietoturvaloukkaukset on ilmoitettava viipymättä tietoturvavastaavalle.

3. TIETOTURVAN KÄYTÄNNÖN TOIMENPITEET

Käytä työtehtävien hoitamiseen työnantajan laitteita.

Olet vastuussa tunnuksesi käytöstä. Suojaa hallussasi olevat tiedot, niin omat kuin yrityksen toimintaan liittyvät tiedot. Älä luovuta salasanaasi kenellekään toiselle.

Valitse salasana, jonka muistat itse helposti, mutta jota ulkopuoliset eivät pysty murtamaan. Älä käytä missään yrityksen ulkopuolisessa palvelussa samaa salasanaa kuin yrityksen palveluissa.

Huolehdi sähköpostin käsittelystä myös poissaolon aikana. Käytä tarvittaessa automaattivastauksia tai sovi kollegasi kanssa kuka lukee lomasi aikana sähköpostisi. Muista, että työnantaja voi tietyissä tilanteissa avata sähköpostisi ja etsiä yrityksen liiketoimintaan kuuluvia viestejä.

Älä avaa sähköpostiviestiä, jos et ole varma viestin alkuperästä. Viesti voi sisältää haittaohjelmia tai ohjata haittaohjelmia sisältävälle sivulle.

Varo kalasteluviestejä, joissa sinua pyydetään luovuttamaan tunnuksesi ja salasanasi tai kirjoittamaan ne jollekin verkkosivulle. Ulkopuoliset ylläpitäjät eivät koskaan kysy salasanaasi.

Varo kalastelusoittoja oudoista ulkomaisista puhelinnumeroista. Jos et odota puhelua ulkomaisesta puhelinnumerosta niin harkitse vastaamista. Jos puhelimesi hälyttää vain kerran, niin kyseessä voi olla huijaus, jossa sinua veloitetaan takaisinsoitosta.

Tarkista linkin todellinen kohdeosoite aina ennen klikkaamista. Ole erityisen varovainen, jos olet saanut linkin sähköpostiviestissä. Opettele erottamaan asialliset verkko-osoitteet huijareiden käyttämistä. Hyvä luotettavan linkin tuntomerkki on, että sen alussa on linkin lähettäneen yrityksen oma domainosoite, esimerkiksi www.elisa.fi/login/omaelisa/fi.

Tarkista palveluiden käyttöehdoista jo ennen palvelun käyttöönottoa ainakin tiedon omistajuuden säilyminen ja ettei tietoja luovuteta eteenpäin. Harkitse, mitä yrityksen tai omia tietoja viet verkkopalveluihin (Facebook, kuvienjakopalvelut ym.).

Haittaohjelmat leviävät tehokkaasti internet-palveluissa ja sosiaalisessa mediassa. Varo ponnahdusikkunoita, mainoksia ja kutsuja, älä klikkaile varomattomasti.

Huolehdi kotitietokoneesi suojaamisesta mm. palomuurin, haittaohjelmatorjunnan, varmuuskopioinnin ja ohjelmistopäivitysten avulla. Huolehdi myös älypuhelimesi ja mobiililaitteesi suojaamisesta mm. lukituskoodilla. Asenna tietokoneeseen ja mobiililaitteeseen vain ne ohjelmat, joita tarvitset. Haittaohjelmat leviävät tehokkaasti muistitikkujen välityksellä. Vältä muistitikkujen käyttöä tiedostojen siirtoon esimerkiksi kotitietokoneen ja työpaikan, tai yhteistyökumppaneiden välillä.

Älä käytä muistitikkua tai muuta siirrettävää muistilaitteita tiedostojen ensisijaisena tai ainoana tallennuspaikkana. Huolehdi siirrettävien muistilaitteiden turvallisuudesta ja vältä arkaluonteisen materiaalin tallentamista niille.

Jos tulostat yhteiskäytössä olevalle kirjoittimelle, nouda tuloste heti tulostamisen jälkeen.

Jos epäilet tietoturvarikkomusta tai järjestelmän väärinkäyttöä, ota yhteyttä tietoturvavastaavaan.

4. TIETOTURVAN KÄYTÄNNÖN TOIMENPITEET YRITYS OY:SSÄ VIERAILEVILLE HENKILÖILLE

Yritys Oy:n sisäverkkoa eivät saa käyttää vierailijat tai ulkopuoliset yhteistyökumppanit. Vierailijoille on erikseen oma vierailijaverkko.

Vierailijoiden tulee käyttää Yritys Oy:n tietojen käsittelyyn ainoastaan työkäyttöön tarkoitettuja laitteita, joissa on ajan tasalla oleva tietoturva.

Siirrettävien muistilaitteiden käytössä pitää noudattaa erityistä huolellisuutta ja molempien osapuolten virustorjunnan pitää olla päivittyneenä kun tietoa siirretään muistilaitteella.

LIITE 3: MALLIVIESTI YHTEISTYÖKUMPPANEILLE/ASIAKKAILLE TIETOTURVAHYÖKKÄYKSESTÄ TIEDOTTAMISEEN

Viestin aihe: *Yritys Oy:n* sähköpostiin kohdistunut tietoturvahyökkäys

Viesti:

Hyvä yhteistyökumppanimme,

x.x.2020 *Yritys Oy:n* sähköpostipalveluihin kohdistui tietoturvahyökkäys. Hyökkäyksessä lähetettiin sähköposteja otsikolla ”*tähän viestin otsikko*” ja viesteihin sisältyi linkki ”*tähän linkin teksti*” (mikäli viestissä oli linkki).

Viestit eivät ole *Yritys Oy:n* lähettämiä. Mikäli olet saanut kyseisen viestin, älä avaa viestiin sisältyvää linkkiä ja poista viesti muutoinkin sähköpostistasi. Mikäli olet jo avannut viestiin sisältyvän linkin, ole välittömästi yhteydessä omaan IT-organisaatioosi tai -palvelutoimittajaasi saadakseni tarkemmat toimintaohjeet.

Yritys Oy:n sähköpostipalveluiden ja IT-ympäristön turvallisuus on tarkistettu ja varmistettu erityistoimenpiteillä välittömästi tietoturvahyökkäyksen tultua ilmi. Hyökkääjä ei ole päässyt tekemään muuta vahinkoa kuin edellä kuvatun viestien lähetyksen.

Hyökkäyksen kulkua selvitetään parhaillaan tarkemmin tietoturva-asiantuntijoiden toimesta. Tietoturvahyökkäyksestä on tehty myös asianmukainen ilmoitus Kyberturvallisuuskeskukselle.

Pahoittelemme aiheetonta sähköpostiviestiä ja siitä mahdollisesti aiheutunutta hämmennystä tai vaivaa.

Allekirjoitus

LIITE 4: ESIMERKKI TIETOSUOJASELOSTEESTA (PROG-IT OY, NÄHTÄVISSÄ MYÖS WWW.PROG-IT.NET)

1. Yleistä

Prog-It Oy arvostaa asiakkaidensa, työntekijöidensä sekä sopimuskumppaniensa yksityisyyttä ja on sitoutunut suojaamaan niitä EU:n tietosuoja-asetusta noudattaen.

Tällä tietosuojaselosteella informoimme yllämainittuja tahoja heidän henkilötietojensa käsittelystä. Käyttääkseen Prog-It Oy:n palveluita, asiakkaiden ja sopimuskumppaneiden on hyväksyttävä tämän tietosuojaselosteen ehdot.

Halutessasi lisätietoa tietosuojakäytännöistämme tai henkilötietojen käsittelystä, vastaamme mielellämme kysymyksiinne. Yhteystietomme löydät täältä https://www.prog-it.net/ota-yhteytta/

2. Rekisterinpitäjä ja yhteystiedot

Käsiteltävien henkilötietojen rekisterinpitäjänä toimii:

Prog-It Oy (jäljempänä “Prog-It” tai ”me”)
Y-tunnus: 0968844-6
Rajatorpantie 8 A
01600 Vantaa

3. Mitä tietoja kerätään

Asiakkaidemme, työntekijöidemme, sopimuskumppaniemme, sekä tilintarkastajan itsensä, tai näiden valtuuttamien osapuolten antamat tiedot

- Tunnistamistiedot, kuten nimi, titteli ja valokuva
- Yhteystiedot, kuten postiosoite, sähköpostiosoite ja puhelinnumero
- Maksutiedot, kuten laskutustiedot, yhteyshenkilö ja muut laskutukseen liittyvät tiedot
- Palvelu- sekä toimitussopimusten tiedot, kuten yrityksen päättäjien tiedot, yhteyshenkilöt ja näiden yhteystiedot
- Asiakasprojektien tuottamiseen liittyvät tiedot kuten työtodistukset

Yllä mainittujen tietojen antaminen on pakollista asioidaksesi Prog-It:n kanssa ja käyttääksesi tarjoamiamme palveluita. Tietojen pääasiallinen lähde on käyttäjän itsensä antamat tiedot, minkä lisäksi saatamme saada lisätietoja yhteistyökumppaneiltamme, yleisesti saatavilla olevista internetlähteistä tai muista saatavilla olevista julkisista lähteistä.

Lisäksi pyydämme erikseen luvan suoramarkkinointiin.

4. Mihin tietoja käytetään

Henkilötietoja käytetään

- Työsuhteiden hallinta ja ylläpito
- Asiakassuhteiden ylläpito, asiakaspalvelu ja laskutus
- Sopimuskumppaneiden hallinta ja taloushallinto
- Tilintarkastus
- Prog-It:n omien palveluiden kehittämiseen

Tietoja käsitellään asiakkaidemme, työntekijöidemme, sopimuskumppaniemme, sekä tilintarkastajan ja Prog-It:n väliseen yllämainittujen henkilötietojen käsittelytarkoituksen toteuttamiseksi yllämainittujen ryhmien erilliseen nimenomaiseen suostumukseen tai lainsäädännön velvoitteisiin perustuen.

5. Miten tietoja suojataan ja säilytetään

Kaikki henkilötiedot ovat suojattu asiattomalta pääsyltä ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelemiseltä.

Prog-It säilyttää asiakastietoja EU:n tai ETA:n sisällä. Järjestelmien sekä palvelinten tekninen tietoturva noudattaa hyviä tietoturvakäytäntöjä. Palvelimet on suojattu tietomurtoja ja palvelunestohyökkäyksiä vastaan. Järjestelmät ovat suojattu pääsynhallinnalla.

Henkilötietojen käsittelyssä ja teknisissä ratkaisuissa noudatamme hyviä tietosuojakäytäntöjä. Kaikkea pääsyä henkilötietoon valvotaan hyvien käytäntöjen mukaisesti.

6. Kuka tietoja käsittelee

Henkilötietoihin on pääsy vain Prog-It:n omilla, palveluiden tuottamiseen osallistuvilla työntekijöillä. Henkilökunta on ohjeistettu ja koulutettu käsittelemään henkilötietoja turvallisesti.

Tarpeen mukaan käytämme luotettuja sopimuskumppaneita, jolloin tietoa voidaan siirtää kolmannelle osapuolelle. Kaikkien kumppanien kanssa on huomioitu EU:n tietosuoja-asetuksen asettamat vaatimukset.

7. Tietojen säilyttäminen

Säilytämme henkilötietoja vain tarvittavan ajan, jotta voimme täyttää selosteessa kuvatut käyttötarkoitukset. Tämän lisäksi joitain tietoja voidaan säilyttää kauemmin niiltä osin kuin se on tarpeen laissa asetettujen velvollisuuksien, kuten kirjanpitoa ja yritysten välistä kauppaa koskevien vastuiden toteuttamiseksi ja niiden asianmukaisen toteuttamisen osoittamiseksi.

Asiakkaan tai sopimuskumppanin pyynnöstä häntä koskevia henkilötietoja voidaan poistaa Prog-It:n järjestelmistä. Poistotoimenpide on peruuttamaton, emmekä voi palauttaa poistettuja henkilötietoja.

8. Asiakkaan oikeudet

Asiakkaalla on oikeus:

- Saada jäljennös henkilötiedoista
- Pyytää itseään koskevien henkilötietojen oikaisemista tai poistamista
- Tietyin edellytyksin pyytää käsittelyn rajoittamista tai vastustaa henkilötietojen käsittelyä

Lisäksi, jos käsittely perustuu erilliseen suostumukseen, asiakkaalla on mahdollisuus peruuttaa suostumus. Tämä ei kuitenkaan vaikuta ennen suostumuksen peruuttamista suoritettuun tietojen käsittelyn lainmukaisuuteen. Voit muuttaa suostumuksesi olemalla yhteydessä meihin. Pyynnön tulee olla riittävällä tavalla yksilöity, jotta voimme todentaa henkilöllisyytesi. Ilmoitamme sinulle, mikäli emme joiltain osin pysty toteuttamaan pyyntöäsi, kuten poistamaan kaikkia tietoja, joiden säilyttämiseen meillä on lakisääteinen velvollisuus tai oikeus.

9. Kuinka järjestelmään tallennetut tiedot saa

Voit pyytää Prog-It:n järjestelmiin tallennetut tiedot itsellesi ottamalla yhteyttä meihin. Yhteystietomme löytyvät osoitteesta: https://www.prog-it.net/ota-yhteytta/

10. Tietojen luovuttaminen kolmansille osapuolille

Voimme luovuttaa joitakin välttämättömiä tietoja kolmansille osapuolille oikean ja laadukkaan palvelun takaamiseksi. Tarvittaessa luovutamme tietoja myös viranomaisille. Informoimme tietopyynnöistä aina myös asiakasta, jos se on lain puitteissa sallittua.

Välitämme seuraavia tietoja kolmansille osapuolille:

- Sopimus- sekä laskutustiedot taloushallintoa ja tilintarkastusta varten
- Työsopimuksen tiedot ja palkkaan vaikuttavat tekijät taloushallintoa varten
- Yhteystietoja seuraavia palveluita varten

- Työterveys
- Vakuutukset
- Puhelinliittymät
- Markkinointi
- Rekrytointi
- Kulkuoikeudet
- Pysäköinti
- Koulutus
- Käyttöoikeus ulkopuolisiin palveluihin

Prog-It huolehtii tietoja siirrettäessä ja käsiteltäessä tietoturvan ja -suojan korkeasta tasosta EU:n Tietosuoja-asetuksen mukaisesti.

11. Tietosuojaselosteen muuttaminen

Palveluiden kehityksen ja lainsäädännön muutosten johdosta pidätämme oikeuden muuttaa tietosuojaselostetta. Merkittävistä muutoksista tietosuojaselosteeseen ilmoitetaan rekisteröityneille asiakkaille ehtojen päivityksen yhteydessä.