TIETOTURVAPOLITIIKKA

Sisällys

1. Johdanto

Tässä dokumentissa määritellään Mandatum-konsernin (jatkossa Mandatum) tietoturvapolitiikka (jatkossa politiikka). Mandatum-konserniin kuuluvat Mandatum Henkivakuutusosakeyhtiö ja Mandatum Asset Management Oy ja niiden omistamat yhtiöt. Politiikka koskee kaikkia Mandatumin työntekijöitä sekä niitä sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Mandatumin tietoja. Ulkoisten sidosryhmien kuten alihankkijoiden ja palvelutoimittajien osalta tämän politiikan vaatimukset sisällytetään soveltuvilta osin hankintasopimuksiin.

Politiikka on Mandatumin tietoturvatyötä ohjaava dokumentti. Politiikkaa voidaan tarkentaa ja täydentää tietoturvaperiaatteilla ja -ohjeilla, jotka saatetaan työntekijöiden sekä oleellisten kolmansien osapuolien tietoon. Periaatteet ja ohjeet eivät saa olla ristiriidassa politiikan kanssa.

2. Tarkoitus ja tavoitteet

Politiikan tarkoituksena on määritellä tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot Mandatumissa. Politiikan tavoitteena on osaltaan varmistaa, että Mandatumin tiedot, palvelut, tietojärjestelmät ja tietoliikenne on suojattu ja varmistettu sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturvallisuus kattaa kaikki Mandatumin tiedot ja tietojenkäsittelyn, sisältäen arkistoinnin.

Tietoturvallisuuden tavoitteet Mandatumissa ovat:

Asiakaslähtöisyys

Asiakkaiden tiedot ovat asianmukaisesti suojattu ja asiakkaille tarjottavat palvelut ovat tietoturvallisia.

Liiketoimintalähtöisyys

Tietoturvallisuus on osa laadukkaiden palveluiden kehittämistä, palveluiden digitalisaatiota ja datalähtöistä liiketoimintaa sekä positiivista asiakaskokemaa.

Tietoturvallisuuden jatkuva parantaminen

Tietoturvallisuuden jatkuvalla parantamisella varmistetaan, että tietoturvallisuuden taso on riittävä liiketoiminnan luonteeseen ja laajuuteen, tietoihin ja tietojärjestelmiin kohdistuviin uhkiin sekä yleiseen tekniseen kehitystasoon nähden. Tietoturvallisuus täyttää lainsäädännön ja viranomaisten asettamat vaatimukset ja velvoitteet sekä vastaa ulkoisten sidosryhmien finanssialan toimijalta yleisesti odottamaa tasoa.

3. Organisointi ja vastuut

3.1 Hallitus ja toimitusjohtaja

Yhtiöiden hallitukset ja toimitusjohtajat vastaavat siitä, että Mandatumin tietoturvallisuus on riittävällä tasolla, ja että tietoturvallisuudelle asetetaan riittävät resurssit. Mandatum Henkivakuutusosakeyhtiö ja Mandatum Asset Management Oy:n hallitukset hyväksyvät tietoturvapolitiikan ja hallituksilla on ylin vastuu tietoturvapolitiikan noudattamisesta.

3.2 Liiketoiminnan johtoryhmät

Mandatum Henkivakuutusosakeyhtiön ja Mandatum Asset Management Oy:n liiketoiminnan johtoryhmät käsittelevät ja liiketoiminnan johtoryhmien puheenjohtajat hyväksyvät tietoturvapäällikön esityksestä tietoturvallisuutta koskevat periaatteet ja strategian.

3.3 Tietoturvallisuus- ja kyberriskien komitea

Tietoturvallisuus- ja kyberriskien komitea varmistaa, että operatiivisten riskien hallinta konsernissa on järjestetty asianmukaisesti tietoturvallisuus- ja kyberriskien alueella. Komitea varmistaa, että yhteistyö ja tiedonkulku tietoturvallisuus- ja kyberriskeistä liiketoiminta- sekä tukiyksiköiden ja ohjaustoimintojen välillä on saumatonta.

3.4 Organisaatioyksiköt

Jokainen organisaatioyksikkö (jatkossa yksikkö) vastaa oman organisaationsa ja hankkimiensa palvelujen tietoturvallisuudesta tietoturvapolitiikan, -periaatteiden ja -ohjeiden mukaisesti. Yksiköt ovat vastuussa tietoturvallisuudesta myös sisäisen valvonnan politiikan mukaisesti. Yksiköt konsultoivat Mandatumin tietoturvatiimiä Mandatumin tietoturvallisuutta koskevissa asioissa, esimerkiksi tietoturvallisuuteen vaikuttavissa hankkeissa ja palveluhankinnoissa.

3.4.1 Henkilöstöyksikkö

Henkilöstöyksikkö vastaa henkilöstö- ja toimitilaturvallisuudesta, työsuhde- ja perehdytysprosesseista sekä esimiesten ohjeistamisesta em. asioissa.

3.4.2 Business Technologies -yksikkö

Business Technologies -yksikkö (jatkossa BT-yksikkö) vastaa teknisen tietoturvallisuuden kehittämishankkeiden toimeenpanosta ja BT-yksikön vastuulla olevien tietoturvapalvelujen ylläpidosta ja valvonnasta.

3.5 Tietoturvatiimi

Tietoturvatiimi vastaa Mandatumin tietoturvatason seurannasta (ml. kyberturvallisuus) ja tietoturvapoikkeamien käsittelystä. Lisäksi tietoturvatiimi nostaa esille tietoturvallisuuteen liittyviä kehittämistarpeita ja edistää niiden toteutumista.

Tietoturvatiimi tukee ja ohjeistaa yksikköjä tietoturvallisuuteen liittyvissä asioissa.

Tietoturvatiimi toteuttaa tietoturva-arviointeja ja -tarkastuksia osana palveluhankintoja ja tietoturvatason seurantaa.

3.5.1 Tietoturvapäällikkö (engl. Chief Information Security Officer, CISO)

Tietoturvapäällikkö vastaa tietoturvatiimin operatiivisesta johtamisesta ja antaa tietoturvapolitiikan ja -periaatteiden mukaisia linjauksia ja lausuntoja sekä hyväksyy tietoturvaohjeet. Tietoturvapäällikkö vastaa tietototurvallisuutta koskevien politiikkojen, periaatteiden ja tietoturvastrategian tuottamisesta ja ylläpidosta, ja valvoo niiden toteutumista.

Tietoturvapäällikkö vastaa siitä, että tietoturvallisuuden hallintajärjestelmä on ISO 27001:n vaatimusten mukainen.

3.5.2 Kyberturvallisuuspäällikkö (engl. Cyber Security Manager)

Kyberturvallisuuspäällikkö suorittaa tietoturvan valvontaa kyberuhkien ja -riskien tunnistamiseksi. Kyberturvallisuuspäällikkö koordinoi kyberturvaa koskevien poikkeamien käsittelyä. Kyberturvallisuuspäällikkö osallistuu liiketoiminnan ja muiden sidosryhmien tietoturvaa koskettaviin hankkeisiin ja suosittelee tietoturvan kannalta hyviä toiminta- ja toteutustapoja.

3.6 Henkilöstö ja toimeksiannosta työskentelevät

Jokainen Mandatumin palveluksessa oleva henkilö tai Mandatumin toimeksiannosta työskentelevä on velvollinen noudattamaan tietoturvapolitiikkaa, -periaatteita ja -ohjeita sekä huolehtimaan lainsäädännössä kulloinkin asetettujen tietoturva- ja tietosuojavelvoitteiden sekä vakuutussalaisuus- ja muiden salassapitovelvoitteiden noudattamisesta.

3.6.1 Esimiehet

Esimiehet vastaavat siitä, että työntekijät suorittavat henkilöstölle suunnatut tietoturvaperehdytykset- ja koulutukset, ja että työntekijät ovat tietoisia tietoturvapolitiikasta ja -periaatteista, ja työtehtävien kannalta keskeisistä tietoturvaohjeista.

Esimiehet vastaavat siitä, että jokaisella Mandatumin toimeksiannosta työskentelevällä ja Mandatumin käyttäjätunnukset omaavalla henkilöllä on esimiesasemassa oleva vastuuhenkilö, ja että toimeksiannosta työskentelevät ovat tietoisia tietoturvapolitiikasta ja -periaatteista, ja työtehtävien kannalta keskeisistä tietoturvaohjeista.

Esimiehet vastaavat myös siitä, että jokainen työntekijä tai Mandatumin toimeksiannosta työskentelevä henkilö on salassapitovelvollinen.

4. Toteutuskeinot

4.1 Tietoturvallisuuden tason arviointi

Tietoturvallisuuden tasoa on arvioitava jatkuvasti sovittujen roolien mukaisesti huomioiden Mandatumin keskeiset toiminnot, resurssit ja käsiteltävät tiedot sekä niihin kohdistuvat uhat, uhkien todennäköisyys ja uhkien toteutumisen vaikutus. Havaitut puutteet on käsiteltävä ja tehtävä riittävät toimenpiteet riskien hallitsemiseksi.

4.2 Tietoturvariskien hallinta

Tietoturvariskien ja -poikkeamien tunnistamiseen on oltava riittävät tekniset ja hallinnolliset valmiudet. Erityisesti on kiinnitettävä huomiota tietoturvariskeihin, jotka kohdistuvat asiakkaiden tietoihin. Tunnistetut tietoturvariskit on käsiteltävä ja raportoitava säännönmukaisesti osana operatiivisten riskien hallintaa.

Tietoturvasta raportoidaan säännöllisesti tietoturvallisuus- ja kyberriskien komitealle, riskienhallintakomitealle sekä muille sidosryhmille osana riskienhallinnan kvartaaliraportointia.

4.3 Tietojen turvaaminen

Mandatumin liiketoiminnan kannalta keskeisillä tiedoilla on oltava tiedonhallintapolitiikan mukaisesti määritetyt omistajat, jotka ovat vastuussa tietojen turvaamisesta huomioiden tietojen luottamuksellisuus ja merkittävyys liiketoiminnalle koko tietojen elinkaaren ajan.

4.4 Palveluiden ja tietojärjestelmien turvaaminen

Tietojärjestelmien turvaaminen

Sisäisillä ja ulkoisilla tietojärjestelmillä (mukaan lukien pilvipalvelut) on oltava nimetyt vastuuhenkilöt. BT-yksikön vastuulla olevien tietojärjestelmien vastuuhenkilöt nimittää BT-yksikön johtaja. Vastaavasti muiden yksiköiden vastuulla olevien tietojärjestelmien vastuuhenkilöt nimittää kunkin yksikön johtaja.

Tietojärjestelmien vastuuhenkilöt ovat vastuussa tietojärjestelmien turvaamisesta yhdessä tietojen omistajien kanssa huomioiden tietojärjestelmillä käsiteltävien tietojen luottamuksellisuus ja merkittävyys Mandatumin liiketoiminnalle.

Palveluiden ja tietojärjestelmien kehittäminen ja hankkiminen

Palveluiden ja tietojärjestelmien kehittämisen ja hankkimisen yhteydessä on vastuuhenkilön huolehdittava etupainotteisesti tietoturvariskien tunnistamisesta ja käsittelystä suhteutettuna palvelun tai tietojärjestelmän merkitykseen Mandatumin liiketoiminnalle ja strategialle, ja sen vaikutuksiin Mandatumin tietoverkoille ja IT-arkkitehtuurille. Vastuuhenkilön tulee tarvittaessa konsultoida Mandatumin tietoturvatiimiä ja BT-yksikköä, ja toimia muiden soveltuvien politiikkojen, kuten hankinta-, tietosuoja- ja ulkoistamispolitiikkojen mukaisesti.

Tietojärjestelmätapahtumien jäljitettävyys

Palveluja ja tietojärjestelmiä kehitettäessä on varmistettava, että liiketoiminnan kannalta merkittävistä tapahtumista ja erityisesti henkilötietojen käsittelystä tehdään lokikirjaus ja tapahtumat ovat jäljitettävissä lokikirjaamista koskevien periaatteiden mukaisesti.

Pääsynvalvonta ja käyttövaltuudet

Tietojärjestelmiin pääsyä on valvottava.

Käyttövaltuudet tietoihin ja tietojärjestelmiin on myönnettävä ja niiden käyttöä valvottava käyttövaltuusperiaatteiden mukaisesti. Käyttövaltuuksien tulee määräytyä työperusteisen tarpeen perusteella.

4.5 Digitaalisen liiketoiminnan turvaaminen

Digitaaliseen ja datalähtöiseen liiketoimintaan liittyvät tietoturvariskit on huomioitava palvelujen kehityksessä ja ylläpidossa, ja niitä on arvioitava jatkuvasti. Lisäksi on toteutettava riittävät toimenpiteet erilaisten häiriöiden ja väärinkäytösten minimoimiseksi.

4.6 Kyberturvallisuuden toteuttaminen

Kyberturvallisuus on huomioitava kaikessa tekemisessä. Erityisesti on kiinnitettävä huomiota kyberuhkien ja -riskien tunnistamiseen sekä niitä koskevien havaintojen viiveettömään käsittelyyn.

Kyberturvallisuutta koskevien suojaustoimenpiteiden on oltava riittäviä ja hyvien tietoturvakäytäntöjen mukaisia, ja suojaustoimenpiteiden toteuttamisessa on pyrittävä mahdollisuuksien mukaan kerrokselliseen suojaamiseen.

4.7 Jatkuvuudenhallinta ja varautuminen

Mandatumilla on oltava jatkuvuussuunnitelma erilaisten häiriöiden ja poikkeusolojen varalle. Jatkuvuussuunnitelmalla tulee olla nimetty omistaja, joka huolehtii jatkuvuussuunnitelman ajan tasalla pitämisestä ja testaamisesta.

4.7.1 Tietoturvaloukkauksista ilmoittaminen

Tietoturvaloukkausten ilmoittamiseen tulee olla välineet ja toimiva prosessi sekä toimintaohjeet, huomioiden lainsäädännön ja viranomaisten asettamat vaatimukset tietoturvaloukkausten ilmoitusvelvollisuutta koskien.

4.8 Tietoturvatietoisuuden ja -osaamisen varmistaminen

Työntekijöiden tietoturvatietoisuudesta ja -osaamisesta on varmistuttava tietoturvakoulutuksen ja -ohjeistuksen avulla. Koulutuksen sisällöstä vastaa tietoturvatiimi.

Kolmansien osapuolien tietoturvatietoisuudesta ja -osaamisesta on varmistuttava sopimuksin ja niihin liitetyin ohjeistuksin sekä mahdollisuuksien mukaan koulutuksen avulla.

4.9 ISO 27001 -sertifioinnin vaatimusten täyttäminen

Mandatumin on täytettävä ISO 27001 -sertifioinnin asettamat vaatimukset tietoturvallisuuden hallintajärjestelmän soveltamisalan mukaisesti ja sitouduttava hallintajärjestelmän jatkuvaan parantamiseen.

5. Viestintä

Tietoturvapolitiikka, -periaatteet, ja -ohjeet julkaistaan Mandatumin Intranetissä. Lisätietoja politiikan soveltamisesta antaa Mandatumin tietoturvatiimi.

Sisäisestä tiedottamisesta tietoturva-asioissa vastaa ensisijaisesti tietoturvatiimi. Varalla toimii Data Governance -yksikön johtaja.

Ulkoisessa tiedottamisessa noudatetaan Mandatumin viestintäpolitiikkaa. Mandatumin tietoturvallisuutta koskevat asiat eivät ole lähtökohtaisesti julkisia, ja ulkoista tiedottamista tulee aina edeltää tietoturvapäällikön, tietoturvatiimin asiantuntijan tai Data Governance -yksikön johtajan kanssa käyty konsultaatio.

6. Valvonta ja rikkomukset

Tietoturvapäällikkö valvoo politiikan noudattamista ja käsittelee politiikkaa koskevat rikkomukset yhdessä esimiesten ja Mandatumin toimivan johdon kanssa. Politiikan tai

sen perusteella laadittujen ohjeiden rikkominen voi johtaa Työsopimuslain (55/2001) seuraamuksiin.

Yksiköt vastaavat politiikan noudattamisesta omissa yksiköissään.

Alihankkijoiden ja palvelutoimittajien osalta vastuu valvonnasta on alihankkijan tai palvelutoimittajan toimintaa ohjaavalla Mandatumin edustajalla.

Muu mahdollinen valvonta tapahtuu sopimusten sallimalla tavalla lain puitteissa.

Tämän lisäksi jokaisella Mandatumin palveluksessa olevalla henkilöllä tai Mandatumin toimeksiannosta työskentelevällä on velvollisuus seurata politiikan noudattamista. Epäillystä rikkomuksesta, väärinkäytöksestä tai tietoturvapuutteista tulee raportoida tietoturvapäällikölle.

7. Poikkeamat

Politiikasta voidaan poiketa, jos politiikasta poikkeamiselle on vahva liiketoiminnallinen peruste, edellyttäen kuitenkin, ettei lainsäädännössä asetettua salassapitovelvollisuutta vaaranneta. Poikkeamasta ilmoitetaan tietoturvapäällikölle, joka arvioi poikkeamaan liittyvät riskit ja antaa tarvittaessa toimintaohjeita. Jos kyse on tietoturvapäällikön arvion mukaan merkittävästä poikkeamasta, poikkeamapäätöksen tekee Mandatumin toimitusjohtaja.

8. Muutokset

Tietoturvapäällikkö valmistelee politiikkaan tehtävät muutokset. Mandatum Henkivakuutusosakeyhtiö ja Mandatum Asset Management Oy:n hallitukset hyväksyvät politiikan vuosittain.