MANDATUM

Tietoturvapolitiikka

Mandatum-konserni

13.8.2024

Sisällys

1 MÄÄRITELMÄT

"**BT-yksikkö**" tarkoittaa Mandatum-konsernin Business Technologies -yksikköä.

"**CISO**" tarkoittaa Mandatum-konsernin Chief Information Security Officeria.

"**Henkilöstöyksikkö**" tarkoittaa Mandatum-konsernin henkilöstöyksikköä.

"**Kyberturvallisuudella**" tarkoitetaan järjestelyjä, joiden tavoitteena on tietojenkäsittelyteknologiaan perustuva digitaalisen ja verkottuneen toimintaympäristön turvaaminen.

"**Mandatum**" tai "**Konserni**" tarkoittaa Mandatum Oyj:tä yhdessä sen kaikkien tytäryhtiöiden kanssa (kukin "**Konserniyhtiö**").

"**Politiikka**" tarkoittaa tätä asiakirjaa.

"**Tietoturvallisuudella**" tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon saatavuus, eheys, aitous ja luottamuksellisuus. Saatavuudella tarkoitetaan sitä, että tieto on käytettävissä haluttuna aikana. Eheydellä tarkoitetaan tiedon yhtenäisyyttä alkuperäisen tiedon kanssa (esim. tietoa siirrettäessä). Aitoudella tarkoitetaan, että tieto ei ole vääristynyt sen luomisen jälkeen ja että tiedot ovat peräisin luotettavasta lähteestä, eli niitä ei ole luotu hyökkääjän tai muun tunkeutujan toimesta. Luottamuksellisuudella tarkoitetaan sitä, että tieto on vain niiden henkilöiden ja tahojen saatavilla, joille se on tarkoitettu (esim. työtehtävät, asiakkuus- tai palvelusopimus).

2 JOHDANTO

2.1 Tausta ja tarkoitus

Tässä asiakirjassa määritellään Mandatum-konsernin tietoturvapolitiikka ("**Politiikka**"). 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 tiedon koko elinkaaren luomispäivästä tuhoamiseen asti.

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 toimijoilta yleisesti odottamaa tasoa.

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

2.2 Soveltamisala

Tämä Politiikka koskee kaikkia Mandatumin Konserniyhtiöitä ja niiden työntekijöitä sekä niitä sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Mandatumin tietoja. Ulkoisten sidosryhmien kuten alihankkijoiden ja palveluntarjoajien osalta tämän Politiikan vaatimukset sisällytetään soveltuvin osin hankintasopimuksiin.

3 ORGANISOINTI JA VASTUUT

3.1 Hallitukset ja toimitusjohtajat

Mandatumin Konserniyhtiöiden hallitukset ja toimitusjohtajat ovat vastuussa siitä, että Mandatumin tietoturvallisuus on korkealla tasolla, ja että tietoturvallisuudelle varataan riittävät resurssit. Mandatum Oyj:n hallitus hyväksyy Politiikan vuosittain ja kantaa ylimmän vastuun Politiikan noudattamisesta.

3.2 Tietoturvallisuus- ja kyberriskien komitea

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

Komitea hyväksyy Mandatum-konsernin riskienhallinnassa käytössä olevat tietoturvariskitasot.

Tietoturvallisuus- ja kyberriskien komitea käsittelee, ja komitean puheenjohtaja hyväksyy, CISO:n esityksestä tietoturvallisuutta koskevat periaatteet ja strategian.

3.3 Ensimmäisen linjan toiminnot

Ensimmäisen linjan toiminnoilla viitataan liiketoimintayksikköihin ja muihin tukitoimintoihin, kuten Henkilöstö- ja BT-yksikköihin, jotka tukevat liiketoimintaa tavoitteiden saavuttamisessa.

Jokainen organisaatioyksikkö vastaa oman organisaationsa ja hankkimiensa palveluiden tietoturvallisuudesta Politiikan ja tietoturvaperiaatteiden ja -ohjeiden sekä muiden soveltuvien Mandatum-konsernin tietoturvallisuutta koskevien politiikoiden ja linjausten mukaisesti. Yksiköt konsultoivat Mandatumin tietoturvaorganisaatiota Mandatumin tietoturvallisuutta koskevissa asioissa, esimerkiksi tietoturvallisuuteen vaikuttavissa hankkeissa ja palveluhankinnoissa.

Henkilöstöyksikkö

Mandatum-konsernin Henkilöstöyksikkö vastaa henkilöstö- ja toimitilaturvallisuudesta, työsuhde- ja perehdytysprosesseista sekä esihenkilöiden ohjeistamisesta edellä mainituissa asioissa.

Business Technologies -yksikkö

BT-yksikkö vastaa teknisen tietoturvallisuuden kehittämishankkeiden ja tietoturvallisuuden hallintajärjestelmän (ISMS) toimeenpanosta sekä BT-yksikön vastuulla olevien tietoturvapalveluiden ylläpidosta ja valvonnasta.

Ensimmäisellä ja toisella linjalla on omat tietoturvallisuusroolinsa. BT-yksikön roolit ovat:

(a) Cyber Security Manager

Cyber Security Manager suorittaa tietoturvan valvontaa kyberuhkien ja -riskien tunnistamiseksi ja koordinoi kyberturvaa koskevien poikkeamien käsittelyä. Cyber Security Manager on vastuussa kyberturvallisuuden kehittämisestä ja osallistuu liiketoiminnan ja muiden sidosryhmien tietoturvaa koskeviin hankkeisiin ja suosittelee tietoturvan kannalta hyviä toiminta- ja toteutustapoja.

(b) Information Security Manager

Information Security Manager suorittaa tietoturvan valvontaa tietoturvauhkien ja -riskien tunnistamiseksi ja koordinoi tietoturvaa koskevien poikkeamien käsittelyä. Information Security Manager on vastuussa tietoturvaa koskevien prosessien kehittämisestä ja osallistuu liiketoiminnan ja muiden sidosryhmien tietoturvaa koskeviin hankkeisiin ja suosittelee tietoturvan kannalta hyviä toiminta- ja toteutustapoja.

3.4 Toisen linjan toiminnot

Toisen linjan toiminnoilla viitataan Konsernin riskienhallinta- ja compliance-toimintoihin.

Konsernin riskienhallintatoiminto vastaa riskien asianmukaisesta tunnistamisesta, arvioinnista ja hallinnasta koko niiden elinkaaren ajan. Konsernin riskienhallintatoiminto tukee myös liiketoimintayksikköjä riskien tunnistamisessa, arvioinnissa ja hallinnassa. Konsernin riskienhallintatoiminnon tietoturva- ja data-asioita johtava Konsernin Chief Information Security Officer (CISO) on vastuussa Mandatumin tietoturvallisuudesta ja liiketoiminnan jatkuvuuden suunnittelusta, turvallisuustason (mukaan lukien kyberturvallisuus) seurannasta ja tietoturvaa koskevien poikkeamien käsittelystä. Se suorittaa tietoturva-arviointeja ja tarkastuksia sekä korostaa tietoturvaan liittyviä kehitystarpeita ja edistää niiden implementointia.

Mandatumissa compliance-riskit on integroitu osaksi Mandatum-konsernin riskienhallintapolitiikassa määriteltyä operatiivisten riskien viitekehystä. Tietosuojan ja henkilötietojen käsittelyn osalta Konsernin compliance-toiminto käsittelee niihin liittyviä compliance-riskejä. Konsernin compliance-toiminto on vastuussa riskienhallinnan viitekehyksen ylläpidosta tietosuojaan liittyvien compliance-riskien riippumatonta arviointia varten. Konsernin tietosuojavastaava (DPO) on osa toimintoa. Tietosuojavastaavan tehtävät on kuvattu yksityiskohtaisesti Mandatum-konsernin tietosuojapolitiikassa.

3.5 Henkilöstö ja toimeksiannosta työskentelevät

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

Esihenkilöt

Esihenkilöt vastaavat siitä, että työntekijät suorittavat henkilöstölle suunnatut tietoturvaperehdytykset- ja koulutukset, ja että työntekijät ovat tietoisia Politiikasta ja tietoturvaperiaatteista -ja ohjeista, jotka ovat keskeisiä heidän työtehtäviensä kannalta.

Esihenkilöt vastaavat siitä, että jokaisella Mandatumin toimeksiannosta työskentelevällä ja Mandatumin käyttäjätunnukset omaavalla henkilöllä on esihenkilöasemassa oleva vastuuhenkilö, ja että toimeksiannosta työskentelevät ovat tietoisia Politiikasta ja tietoturvaperiaatteista ja -ohjeista, jotka ovat keskeisiä heidän työtehtäviensä kannalta.

Esihenkilöt 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 soveltuvin osin muille hallintoelimille osana riskienhallinnan kvartaaliraportointia.

Riskienhallintaan liittyvät keskeiset roolit on määritelty riskienhallintapolitiikoissa. Tietoturvariskien hallintaan sovelletaan edellä mainittujen lisäksi tätä Politiikkaa.

4.3 Tietojen turvaaminen

Mandatumin liiketoiminnan kannalta keskeisillä tiedoilla on oltava Mandatum-konsernin sisäisen tiedonhallintapolitiikan mukaisesti määritetyt omistajat, jotka ovat vastuussa tietojen turvaamisesta huomioiden tietojen luottamuksellisuus, eheys, saatavuus 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 ennakoivasti 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 tietoturva-asiantuntijoita ja BT-yksikköä, ja toimia muiden soveltuvien politiikoiden, kuten hankinta-, tietosuoja- ja ulkoistamispolitiikoiden mukaisesti.

Tietojärjestelmätapahtumien jäljitettävyys

Palveluita 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 palveluiden 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 viivytyksettömään 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.

4.8 Tietoturvaloukkauksien hallinta

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

4.9 Tietoturvatietoisuuden ja -osaamisen varmistaminen

Työntekijöiden tietoturvatietoisuudesta ja -osaamisesta on varmistuttava ohjeiden ja säännöllisen koulutuksen avulla. Koulutuksen sisällöstä vastaa tietoturvatiimi.

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

4.10 ISO 27001 -sertifioinnin vaatimusten täyttäminen

Mandatumin on täytettävä ISO 27001:2022 -sertifioinnin asettamat vaatimukset tietoturvallisuuden hallintajärjestelmän soveltamisalan mukaisesti ja sitouduttava hallintajärjestelmän jatkuvaan parantamiseen.

5 VIESTINTÄ

Politiikka julkaistaan Mandatumin verkkosivuilla ja intranetissä. Politiikkaa täydentävät periaatteet ja ohjeet eivät ole julkisia, ja ne ovat Mandatumin työntekijöiden saatavilla Mandatumin intranetissä ja/tai tuodaan muiden osapuolten tietoisuuteen tarvittaessa. Lisätietoja Politiikan soveltamisesta antaa CISO. Sisäisestä tiedottamisesta tietoturva-asioissa vastaa ensisijaisesti CISO.

Ulkoisessa tiedottamisessa noudatetaan Mandatumin tiedonantopolitiikkaa. Mandatumin tietoturvallisuutta koskevat asiat eivät ole lähtökohtaisesti julkisia, ja ulkoista tiedottamista tulee aina edeltää CISO:n tai muun tietoturvaorganisaation asiantuntijan kanssa käyty konsultaatio.

6 VALVONTA JA RIKKOMUKSET

CISO valvoo politiikan noudattamista ja käsittelee Politiikkaa koskevat rikkomukset yhdessä esihenkilöiden ja Mandatumin toimivan johdon kanssa. Politiikan tai sen perusteella laadittujen ohjeiden rikkominen voi johtaa työsopimuslain (55/2001, muutoksineen) mukaisiin 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 ja lain puitteissa.

Tämän lisäksi jokaisella Mandatumin palveluksessa olevalla henkilöllä tai Mandatumin toimeksiannosta työskentelevällä on velvollisuus noudattaa politiikan vaatimuksia. Epäillystä rikkomuksesta, väärinkäytöksestä tai tietoturvapuutteista tulee raportoida CISO:lle.

7 POLITIIKAN TARKISTAMINEN JA PÄIVITTÄMINEN

Politiikan sisällön ajantasaisuutta arvioidaan tarvittaessa ja vähintään vuosittain CISO:n toimesta. CISO on vastuussa Politiikkaan tehtävien päivitysten tai muutosten valmistelusta. Politiikka esitetään Mandatum Oyj:n hallituksen hyväksyttäväksi vähintään vuosittain.

8 POLITIIKAN KIELI

Tämä Politiikka on laadittu suomen- ja englanninkielisenä. Mahdollisessa ristiriitatilanteessa suomenkielinen versio on määräävä.

MANDATUM

Mandatum Oyj

Rekisteröity kotipaikka ja osoite:
Bulevardi 56, 00120 Helsinki, Suomi

Y-tunnus: 3355142-3

www.mandatum.fi