INFORMATION SECURITY POLICY

Synopsis	The purpose of the policy is to lay down the objectives, responsibilities and means of securing information at Mandatum. The objective of the policy is to ensure that Mandatum's information, services, information systems and data communications systems are protected and secured in both normal and emergency conditions through administrative, technical and other means. Information security encompasses all of Mandatum's information and information processing, including archiving.			
Policy hierarchy	Sampo Group policy (parent level)	Mandatum Group policy (group level)	Mandatum Company policy (company level)	Affirmed guidelines (employee level)
	Sampo Group Information Security Principles	This policy	-	-
Scope of the policy	Companies	Operations	Employees	
	Mandatum Life and MAM as well as their subsidiaries	All operations	All employees	
Policy owner	Data Governance			
Approved by	▪ Board of Directors of Mandatum Life, 8 February 2023 ▪ Board of Directors of MAM, 7 February 2023			
Last updated by	Vesa Tupala, 11 January 2023			
Purpose of the update	Annual review			
Regular review interval	Annual			
Relating policies	▪ Mandatum Group's Information Management Policy ▪ Mandatum Group's Data Protection Policy			
Applicable regulation	▪ ISO 27001			

In case of any discrepancy between this summary and the policy, the policy text shall prevail.

INFORMATION SECURITY POLICY

Contents

1 Johdanto

1.1 Tausta ja tarkoitus

Tässä dokumentissa määritellään Mandatum Henkivakuutusosakeyhtiön ja Mandatum Asset Management Oy:n sekä näiden omistamien tytäryhtiöiden (jatkossa yhdessä Mandatum) Tietoturvapolitiikka (jatkossa 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 arkistoinnin.

Tietoturvallisuudella tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuudella tarkoitetaan sitä, että tieto on käytettävissä haluttuna aikana. Eheydellä tarkoitetaan tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa (esim. tietoa siirrettäessä). Luottamuksellisuudella tarkoitetaan sitä, että tieto on vain niiden henkilöiden ja tahojen saatavilla, joille se on tarkoitettu (esim. työtehtävät, asiakkuus- tai palvelusopimus).

Kyberturvallisuudella tarkoitetaan järjestelyjä, joiden tavoitteena on tietojenkäsittelyn teknologiaan perustuva digitaalisen ja verkottuneen toimintaympäristön turvaaminen.

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.

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.

Politiikasta on laadittu englanninkielinen käännös. Mikäli kieliversioiden välillä on ristiriitaisuutta, suomenkielinen versio on määräävä.

1.2 Soveltamisala

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.

2 Organisointi ja vastuut

2.1 Hallitus ja toimitusjohtaja

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

2.2 Group Committee

Mandatum Group Committee käsittelee ja puheenjohtaja hyväksyy Mandatum Group CISOn esityksestä tietoturvallisuutta koskevat periaatteet ja strategian.

2.3 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.

Komitea hyväksyy konsernin riskienhallinnassa käytössä olevat hyväksytyt tietoturvariskitasot. Ajantasaiset tietoturvariskitasot dokumentoidaan Tietoturvariskitasot-dokumenttiin (Tietoturvariskitasot.ppt).

2.4 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 tietoturvaorganisaatiota Mandatumin tietoturvallisuutta koskevissa asioissa, esimerkiksi tietoturvallisuuteen vaikuttavissa hankkeissa ja palveluhankinnoissa.

2.4.1 Henkilöstöyksikkö

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

2.4.2 Business Technologies -yksikkö

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

2.5 Tietoturvaorganisaatio

Ensimmäisellä ja toisella puolustuslinjalla on omat tietoturvaorganisaationsa. Operatiivinen tietoturvatyö on Business Technologies -yksikön vastuulla, joka suunnittelee ja toteuttaa tietoturvaan liittyviä teknisiä ratkaisuja ja hallinnan prosesseja.

Riskienhallintatoiminnon tietoturvaorganisaatio vastaa Mandatumin tietoturvallisuuden ohjaamisesta sekä tietoturvatason seurannasta (ml. kyberturvallisuus) ja tietoturvapoikkeamien käsittelystä. Se toteuttaa tietoturva-arviointeja ja -tarkastuksia sekä nostaa esille tietoturvallisuuteen liittyviä kehittämistarpeita ja edistää niiden toteutumista.

2.5.1 CISO (Chief Information Security Officer)

Mandatum konsernin CISO johtaa tietoturvallisuutta ja antaa tietoturvapolitiikan ja -periaatteiden mukaisia linjauksia ja lausuntoja sekä hyväksyy tietoturvaohjeet. CISO vastaa tietototurvallisuutta koskevien politiikkojen, periaatteiden ja tietoturvastrategian tuottamisesta ja ylläpidosta, ja valvoo niiden toteutumista.

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

2.5.2 Cyber Security Manager

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

2.5.3 Information Security Manager

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

2.6 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.

2.6.1 Esihenkilöt

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

Esihenkilöt 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.

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

3 Toteutuskeinot

3.1 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.

3.2 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.

Riskienhallintaan liittyvät keskeiset roolit on määritetty Mandatum Holdingin sekä Mandatum Lifen ja Mandatum Asset Managementin riskienhallintapolitiikoissa. Tietoturvariskien hallintaan sovelletaan edellä mainittujen lisäksi tätä Mandatumin tietoturvapolitiikkaa.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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.

3.8 Tietoturvaloukkauksien hallinta

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

3.9 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.

3.10 ISO 27001 -sertifioinnin vaatimusten täyttäminen

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

4 Viestintä

Tietoturvapolitiikka, -periaatteet, ja -ohjeet julkaistaan Mandatumin Intranetissä. Lisätietoja politiikan soveltamisesta antaa Mandatum-konsernin CISO.

Sisäisestä tiedottamisesta tietoturva-asioissa vastaa ensisijaisesti CISO.

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

5 Valvonta ja rikkomukset

CISO 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 CISOlle.

6 Poikkeamat

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

7 Politiikan tarkistaminen ja päivittäminen

Politiikan ajantasaisuutta arvioidaan tarvittaessa ja vähintään vuosittain CISO:n toimesta. CISO valmistelee politiikkaan tehtävät muutokset. Mandatum Henkivakuutusosakeyhtiön ja Mandatum Asset Management Oy:n hallitukset hyväksyvät politiikan vuosittain.