

## Summary of the Policy

<b>INFORMATION SECURITY POLICY</b>				
<b>Synopsis</b>	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.			
<b>Policy hierarchy</b>	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	-	-
<b>Scope of the policy</b>	Companies		Operations	
	Mandatum Life and MAM as well as their subsidiaries		All employees	
<b>Policy owner</b>	Data Governance			
<b>Approved by</b>	<ul style="list-style-type: none"> <li>▪ Board of Directors of Mandatum Life, 8 February 2023</li> <li>▪ Board of Directors of MAM, 7 February 2023</li> </ul>			
<b>Last updated by</b>	Vesa Tupala, 11 January 2023			
<b>Purpose of the update</b>	Annual review			
<b>Regular review interval</b>	Annual			
<b>Relating policies</b>	<ul style="list-style-type: none"> <li>▪ Mandatum Group's Information Management Policy</li> <li>▪ Mandatum Group's Data Protection Policy</li> </ul>			
<b>Applicable regulation</b>	<ul style="list-style-type: none"> <li>▪ ISO 27001</li> </ul>			
<i>In case of any discrepancy between this summary and the policy, the policy text shall prevail.</i>				

7.2.2023

**TIETOTURVAPOLITIIKKA****Contents**

1	Johdanto .....	2
1.1	Tausta ja tarkoitus .....	2
1.2	Soveltamisala .....	3
2	Organisointi ja vastuut .....	3
2.1	Hallitus ja toimitusjohtaja .....	3
2.2	Group Committee .....	3
2.3	Tietoturvallisuus- ja kyberriskien komitea .....	3
2.4	Organisaatioyksiköt .....	3
2.4.1	Henkilöstöyksikkö .....	3
2.4.2	Business Technologies -yksikkö .....	4
2.5	Tietoturvaorganisaatio .....	4
2.5.1	CISO (Chief Information Security Officer) .....	4
2.5.2	Cyber Security Manager .....	4
2.5.3	Information Security Manager .....	4
2.6	Henkilöstö ja toimeksiannosta työskentelevät .....	4
2.6.1	Esihenkilöt .....	5
3	Toteutuskeinot .....	5
3.1	Tietoturvallisuuden tason arviointi .....	5
3.2	Tietoturvariskien hallinta .....	5
3.3	Tietojen turvaaminen .....	5
3.4	Palveluiden ja tietojärjestelmien turvaaminen .....	5
3.5	Digitaalisen liiketoiminnan turvaaminen .....	6
3.6	Kyberturvallisuuden toteuttaminen .....	6
3.7	Jatkuvuudenhallinta ja varautuminen .....	7
3.8	Tietoturvaloukkauksien hallinta .....	7
3.9	Tietoturvatietoisuuden ja -osaamisen varmistaminen .....	7
3.10	ISO 27001 -sertifiointin vaatimusten täyttäminen .....	7
4	Viestintä .....	7
5	Valvonta ja rikkomukset .....	7
6	Poikkeamat .....	8
7	Politiikan tarkistaminen ja päivittäminen .....	8

LUOTTAMUKSELLINEN

Tämä asiakirja on tarkoitettu ainoastaan sisäiseen käyttöön eikä sitä tule jakaa kolmansille osapuolille.

7.2.2023

## 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) Tietoturvapoliittikka (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:

#### **Asiakslähtöisyys**

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 veloitteet 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.

LUOTTAMUKSELLINEN

Tämä asiakirja on tarkoitettu ainoastaan sisäiseen käyttöön eikä sitä tule jakaa kolmansille osapuolille.

7.2.2023

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 tietoturvasuus on riittävällä tasolla, ja että tietoturvasuudelle asetetaan riittävät resurssit. Mandatum Henkivakuutusosakeyhtiön ja Mandatum Asset Management Oy:n hallitukset hyväksyvät tietoturvapoliittikan ja hallituksilla on ylin vastuu tietoturvapoliittikan noudattamisesta.

### **2.2 Group Committee**

Mandatum Group Committee käsittelee ja puheenjohtaja hyväksyy Mandatum Group CISON esityksestä tietoturvasuutta koskevat periaatteet ja strategian.

### **2.3 Tietoturvasuus- ja kyberriskien komitea**

Tietoturvasuus- ja kyberriskien komitea varmistaa, että operatiivisten riskien hallinta konsernissa on järjestetty asianmukaisesti tietoturvasuus- ja kyberriskien alueella. Komitea varmistaa, että yhteistyö ja tiedonkulku tietoturvasuus- 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 tietoturvasuudesta tietoturvapoliittikan, -periaatteiden ja -ohjeiden mukaisesti. Yksiköt ovat vastuussa tietoturvasuudesta myös sisäisen valvonnan politiikan mukaisesti. Yksiköt konsultoivat Mandatumin tietoturvaorganisaatiota Mandatumin tietoturvasuutta koskevissa asioissa, esimerkiksi tietoturvasuuteen vaikuttavissa hankkeissa ja palveluhankinnoissa.

#### **2.4.1 Henkilöstöyksikkö**

Henkilöstöyksikkö vastaa henkilöstö- ja toimitilaturvasuudesta, työsuhte- ja perehdytysprosesseista sekä esimiesten ohjeistamisesta em. asioissa.

LUOTTAMUKSELLINEN

Tämä asiakirja on tarkoitettu ainoastaan sisäiseen käyttöön eikä sitä tule jakaa kolmansille osapuolille.

7.2.2023

### **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.

### **2.5.1 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. CISO (Chief Information Security Officer)**

Mandatum konsernin CISO johtaa tietoturvallisuutta ja antaa tietoturvapoliittikan ja -periaatteiden mukaisia linjauksia ja lausuntoja sekä hyväksyy tietoturvaohjeet. CISO vastaa tietoturvallisuutta 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 tietoturva-uhkien 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 tietoturvapoliittikkaa, -periaatteita ja -ohjeita sekä huolehtimaan lainsäädännössä kulloinkin asetettujen tietoturva- ja tietosuojavelvoitteiden sekä vakuutuslainsäädännön ja muiden salassapitovelvoitteiden noudattamisesta.

LUOTTAMUKSELLINEN

Tämä asiakirja on tarkoitettu ainoastaan sisäiseen käyttöön eikä sitä tule jakaa kolmansille osapuolille.

7.2.2023

### **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**

LUOTTAMUKSELLINEN

Tämä asiakirja on tarkoitettu ainoastaan sisäiseen käyttöön eikä sitä tule jakaa kolmansille osapuolille.

7.2.2023

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 tietoturvatyimiä ja BT-yksikköä, ja toimia muiden soveltuvien politiikkojen, kuten hankinta-, tietosuojaja 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 käyttövaltuutusperiaatteiden 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.

LUOTTAMUKSELLINEN

Tämä asiakirja on tarkoitettu ainoastaan sisäiseen käyttöön eikä sitä tule jakaa kolmansille osapuolille.

7.2.2023

### **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**

Tietoturvapoliittikka, -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. Poliitiikan 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.

LUOTTAMUKSELLINEN

Tämä asiakirja on tarkoitettu ainoastaan sisäiseen käyttöön eikä sitä tule jakaa kolmansille osapuolille.



7.2.2023

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. Epäilyistä rikkomuksesta, väärinkäytöksestä tai tietoturvaluutteista 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 Poliitiikan 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.

LUOTTAMUKSELLINEN

Tämä asiakirja on tarkoitettu ainoastaan sisäiseen käyttöön eikä sitä tule jakaa kolmansille osapuolille.