midpointed

ASIANAJOLIITON TIETOTURVAOHJEISTUKSET VS. MIDPOINTEDIN PALVELUT

Miten Midpointedin osaaminen ja palvelut kohtaavat asianajoliiton tietoturvaohjeiden kanssa?

Henkilökunnan osaaminen ja ulkoinen tietoturva-auditointi

Asianajajan ja toimiston henkilökunnan tietoturvaosaaminen tulee olla riittävän korkealla tasolla ohjeistuksen soveltamiseen.

Vähintään 10 työntekijän asianajotoimistojen on suoritettava säännöllisiä ulkoisia tietoturva-auditointeja.

Meillä on pitkä kokemus modernien työskentelytapojen koulutuksista, tietoturvanäkökulmalla tai ilman. Pystymme avustamaan yritystänne siirtymään uusiin ketterämpiin ja turvallisempiin toimintatapoihin.

Tarkastukset ja tietopyynnöt

Asianajotoimistoon tai asianajotoimintaan ei toteuteta tarkastuksia tai tietopyyntöjä, jotka liittyvät asiakkuuksiin tai toimeksiantoihin.

Mallinnamme yhdessä kanssanne mihin dataan ulkopuolisilla toimijoilla on tai ei ole pääsyä. Koulutamme myös työntekijöille oikeat ja turvalliset työskentelytavat.

Fyysiset tilat ja aineiston suojaus

Toimitilat tulee suojata ja lukita huolellisesti. Kaikki asianajajasalaisuuden piirissä oleva aineisto on suojattava riippumatta tallennustavasta.

Pystymme antamaan suosituksia aineiston tallennustavoista, sekä auttamaan huolehtimaan, että pääsy yrityksen verkkolaitteille on asianmukaisesti suojattu.

Laite- ja välineturvallisuus

Käytettävien laitteiden ja välineiden tiedot on salattava. Laitteiden elinkaarta on valvottava, poistamalla vanhentuneet laitteet ja vaihtamalla ne uusiin.

Laite ja laitteen data saadaan laitehallinnan avulla suojattua erinomaisesti. Lisäksi henkilöstömme seuraa laitteidenne elinkaarta ja viestii teille, kun olisi aika päivittää laitekantaa tai loppukäyttäjän laite osoittaa merkkejä hajoamisesta.

Langattomat verkot ja verkkoturvallisuus

Toimiston langattomat verkot tulee suojata ja vierailijoille on tarjottava erillinen langaton verkko. Julkisia verkkoja tai kotiyhteyttä käyttäessä käytetään VPN-yhteyttä.

Kauttamme saatte modernit verkkolaitteet, riittävän määrän tukiasemia ja VPN-yhteydet käyttäjien laitteille. Kauttamme saatavilla myös verkkoyhteyden kahdennuspalvelu, jotta työn tekeminen voi jatkua, vaikka pääyhteys katkeaisikin.

Salasanat ja tunnistautuminen

Salasanojen on oltava monimutkaisia ja niitä on vaihdettava säännöllisesti. Lisätunnistautumismenetelmiä tulee käyttää korkeamman turvallisuustason saavuttamiseksi.

Annamme ohjeistuksia ja suosituksia turvallisista tietoturvapolitiikoista. M365-ekosysteemistä löytyy paljon tietoturvaa edistäviä toiminnallisuuksia ja asetuksia, joissa pystymme auttamaan teitä tarvittaessa.

Tietoturva on turvallisuuden ja käytettävyyden välillä tasapainoilua, ja meillä on pitkä toimialakokemus lakialalta tietoturvan osalta.

Tietoturvaohjelmistot ja päivitykset

Tietoturvaohjelmistot ja palomuuri tulee pitää ajan tasalla. Laite-, käyttöjärjestelmä-, ohjelma- ja sovelluspäivitykset tulee asentaa ilman viivästyksiä.

Suunnittelemme yhdessä kanssanne juuri teille sopivan tietoturvakokonaisuuden. Haittaohjelmasuojaus, laitehallinta ja keskitetty valvonta muodostavat turvallisen ympäristön työskentelylle. Suosituksemme rakentuvat Zero Trust -mallin ympärille.

Asiakirjojen pääsy ja hallinta

Vain tarvittavilla henkilöillä on oikeus päästä käsiksi salassa pidettäviin tietoihin.

Avustamme ja määritämme haluamiinne järjestelmiin käyttöoikeudet ja ehdollisen käytönseurannan. Tiedostonne voidaan luokitella, ja niille voidaan määrittää erilaisia suojaustasoja.

Varmuuskopiointi

Varmuuskopiot tulee tehdä säännöllisesti ja niitä tulee testata säännöllisesti.

Varmuuskopioimme sekä käyttäjien henkilökohtaisen datan että myös organisaationne Microsoft 365 -datan erillisillä palveluilla.

Palveluntarjoajien sopimukset

Ulkopuolisten palveluntarjoajien kanssa tehdyt sopimukset tulee täyttää tietoturvavaatimukset.

Konsultoimme mielellämme sopimuksissa ja hankinnoissa, vaikka ne eivät tapahtuisikaan kauttamme.

Sähköpostin ja sähköisen viestinnän tietoturva

Sensitiivinen sähköinen aineisto on salattava tarvittaessa.
Asiakkaita tulee ohjeistaa käyttämään suojattuja menetelmiä aineiston toimittamiseen.

Me voimme antaa henkilökunnallenne ohjeita salatun sähköpostin käyttöön tai ottaa sen käyttöön puolestanne, jos se ei ole vielä käytössä.

Asiakirjojen hallinta ja säilytys

Asiakirjat tulee tallentaa, säilyttää, arkistoida ja tuhota turvallisesti.

Pystymme konsultoimaan ja määrittämään yrityksellenne hyvän prosessin työskentelyä, tallentamista, säilyttämistä ja tuhoamista varten. Apuna voidaan käyttää erilaisia automaatioita ja tiedostojen luokittelua, sekä henkilöstön kouluttamista.

Laitteiden ja palveluiden poistaminen käytöstä

Käytöstä poistetut laitteet ja palvelut tulee tyhjentää turvallisesti.

Lisäpalveluna käytöstä poistetut laitteet tyhjennetään käyttäen alan parhaita käytäntöjä. Tyhjennyksestä saat sertifikaatin, josta käy ilmi oleelliset tiedot ja varmuus onnistuneesta tyhjennyksestä.

Toiminnan jatkuvuus

Toimiston jatkuvuuden varmistamiseksi tarvittavat tiedot tulee dokumentoida ja olla saatavilla.

Tarjoamme asiakkaidemme käyttöön monipuoliset tietoturvaratkaisut, datan ja verkkoyhteyden kahdennuspalvelut, varalaite-ratkaisut, tukipalvelut ja tarpeisiin räätälöityä konsultointia kaikkiin IT-ongelmiin.

Tämä ohjeistus pyrkii varmistamaan asianajotoimiston tietoturvan ja luottamuksellisten tietojen asianmukaisen käsittelyn.

Me Midpointedilla tarjoamme kattavat ja tietoturvalliset IT-palvelut huomioiden alakohtaiset eritystarpeet. Missionamme on tehdä työstänne parempaa toimivan IT:n, modernien työtapojen ja automaatioiden avulla.

Ole yhteydessä, mikäli haluat olla varma siitä, että IT:si toimii, on tietoturvallinen ja ennen kaikkea kiinteähintainen.

Tomi Keränen

Account Executive, Partner

+358 45 189 8600

tomi.keranen@midpointed.fi