# Dokumentin tarkoitus

Tässä dokumentissa on kuvattu Maxtech Oy:n (myöhemmin “Yritys”) tietoturvakäytännöt Asiakkaan kannalta olennaisin osin. Tämä dokumentti pohjautuu Yrityksen sisäiseen tietosuojapolitiikkaan sekä muuhun tietosuojaan ja -turvaan liittyvään dokumentaatioon.

# Tekniset suojaukset

## Tietoliikenteen salaus

Tietoliikenne Maxtech-järjestelmään on aina salattu nykyaikaisin salausmenetelmin, kun järjestelmää käytetään verkkoselaimella, mobiilisovelluksella tai leimauslaitteella.

## Tilaturvallisuus

Kaikissa Yrityksen tiloissa on käytössä kulunvalvonta ja kulku tiloihin on sallittu vain nimetyille henkilöille. Mihinkään Yrityksen tiloihin ei ole ulkopuolisilla vapaata kulkua.

Kaikki Maxtech-järjestelmän palvelimet sijaitsevat Suomessa ja palvelintiloihin kulku on rajattu vain niille henkilöille, joilla työtehtäviensä puolesta on tarvetta päästä kyseisiin tiloihin ja tiloissa on kulunvalvonta

## Laitteistojen turvallisuus

### Palomuurit

Yrityksen verkko sekä palvelinten konesalin verkko on suojattu ulkopuoliselta tunkeutumiselta palomuureilla.

### Ohjelmistopäivitykset

Palvelinohjelmistojen päivityksille on käytössä reaaliaikainen seuranta. Kiireelliset tietoturvapäivitykset asennetaan viipymättä.



Maxtech Oy
2145296-2

Vihikari 10
90440 Kempele
Finland

+358 10 229 6200
www.maxtech.fi
info@maxtech.fi

### Levyjen salaus

Maxtech-järjestelmän tuotantopalvelinten datalevyt on salattu. Lisäksi työasemien levyistä vähintään käyttäjän tiedostot sisältävä osio on salattu.

# Käyttöoikeudet

## Käyttäjien oikeuksien hallinta

Yrityksellä on dokumentoitu prosessi työntekijöiden käyttäjätunnusten myöntämiseen ja sulkemiseen.

## Pääsy järjestelmiin ja laitteille

Kaikkien Yrityksen käytössä olevien järjestelmien, palvelinten ja työasemien käyttö on rajattu käyttäjäkohtaisilla käyttäjätunnuksilla.

## Roolipohjaiset käyttöoikeudet ja kaksivaiheinen kirjautuminen

Järjestelmissä käytetään mahdollisuuksien mukaan roolipohjaisia oikeuksia, joilla käyttäjäkohtainen pääsy rajataan vain työtehtävien kannalta tarpeellisiin tietoihin ja toimintoihin.

Ylläpitäjäkäyttäjien tunnistautumisessa käytetään tietoturvan parantamiseksi kaksivaiheista kirjautumista niissä järjestelmissä, joissa kyseinen toiminto on käytettävissä. Maxtech-järjestelmässä ylläpitotoimintojen käyttäminen vaatii tunnistautumisen lisäksi erillisen, vain ylläpitäjäkäyttäjien hallussa olevan salasanan syöttämisen.

## Turvaluokitukset

Yrityksen tietosuojapolitiikassa on määritetty henkilöstön turvaluokitukset. Turvaluokitustaso määrittää korkeimman tason tiedoille, joihin henkilöllä voi olla pääsy. Suurempi taso tarkoittaa pääsyä kriittisempiin tietoihin ja edellyttää lisävaatimusten täyttämistä.



Maxtech Oy
2145296-2

Vihikari 10
90440 Kempele
Finland

+358 10 229 6200
www.maxtech.fi
info@maxtech.fi

# Varmuuskopiot

Maxtech-järjestelmän tiedoista otetaan automaattisesti varmuuskopiot vähintään kerran vuorokaudessa. Varmuuskopiot säilytetään palvelintilasta fyysisesti erillisessä tilassa.

# Kyberuhkien torjunta

## Uhkien seuranta tiedotteista

Kyberuhkia seurataan aktiivisesti muun muassa Kyberturvallisuuskeskuksen tiedotteista.

## Palvelunestohyökkäyksiltä (DDoS) suojautuminen

Maxtech-järjestelmän palvelinympäristössä on käytössä palveluntarjoajan tuottama DDoS-suojaus sekä liikenteen reaaliaikainen, ympärivuorokautinen valvonta.

## Tietoturvatestaus

Maxtech-järjestelmään suoritetaan säännöllisesti ulkoisen tahon tekemiä tietoturvatestauksia.

# Henkilöstö ja osaaminen

## Salassapito

Kaikki Yrityksen työntekijät sekä henkilö- tai muita arkaluontoisia tietoja käsittelevät alihankkijoiden työntekijät ovat allekirjoittaneet salassapitosopimuksen.

## Dokumentointi ja koulutukset

Tietoturvaan liittyvä sisäinen ohjeistus pidetään ajantasaisesti saatavilla yrityksen dokumentaatiossa. Olennaiset muutokset huomioidaan myös



Maxtech Oy
2145296-2

Vihikari 10
90440 Kempele
Finland

+358 10 229 6200
www.maxtech.fi
info@maxtech.fi

henkilöstön osaamisen testauksessa (ks. kohta Tietosuojaosaamisen testaaminen alla) päivittämällä kyselyä tarvittavilta osin.

Henkilöstön tietosuojaosaamista pidetään lisäksi yllä tarpeen mukaan pidettävillä koulutuksilla.

### Tietosuojaosaamisen testaaminen

Henkilöstön tietosuojaosaamista testataan säännöllisesti määräajoin sisäisillä testeillä, joissa kaikkiin kysymyksiin on vastattava oikein testin läpäisemiseksi.

### Tiedonkalastelusimulaatiot

Yrityksen sähköposteihin tehdään ajoittain tiedonkalastelusimulaatioita, joilla kartoitetaan ja ylläpidetään henkilöstön osaamista huijausviestien tunnistamisessa.

## Valvonta ja auditointi

### Palvelinten valvonta

Maxtech-järjestelmän palvelinten laitteiston sekä ohjelmistojen tilaa valvotaan reaaliaikaisesti ja palvelinten ylläpitäjät saava poikkeamista ilmoitukset.

### Lokitus

Maxtech-järjestelmään tallentuu muutosloki asiakastietoihin tehdyistä olennaisista muutoksista.

Admin-käyttäjän ottaessa oikeuden asiakasorganisaation tietoihin (esimerkiksi tukipyynnön ratkaisemista varten) tästä jää järjestelmään asiakkaalle näkyvä merkintä, josta näkee oikeudet ottaneen henkilön sekä perusteen oikeuksien ottamiselle.



Maxtech Oy
2145296-2

Vihikari 10
90440 Kempele
Finland

+358 10 229 6200
www.maxtech.fi
info@maxtech.fi

# Viestintä

Maxtechilla on dokumentoidut sisäiset käytännöt, joissa kuvataan viestintä sisäisesti, asiakkaille (ja/tai asianomaisille henkilöille) sekä viranomaisille tietoturvaloukkaus- ja muissa poikkeamatilanteissa. Viestittäessä Asiakkaalle yhteyttä otetaan Asiakkaan asiakastietoihin merkittyihin pääkäyttäjiin, joiden ajantasaisuudesta vastaa Asiakas.



Maxtech Oy
2145296-2

Vihikari 10
90440 Kempele
Finland

+358 10 229 6200
www.maxtech.fi
info@maxtech.fi