

**SIA “MED PROF”**

**IT drošības politika**

**SATURS**

[1. Definīcijas 2](#_Toc534724201)

[2. Vispārīgā informācija 2](#_Toc534724202)

[3. Darbstaciju drošās lietošanas pamatprincipi 3](#_Toc534724203)

[4. Darbstaciju paroļu uzbūve un lietošana 4](#_Toc534724204)

[5. Drošības incidenti 5](#_Toc534724205)

[6. Sīkdatņu politika 5](#_Toc534724206)

[7. Elektroniskā pastA lietošana 5](#_Toc534724207)

[8. Stāšanās spēkā 5](#_Toc534724208)

# Definīcijas

## Datoriekārta – jebkura iekārta, kura tiek izmantota kopā vai bez datorsistēmas, un ar kuras palīdzību vai starpniecību tiek veikta datu apstrāde.

## Datu apstrāde – jebkura ar Personas datiem vai Personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, piekļuve, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana.

## Datu subjekts – ir katra fiziska persona, kuras Personas dati tiek apstrādāti.

## IT (*no angļ. - Information Tehnologies*) – informācijas tehnoloģijas.

## IT drošības politika – šī drošības politika, kas nosaka minimālo standartu, ko Sabiedrība apņemas nodrošināt Personas datu apstrādē.

## Ļaunatūra - ļaunprātīga programmatūra. Tāds programmnodrošinājums, datorprogramma, citā programmā iestrādātais programmkods, kas izveidots ar nolūku rādīt nevēlamu vai kaitīgu efektu.

## Personas dati – jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu; identificējama fiziska persona ir tāda persona, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem.

## Sabiedrība – SIA “MED PROF”, juridiskā adrese: Krišjāņa Valdemāra iela 94-11, Rīga, LV-1013, kontaktinformācija personas datu aizsardzības jautājumiem: e-pasts \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, tālr.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

## UPS (*no angļ* - *Uninterruptible Power Supply*) – Nepārtrauktās barošanas ierīce, jeb ierīce, kura īslaicīgi nodrošina strāvas padevi pēkšņas elektrības pažūšanas gadījumā. Parasti izmanto nepabeigto darbu saglabāšanai un pareizai datortehnikas izslēgšanai.

## VDAR – Eiropas Vispārīgā datu aizsardzības regula Nr. 679/2016, kas piemērojama visās dalībvalstīs no 2018. gada 25. maija.

# Vispārīgā informācija

## Ievads

Sabiedrība ir apņēmusies nodrošināt Personas datu aizsardzību un īpaši rūpīgu to apstrādi. Sabiedrībai ir būtiska tās rīcībā esošo fizisko personu datu aizsardzība un privātuma nodrošināšana. IT drošības politika ir viens no Personas datu aizsardzības būtiskākajiem punktiem, ar kuru iespējams paredzēt un piemērot gan tehniskus, gan arī juridiskus risinājumus.

## Mērķis

Šī IT drošības politika nosaka pamatprincipus, kuri ir izmantojami Sabiedrības ikdienas darba veikšanā, ievērojot kurus, ir iespējams būtiski uzlabot apstrādājamo datu drošību. IT drošības politikā ietverti ne tikai ieteikumi Sabiedrības darbiniekiem, bet arī minimālā informācija, kas ir sniedzama, piemēram, Sabiedrībai piederošās tīmekļa vietnes <http://medprof.lv/> apmeklētājiem.

## Piemērošanas joma

Šī IT drošības politika ir piemērojama jebkādai Personas datu apstrādei un saistoša visiem Sabiedrības darbiniekiem.

Šī IT drošības politika ir piemērojama papildus Latvijas Republikā piemērojamo normatīvo aktu (t.sk., VDAR) prasībām un atspoguļo minimālo standartu, kas tiek piemērots jebkurai Sabiedrības pārziņā esošajai Personas datu apstrādei. Gadījumā, ja piemērojamie tiesību akti paredz stingrākas prasības kā šajā politikā, tiek piemēroti attiecīgo piemērojamo tiesību aktu prasības.

Šī IT drošības politika aizstāj visas iepriekšējās politikas un vadlīnijas attiecīgajā jomā. Izņēmums no šī punkta ir tādi iekšēji noteikumi, kuri ir saskaņā ar šo IT drošības politiku un ietver detalizētāku šajā IT drošības politikā noteikta jautājuma īstenošanas kārtību.

## Atbildība

Kompetenci un atbildību par šo IT drošības politikas saturu, uzturēšanu, aktualizāciju ieviešanu un ievērošanu uzņemas Sabiedrības valde. Šī uzdevuma izpildi var deleģēt citām personām (attiecīgām struktūrvienībām, to vadītājiem, datu aizsardzības speciālistam utt.). Deleģēšanas gadījumā ir jānodrošina tieša atskaišu sniegšana valdei. Vispārējo atbildību par Sabiedrības rīcību ar Personas datiem uzņemas Sabiedrības valde. Par esošo un jauno darbinieku informēšanu par šo IT drošības politiku un tās saturu uzņemas Sabiedrības valde.

# Darbstaciju drošās lietošanas pamatprincipi

## Izvietojums

Darbstacijas jāizvieto tādā veidā, lai pie tām fiziski nevarētu piekļūt trešās personas, nodrošinoties pret iespējama ļaundara destruktīvajām darbībām, piemēram, inficētās zibatmiņas ievietošanas darbstacijā, barošanas vada izraušana utt. Izvades iekārtas (printeris, monitors) vēlams izvietot tādā veidā, lai trešās personas, ierodoties uz konsultāciju, nevarētu nesankcionēti piekļūt tiem neparedzētai informācijai.

## Darbstaciju konfigurācija un loģiskā aizsardzība

Sākotnējo darbstacijas konfigurēšanu veic Sabiedrības valde. Darbstacija tiek nokonfigurēta darba pienākumu veikšanai, ievērojot šādas minimālās prasības:

* katram datora lietotājam ir izveidota normatīvajiem aktiem atbilstoša pieslēgšanas parole;
* ikdienas datora lietotājam nav piešķirtas datora administratora tiesības;
* tīmekļa pārlūkprogrammās (Mozilla Firefox, Opera, Google Chrome u.c.) ir atslēgta automātiskā paroļu un lietotājvārdu saglabāšana, kā arī automātiskā ielogošanās sistēmā;
* ir ieslēgta automātiskā darbstacijas bloķēšana vismaz pēc 5 minūtēm, kad tā netika izmantota;
* operētājsistēmas atjauninājumi, antivīruss, ugunsmūris ir nepārtraukti aktīvi un aktuāli;

Sabiedrības valde ne retāk ka divas reizes gadā veic visu Sabiedrības darbstaciju pāraudi atbilstībai iepriekšminētajām prasībām, vajadzības gadījumā uzaicinot IT speciālistu neskaidru jautājumu risināšanai un citu problēmu novēršanai.

## Datoriekārtu fiziskā aizsardzība

Telpas, kurās atrodas Sabiedrībai piederošas datoriekārtas, ir aprīkotas ar ugunsgrēka signalizācijas iekārtām, ugunsdzēšamajiem aparātiem un apsardzes signalizāciju. Nepieciešamības gadījumā datoriekārtas tiek aprīkotas ar nepārtrauktās barošanas ierīcēm.

Sabiedrības valde rūpējas par datu rezerves kopiju izveidošanu un attiecīgu drošu glabāšanu.

## Darbstacijas ikdienas lietošana

Darba pienākumu veikšanas laikā datora lietotājs izmanto tikai savu, darba pienākumu veikšanai noskaņotu lietotāja kontu. Ieejot sistēmā, izmanto savu paroli, kura ir zināma tikai viņam. Darbstacijas lietošanas laikā darbinieks neveic sākotnējās konfigurācijas maiņu, izņemot gadījumus, kad tas ir saskaņots ar Sabiedrības valdi un par to ir brīdināts Sabiedrības datortehniku apkalpojošais IT speciālists. Sākotnējās konfigurācijas maiņa tiek veikta tikai uz noteiktu laiku vai darba īpašu uzdevumu pildīšanas brīdi, pēc kā tiek atgriezti sākotnējie uzstādījumi.

Ikdienas darba pienākumu veikšanas laikā, darbstacijas lietotājs seko drošības sistēmas (antivīruss, ugunsmūris u.c.) paziņojumiem, un, vajadzības gadījumā konsultējas ar Sabiedrības datortehniku apkalpojošais IT speciālistu. Gadījumā, ja ir aizdomas, ka lietojamais dators ir inficēts, vai var būt inficēts ar ļaunatūru, datorsistēmas lietotājs par to nekavējoties paziņo minētajam IT speciālistam, kurš veic atbilstošas darbības iespējamo problēmu novēršanai.

Jebkurš Sabiedrības darbinieks ir atbildīgs par viņa izmantotās datorsistēmas drošību, un tā pienākums ir nodrošināt, ka viņa prombūtnes laikā ieslēgts ar paroli aizsargāts ekrānsaudzētājs, vai arī dators ir nobloķēts, nospiežot pogu Ctrl-Alt-Del kombināciju, pēc kā izvēlēta iespēja „Lock Computer”, vai arī nospiežot pogu kombināciju  +L.

Darba dienas beigās, kad darbs pie datora ir pabeigts, datora lietotājs izslēdz darbstaciju, izmantojot funkciju „Shut down” vai „Install updates and shut down”, jā tāda tiek piedāvāta.

# Darbstaciju paroļu uzbūve un lietošana

Darbstacijas lietotājs pats izveido zemāk esošiem noteikumiem atbilstošu paroli, pret kuru nomaina sākotnējo, vai pirms tam izmantoto paroli. Darba konta lietotāja parole ir zināma tikai darbiniekam, kurš strādā pie noteiktā datora, izmantojot noteikto lietotāja kontu. Ja lietotājs ir aizmirsis lietotāja paroli, viņš par to paziņo Sabiedrības datortehniku apkalpojušajam IT speciālistam, kurš palīdz to nomainīt, vai arī, izmantojot lietotāju ar administratora tiesībām, pats nomaina sava lietotāja paroli.

Jebkuras darbstacijas jebkura lietotāja parolei jāatbilst vismaz sekojošām prasībām:

* minimālais paroles garums nedrīkst būt mazāks par 9 simboliem;
* maksimālais paroles maiņas biežums nedrīkst būt ilgāks par 90 dienām;
* paroles uzbūvei jābūt komplicētai, tajā jāiekļauj vismaz viens liels latīņu alfabēta burts, mazs latīņu alfabēta burts, cipars un īpaša rakstzīme (piemēram, !@#$%^&\*);
* parolē nav vēlams iekļaut vārdus, uzvārdus, dzimšanas datumus, citus bieži izmantotus veselus vārdus utt., kā arī slāvu alfabēta burtus;
* izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm.

# Drošības incidenti

Darbstacijas lietotājs, konstatējot iespējamo ielaušanos viņa datorsistēmā no ārpuses, vai pamanot citas neparastas aktivitātes viņa datorsistēmā, par konstatēto paziņo Sabiedrības valdei, kura savukārt lemj par turpmākām darbībām.

Gadījumā, ja tiek konstatēti ielaušanās mēģinājumi vai būtiski incidenti, Datortīklu administrators veic to reģistrēšanu un izmeklēšanu, kā arī par tās rezultātiem, bet ne ilgāk kā 72 stundu laikā pēc konstatēšanas, informē Drošības incidentu novēršanas institūciju (CERT.lv).

# Sīkdatņu politika

Sabiedrībai piederošajā tīmekļa vietnē iestrādāta informācija par sīkdatņu politiku, kurā tiek informēts par izmantotajām sīkdatnēm, to izmantošanas mērķiem, izmantotās informācijas iespējamiem saņēmējiem un iespēju tās dzēst. Sīkdatņu izmantošanai nepieciešams iegūt tīmekļa vietnes apmeklētāja piekrišana. Piekrišanai ir jābūt aktīvai darbībai (piemēram, elektronisks izvēles logs, kurš personai ir nepārprotami jāatzīmē, ka tā piekrīt). Piekrišana nevar tikt iegūta, ja elektroniskā pieteikuma formā izvēles lodziņu, kas paredzēts, lai atzīmētu piekrišanu personas datu apstrādei, sistēma aizpilda pēc noklusējuma. Papildus minētajam, tīmekļa vietnē tiek iestrādāta informācija par iespēju piekļūt saviem personas datiem, kā arī citām datu subjekta tiesībām, tostarp atsaukt piekrišanu.

Papildus informācija par Sabiedrības tīmekļa vietnē izmantojamām sīkdatnēm un sīkāka informācija par to kādai informācijai jāatrodas minētajā vietnē, ir noteikts „Sīkdatņu politika un skaidrojumi” (Pielikums 1).

# Elektroniskā pastA lietošana

Sabiedrības piešķirtais darbinieku elektroniskais pasts ir lietojams tikai darba pienākumu veikšanai. Darba elektronisko pastu aizliegts izmantot personīgajām vajadzībām. Nosūtot elektronisko pastu, tā apakšā, pēc paraksta jānorāda sekojoša informācija: „*Šīs elektroniskais pasts var saturēt fiziskās personas datus. Ja jūs neesat persona, kam ir domāts šīs elektroniskais pasts, lūdzu to izdzēst, kā arī informēt mani par kļūdaini nosūtīto elektronisko pastu*.” Nepieciešamības gadījumā šo uzrakstu iztulko un pievieno arī citā valodā.

# Stāšanās spēkā

Šī Privātuma politika stājas spēkā 2019.gada \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ .

Rīga, 2019.gada \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Valdes locekle Jeļena Lapkovska