LATVIJAS REPUBLIKA
**KĀRSAVAS NOVADA PAŠVALDĪBA**

Reģ.Nr.90000017398
Vienības iela 53, Kārsava, Kārsavas novads,LV-5717
tālr.65781390, fakss 65711030, e-pasts: dome@karsava.lv

Apstiprināts
Kārsavas novada domes
2020. gada 23. jūlija sēdē
/lēmums Nr.1, protok. Nr.11 /

# Iekšējie datu drošības noteikumi

**Termini**

**Pārzinis** – Kārsavas novada pašvaldības, reģistrācijas Nr. 90000017398.

**Darbinieks** – persona, kura slēdz vai ir noslēgusi darba līgumu (vai saskaņā ar citu civiltiesisku līgumu veic vai varētu veikt personas datu apstrādi) ar Pārzini un piekrīt ievērot šajos noteikumos minētos nosacījumus;

**Lietotājs** – persona, t.sk., Darbinieks, kas lieto vai kam ir piekļuve Informācijai, Konfidenciālai informācijai, Personas datiem;

**Konfidenciāla informācija** – jebkāda informācija, kas raksturo Pārziņa darbību, tajā skaitā, informācija par klientiem, sadarbības partneriem, sadarbības veidošanas politiku, pašvaldības algu saraksti, informācija par sertifikācijas pakalpojumu sniegšanu, tehnisko iekārtu izvietojumu, apsardzes nosacījumi;

**Personas dati** – jebkāda informācija, kas attiecas uz identificējamu vai identificētu fizisko personu, tajā skaitā, vārds, uzvārds, personas kods, dzīvesvietas, īpašuma adrese, darba vieta, tālruņa numurs, ģimenes stāvoklis, kā arī sensitīvie dati –personas dati, kas norāda personas rasi, etnisko izcelsmi, reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi.

Lai noteiktu vai persona ir identificējama tiek ņemti vērā jebkādi līdzekļi, ko jebkura trešā persona teorētiski varētu izmantot, lai identificētu fizisko personu.

**Informācija** – dokumenti, finanšu rezultāti, piezīmes, fotouzņēmumi, audioieraksti, videoieraksti, mutvārdos izteiktas ziņas, rīkojumi, u.tml. kā arī, Konfidenciāla informācija un Personas dati kopā saukti vai katrs atsevišķi.

**Tehniskie resursi** – datori, serveri, telefoni, kopētāji, printeri, skeneri.

**Informācijas resursi** – informācijas tehnoloģiju lietojumi (programmatūra), datu bāzes, mobilās aplikācijas, interfeisi.

## 1. Vispārīgie jautājumi

1.1. Noteikumi reglamentē Pārziņa personas datu drošības obligātos tehniskos un organizatoriskos pasākumus.

1.2. Noteikumu mērķis ir aizsargāt fizisko personu pamattiesības un brīvības, it īpaši privātās dzīves neaizskaramību, attiecībā uz fiziskās personas datu apstrādi pašvaldībā.

1.3. Informācijas resursiem, kas satur personas datus drīkst piekļūt vienīgi Darbinieki, kuriem piekļuves tiesības ir piešķīris Informācijas un Tehnisko resursa turētājs un kuri ir iepazinušies ar šiem noteikumiem un apņemas tos ievērot.

1.4. Noteikumi ir saistoši visiem Darbiniekiem, kā arī trešajām personām, kuras ir iesaistītas personas datu apstrādē pašvaldībā.

1.5. Pārzinis apzinās, ka darba pienākumu veikšanai ir nepieciešams nodot Darbinieka rīcībā Informāciju, līdz ar to noteikumos Pārzinis nosaka vispārējo Informācijas apstrādes kārtību, kuru Darbinieks apņemas ievērot un veikt visas nepieciešamās un lietderīgās darbības, lai tā tiktu ievērota.

## 2. Par Informācijas un Tehniskajiem resursiem atbildīgā persona un tās pienākumi.

2.1. Par Informācijas resursiem (resursu uzglabāšanu, drošību un pieejamību, paroļu veidošanu un lietošanas uzraudzību) un Tehniskajiem resursiem (tehnisko resursu uzturēšanu un izmantošanu) ir atbildīgs resursu turētājs – Kārsavas novada pašvaldības IT speciālists.

2.2. Attiecībā uz Informācijas resursiem turētājs:

2.2.1. nodrošina loģiskās aizsardzības pasākumus;

2.2.2. nodrošina Informācijas resursu darbības atjaunošanu, ja noticis Tehnisko resursu bojājums vai arī Informācijas resursa darbība ir tikusi traucēta citu iemeslu dēļ.

2.3. Attiecībā uz Tehniskajiem resursiem turētājs:

2.3.1. nodrošina fiziskās aizsardzības pasākumus;

2.3.2. nodrošina Tehnisko resursu darbspēju;

2.3.3. organizē Tehnisko resursu atjaunošanu vai nomaiņu, ja tie bojāti.

**3. Resursu turētājs nosaka Informācijas resursu klasifikāciju:**

3.1. vispārējas piekļuves – pieejami bez ierobežojuma visiem Darbiniekiem,

3.2. ierobežotas piekļuves – informācija, kurai piekļūt var tikai pilnvarots Darbinieks un/vai uzraudzības un kontroles iestādes atbilstoši to kompetencei.

**4. Personas datu apstrādes tehniskās un organizatoriskās prasības:**

4.1. Personas datu apstrāde tiek veikta pašvaldības juridiskajā adresē.

4.2. Lai nodrošinātos pret nesankcionētu piekļuvi, Tehniskie resursi pēc iespējas tiek novietoti telpā, kurai var piekļūt tikai pilnvaroti Darbinieki. Ja Tehniskie resursi atrodas publiski pieejamā telpā, piemēram, visu uzņemšanā (recepcijā), tad tiek nodrošināti attiecīgi drošības pasākumi – paroles pieprasīšana pēc īsa (2-5 min.) datora dīkstāves laika utml.

4.3. Resursu turētājs iespēju robežās nodrošina Tehnisko resursu aizsardzību pret dabas stihijām, ugunsgrēka, plūdiem u.tml.

4.4. Aizliegts nodot trešajām personām Tehniskos resursus, ja tie satur personas datus. Šis aizliegums jāievēro arī gadījumos, kad tehnika tiek nodota utilizācijai.

4.5. Piekļuve Informācijas resursiem tiek ierobežota ar paroli:

4.5.1. Parole veidojama no vismaz astoņiem simboliem, starp kuriem ir vismaz viens latīņu alfabēta mazais burts, vismaz viens latīņu alfabēta lielais burts un vismaz viens cipars;

4.5.2. Paroli aizliegts veidot, izmantojot ar sistēmas lietotāju saistītu informāciju (piemēram, vārdus, uzvārdus, dzimšanas dienas, tālruņa numurus, u. Tml.).

4.5.3. Paroli ieteicams mainīt ne retāk kā reizi trijos mēnešos.

4.5.4. Parole nedrīkst būt pieejama trešajām personām. Paroli nedrīkst uzglabāt pierakstītu uz papīra vai arī elektroniskā formā, ja tas rada apdraudējumu parolei nokļūt trešās personas rokās.

4.6. Attālināta piekļuve Informācijas resursiem caur internetu tiek aizsargāta ar lokālā tīkla maršrutētāju, kam ir ugunsmūra funkcija.

4.7.Par jebkuru personas datu apstrādes incidentu Darbiniekam, kas to konstatējis, ir nekavējoties jāpaziņo resursu turētājam:

4.7.1. ja konstatēts jebkāda veida apdraudējums Tehniskajiem resursiem (elektroenerģijas padeves pārtraukums, šķidrumu vai svešķermeņu iekļūšana, bojājumi fiziska trieciena, uguns iedarbības vai plūdu rezultātā u.c.);

4.7.2. ja konstatēts jebkāda veida apdraudējums Informācijas resursiem (trešajām personām kļuvusi zināma pieejas parole, konstatēta nesankcionēta piekļuve, konstatēti darbības pārtraukumi u.c.).

4.8.Incidentu gadījumā Darbiniekam savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt tehnisko un Informācijas resursu drošību līdz attiecīgo resursu turētāja ierašanās brīdim.

## 5. Personas datu aizsardzības klasifikācija atbilstoši to vērtības un konfidencialitātes pakāpei.

5.1.Lai aizsargātu konfidenciālo informāciju tā tiek klasificēta atbilstoši Pārziņa noteiktajai kārtībai:

5.1.1. Ierobežotas pieejamības informācija – paredzēta ierobežotam Darbinieku vai personu, kuras ir līgumsaistībās ar pašvaldību, lokam. Šīs informācijas izpaušana vai nozaudēšana apgrūtina vai var apgrūtināt pašvaldības darbību, nodara vai var nodarīt kaitējumu Pārzinim.

5.1.2. Vispārpieejama informācija – kas nav klasificēta kā ierobežotas pieejamības informācija. Brīvi pieejama visiem Darbiniekiem un jebkurai trešajai personai, kas šo informāciju ir pieprasījusi. Šīs informācijas izpaušana vai nozaudēšana neietekmē pašvaldību negatīvā veidā.

## 6. Tehniskie resursi, ar kādiem tiek nodrošināta personas datu apstrāde.

6.1.Pārzinis personas datu apstrādei lieto šādus Tehniskos resursus:

6.1.1. Darbstacijas ar operētājsistēmu;

6.1.2. Serverus ar operētājsistēmu;

6.1.3. Citas iekārtas un programmatūru pēc vajadzības.

## 7. Personas datu lietotāju tiesības, pienākumi, ierobežojumi un atbildība.

7.1.Lietotājam ir šādi pienākumi:

7.1.1. Savlaicīgi pieprasīt piekļuvi Informācijas resursiem, kas nepieciešami darba pienākumu pildīšanai vai pakalpojuma sniegšanai pašvaldībai;

7.1.2. Veikt personas datu apstrādi tikai tādā apjomā un tikai tādiem mērķiem kā norādīti zemāk:

7.1.2.1.realizējot savu tiešo darba pienākumu un/vai citu līgumisko saistību izpildi;

7.1.2.2.identificējot Darbinieku, kas nepieciešams viņam piešķirto pienākumu, atbildības un saistību izpildei;

7.1.2.3.identificējot konkrētā Darbinieka kompetenci;

7.1.2.4.pārliecinoties, ka konkrētais Darbinieks ir saņēmis pienākumu izpildei saistošo informāciju;

7.1.2.5.identificējot konkrētā Darbinieka izpildītos pienākumus, iepazīstināšanu ar informāciju.

7.1.2.6.uzturot datu apmaiņu noslēgto līgumu ietvaros.

7.1.2.7.Citiem mērķiem, kas saistīti ar Pārziņa pamatdarbību.

7.1.3. Incidentu gadījumā Darbiniekam savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt Tehnisko resursu un Informācijas resursu drošību līdz attiecīgo resursu turētāja ierašanās brīdim.

7.1.4. Veikt visus nepieciešamos aizsardzības pasākumus, lai tam pieejamiem personas datiem nepiekļūtu trešās personas.

7.1.5. Rūpēties, lai datora ekrānā redzamā informācija, kas satur personas datus, nebūtu redzama citiem.

7.1.6. Spēt pamatot nepieciešamību piekļūt personas datiem un savas darbības informācijas sistēmā.

7.1.7. Sniegt palīdzību informācijas drošības incidentu izmeklēšanā.

7.2.Lietotājam ir šādas tiesības:

7.2.1. Pieprasīt tehnisko nodrošinājumu šo noteikumu prasību realizēšanai;

7.2.2. Saņemt paskaidrojumus par piešķirto lietotāja tiesību ierobežojumiem;

7.2.3. Sniegt priekšlikumus informācijas drošības uzlabošanai;

7.2.4. Pieprasīt konsultācijas un apmācību saistībā ar personas datu apstrādes normatīvo regulējumu un drošību.

7.3.Lietotājam ir aizliegts:

7.3.1. Veikt darbības, kas apdraud Informācijas resursa vai informācijas, kas satur personas datus, drošību;

7.3.2. Nodot vai izpaust savus autentifikācijas datus citām personām vai veikt darbības, kas var sekmēt to nonākšanu citu personu rīcībā;

7.3.3. Izmantojot Informācijas resursus, veikt darbības, kas:

7.3.3.1.Vērstas uz noteikto lietotāja tiesību paplašināšanu;

7.3.3.2.Saistītas ar Informācijas resursa drošības sistēmas apiešanu un bojāšanu

7.3.4. Veikt darbības, kas var nodarīt kaitējumu Pārzinim.

7.3.5. Izmantot saņemto informāciju citu datu apstrādes sistēmu izveidei bez saskaņošanas ar resursa turētāju;

7.3.6. Nodot trešajām personām tehniskos resursus, ja tie satur personas datus. Šis aizliegums jāievēro arī gadījumos, kad tehnika tiek nodota utilizācijai.

7.4.Darbinieks ir atbildīgs par Tehniskajiem resursiem, kas nodoti viņa rīcībā, kā arī par darbībām, kas ar tiem tiek veiktas.

## 8. Informācijas arhivēšana iznīcināšana.

8.1.Informācija uzglabājama un arhivējama saskaņā ar pašvaldībai apstiprināto lietu nomenklatūru, kā arī normatīvo aktu noteikumiem un prasībām.

8.2.Informācija, kura vairs nav nepieciešama un paredzēts iznīcināt, iznīcināma tādejādi, ka tās atkārtota lietošana nav iespējama, proti, papīra formātā esošie dokumenti sasmalcināmi pirms izmešanas atkritumu urnā, ierakstu ierīcēs (piemēram, CD, SD, Flash atmiņu kartēs, cietajos diskos, u.tml) esošā informācija dzēšama un pati ierīce padarāma fiziski nelietojama.

8.3.Bez resursu turētāja atļaujas Darbiniekam nav tiesības veikt klientu dokumentācijas iznīcināšanu. Informācijas resursu turētāja pienākumos ietilpst veikt regulāru un sistēmātisku novecojošās Informācijas iznīcināšanu (ne retāk kā vienu reizi mēnesī), ievērojot normatīvajos aktos noteiktos glabāšanas termiņu, vai nodrošināt Informācijas iznīcināšanu, ievērojot individuāli noteiktus glabāšanas termiņus, kas nepārsniedz fizisko personu datu aizsardzības likumā definēto mērķi – līdz datu apstrādes mērķa sasniegšanai.

8.4.Par iznīcināšanas faktu veicams attiecīgs ieraksts vai sastādams akts.

Kārsavas novada pašvaldības domes priekšsēdētāja Ināra Silicka