

Projekts uz 03.03.2023.

Vēlamais izskatīšanas laiks:

Finanšu komitejā 15.03.2023.

domē 22.03.2023.

Ziņotājs: Māris Lazdiņš

APSTIPRINĀTI

Ādažu novada pašvaldības domes sēdē

2023. gada 22. martā (protokols Nr. \_\_ § \_\_)

NOTEIKUMI

Ādažos, Ādažu novadā

2023. gada 22. martā  **Nr. X/2023**

**Ādažu novada pašvaldības Informācijas sistēmu drošības iekšējie noteikumi**

*Izdoti saskaņā ar Ministru kabineta 20.07.2015.*

*noteikumu Nr. 442 „Kārtība, kādā tiek nodrošināta*

*informācijas un komunikācijas tehnoloģiju sistēmu*

*atbilstība minimālajām drošības prasībām”*

*8. un 11. un 25. punktu*

# Vispārīgie jautājumi

1. Šie noteikumi ietver kārtību, kādā Ādažu novada pašvaldībā (turpmāk – Pārzinis) un tās struktūrvienībās un iestādēs (turpmāk – institūcijas) tiek nodrošināta informācijas sistēmu aizsardzība.
2. Noteikumos lietotie termini:
   1. **par tehniskajiem resursiem atbildīgā persona** – Pārziņa atbildīgā persona, kurai ar amata aprakstu uzticēta atbildība par informācijas tehnoloģiju resursiem un to drošību (Informācijas tehnoloģijuadministrators);
   2. **informācijas sistēma** (turpmāk - IS) – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kas nodrošina Pārziņa funkciju izpildei nepieciešamās informācijas ierosināšanu, radīšanu, apkopošanu, uzkrāšanu, apstrādāšanu, izmantošanu un iznīcināšanu;
   3. **IS tehniskie resursi –** serveri, tīkla aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas uzglabāšanai un apritei;
   4. **IS informācijas resursi** – datu faili, datu bāzes, arhīvi, u.c. informācija;
   5. **IS lietotājs** **–** persona, kurai darba pienākumu veikšanai piešķirta datortehnika un piekļuves tiesības darbam Pārziņa IS;
   6. **IS ārējie lietotāji** – personas, kurām ir tiesisks pamats un nodrošinātas tehniskas iespējas piekļūt Pārziņa IS;
   7. **drošības incidents** - jebkāds kaitīgs notikums vai nodarījums, kura rezultātā tiek vai var tikt ietekmēta IS integritāte, konfidencialitāte un pieejamība;
   8. **risks** - varbūtība, ka īstenojoties drošības apdraudējumam, Pārziņa informācijas vai tehniskie resursi varētu mainīties, sabojāties, tikt iznīcināti vai nonākt tādu personu rīcībā, kuras nav tam pilnvarotas, vai piekļūšana informācijas resursiem varētu būt traucēta, vai neiespējama;
   9. **integritāte** - nesankcionēta lietotāja veiktās informācijas izmaiņas nav iespējamas (vai vismaz ir atklātas), un autorizēto lietotāju veiktās izmaiņas tiek izsekotas;
   10. **konfidencialitāte** - informāciju redz un izmanto tikai personas, kurām tas atļauts;
   11. **auditācijas pieraksti** – analīzei pieejami pieraksti, kuros reģistrēti dati par konkrētiem IS notikumiem (piekļuve, datu ievade, maiņa, dzēšana, izvade, u.c.);
3. Šie noteikumi ir saistoši visiem IS lietotājiem.

# II. Informācijas resursu izveidošana, papildināšana, mainīšana, apstrāde, pārraidīšana, glabāšana, atjaunošana un iznīcināšana

1. Ja Pārzinis uzsāk iepirkumu par esošas IS uzlabojumiem, tas nodrošina, ka atbilstošās drošības prasības tiek iekļautas iepirkuma specifikācijā. Jaunas IS izstrādes iepirkuma specifikācijā nosaka:
   1. noteiktu IS uzturēšanas un atbalsta nodrošināšanas (tai skaitā IS drošības nepilnību novēršanas) laikposmu;
   2. IS datorprogrammu pirmkoda un tā izmantošanas tiesību nodošanu Pārzinim ne vēlāk kā pēc noteikta laikposma beigām, kā arī pēc katru izmaiņu vai uzlabojumu veikšanas tajā;
   3. iespēju noteiktajā laikposmā turpināt IS ekspluatēšanu ar IS funkcionēšanai obligāti nepieciešamā programmnodrošinājuma (piemēram, operētājsistēma, datubāzu vadības sistēma, interpretators) jaunākām versijām.
2. Veicot IS izstrādes, iegādes, ieviešanas un pārmaiņu pārvaldīšanas procesu, Pārzinis  
   atbild par IS drošības prasību ievērošanu neatkarīgi no tā, vai šos procesus veic Pārzinis vai ārējais izstrādātājs un piegādātājs.
3. Pārzinis dokumentē IS izstrādes, iegādes, ieviešanas un pārmaiņu pārvaldīšanas norisi.
4. Pārzinis ar rīkojumu nosaka par tehniskajiem resursiem atbildīgo personu. Par tehniskajiem resursiem atbildīgā persona nosaka IS drošības prasības un risku ierobežošanas pasākumus.
5. Sistēmas izstrādes videi ir jāatbilst drošības prasībām, un tai jābūt nodalītai no ikdienas darba vides.
6. Pieejas tiesības IS izstrādes videi nosaka atbilstoši darba pienākumiem.
7. ITN nodrošina IS dokumentācijas sagatavošanu un uzturēšanu.
8. Dokumentācijā iekļauj nepieciešamo informācijas apjomu, lai varētu kvalitatīvi veikt IS lietošanu, uzturēšanu un pārmaiņu pārvaldīšanu.
9. Pirms IS ieviešanas, ITN veic pārbaudi par IS funkcionalitātes un drošības atbilstību noteiktajām prasībām. Pārbaudē piedalās personas, kas ir noteikušas funkcionalitātes un drošības prasības un lietotāji. Pamatojoties uz pārbaudes rezultātiem, ITN nodrošina IS koriģēšanu vai uzsāk tās ieviešanu.
10. **IS ieviešana:**
    1. IS ievieš, saņemot saskaņojumu no tiem informācijas resursu turētājiem, kuru  
       informācijas resursi tiks ietekmēti;
    2. pirms IS nodošanas lietošanā, atbildīgās personas veic darbinieku apmācību  
       un citus pasākumus, lai nodrošinātu izpratni par IS  
       lietošanu, aizsardzības pasākumiem un to nozīmīgumu;
    3. ieviešot IS, tajā nedrīkst būt testētāju lietotāja konti un testēšanas datu faili;
    4. ITN nodrošina, lai tiktu saglabāti ieviestās IS pirmkodi.
11. **IS izmaiņu pārvaldība:**
    1. IS pārmaiņas veic ar visu saistīto informācijas resursu turētāju atļauju;
    2. ITN identificē visus informācijas un tehniskos resursus, kurus ietekmē pārmaiņas;
    3. par tehniskajiem resursiem atbildīgā persona analizē, kā pārmaiņas ietekmēs esošos IS drošības pasākumus un vai pārmaiņu rezultātā nesamazināsies IS drošības līmenis;
    4. ITN veic IS dokumentācijas papildināšanu;
    5. ITN uztur visu pārmaiņu reģistrācijas žurnālu;
    6. pirms izmaiņu ieviešanas veido rezerves kopijas tiem informācijas resursiem, ko  
       var ietekmēt izmaiņas;
    7. pēc izmaiņu ieviešanas par tehniskajiem resursiem atbildīgā persona pārliecinās, vai IS pārmaiņu rezultātā ir saglabāta datu integritāte;
    8. par tehniskajiem resursiem atbildīgā persona izstrādā procedūru par darbībām ārkārtas (neplānotu) pārmaiņu apstākļos un nosaka, kas ir tiesīgs pieņemt lēmumu par ārkārtas pārmaiņām.
12. **IS lietošanas izbeigšana:**
    1. likvidējot vai nododot IS citai personai, ITN veic nepieciešamos drošības pasākumus;
    2. pirms IS likvidācijas, par tehniskajiem resursiem atbildīgā persona organizē risku analīzi, kurā izvērtē iespējamo apdraudējumu citām IS un Pārzinim kopumā;
    3. pašvaldības izpilddirektors nosaka turpmākās darbības ar IS - pilnīga likvidēšana vai glabāšana arhīvā;
    4. ja IS pilnībā likvidē, ITN nodrošina tajā ietilpstošo informācijas resursu likvidēšanu. Ja IS ievieto arhīvā, ITN nodrošina noteikto IS drošības līmeni un  
       likvidē lietošanas tiesības, kuras var atjaunot vēsturisko datu caurskatīšanai ar  
       Pārziņa izpilddirektora lēmumu.

# III. Informācijas un tehnisko resursu lietošana un kontrole

1. Piekļuves tiesības apstiprina pašvaldības izpilddirektors, pēc institūcijas vadītāja rakstveida iesnieguma. Balstoties uz izpilddirektora apstiprinātu pieprasījumu, par tehniskajiem resursiem atbildīgā persona vai ITN izveido lietotājam  
   piekļuvi.
2. Institūcijas vadītājs atbild par ITN informēšanu par lietotājiem, kuri pārtrauc vai maina darba attiecības ar Pārzini un ITN nekavējoties anulē vai izmaina attiecīgā darbinieka piekļuves tiesības.
3. Katrs IS lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa lietotājvārdu  
   (identifikatoru).
4. ITN nodrošina:
   1. automātisku paroles maiņas pieprasījumu, IS lietotājam pirmo reizi reģistrējoties tīklā;
   2. automātisku paroles maiņas pieprasījumu Pārziņa IT jomas normatīvajos aktos noteiktajā kārtībā;
   3. sistēmas bloķēšanu, ja lietotājs piecas reizes pēc kārtas ir ievadījis nepareizu paroli vai lietotājvārdu.
5. Rakstiskā veidā paroles atļauts glabāt tikai aizslēgtā seifā vai izmantojot par tehniskajiem resursiem atbildīgās personas apstiprinātus elektroniskus saglabāšanas līdzekļus.
6. Ja radušās aizdomas, ka paroli uzzinājusi cita persona, IS lietotājs to nekavējoties nomaina un par incidentu ziņo par tehniskajiem resursiem atbildīgai personai.
7. Aizliegts mēģināt uzzināt citu IS lietotāju paroles, izņemot, ja tas nepieciešams par tehniskajiem resursiem atbildīgai personai vai ITN tiešo pienākumu veikšanai. Pēc minēto darbu pabeigšanas IS lietotāja parole tiek nomainīta.
8. Uz datora ir jābūt uzstādītam ekrāna saudzētājam ar aktivizācijas paroli. Tam ir  
   automātiski jāaktivizējas, ja desmit minūšu laikā IS lietotājs nav veicis nekādas darbības.
9. Tehnisko resursu valdītājam ir tiesības veikt lietotāju darbības auditus. Šādi auditi  
   var ietvert lietotāja darbību auditācijas veikšanu
10. Ja institūciju IS uzturēšanai slēdz ārpakalpojuma līgumu ar pakalpojuma sniedzēju, līguma izpildi uzrauga par tehniskajiem resursiem atbildīgā persona un līgumā iekļauj vismaz šādas drošības prasības:
    1. saņemamā ārpakalpojuma aprakstu;
    2. precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;
    3. par tehniskajiem resursiem atbildīgās personas un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā:
       1. par tehniskajiem resursiem atbildīgās personas tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti;
       2. par tehniskajiem resursiem atbildīgās personas tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi;
       3. par tehniskajiem resursiem atbildīgās personas tiesības iesniegt ārpakalpojuma sniedzējam pamatotu rakstisku pieprasījumu nekavējoties izbeigt ārpakalpojuma līgumu, ja par tehniskajiem resursiem atbildīgā persona konstatējusi, ka ārpakalpojumu sniedzējs nepilda ārpakalpojuma līgumā noteiktās prasības attiecībā uz ārpakalpojuma apjomu vai kvalitāti;
       4. ārpakalpojuma sniedzēja pienākumu nodrošināt par tehniskajiem resursiem atbildīgās personas iespēju pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti;
    4. iekļaujot pušu atbildību, atbilstoši Personas datu regulas prasībām, nodrošinot, ka datu saņēmējs/uzglabātājs uzņemas pilnu atbildību par personu datu drošību un apstrādi;
    5. nepieciešamās izmaiņas lietotāju kontos piesakāmas tikai caur vienu atbildīgo personu.

# IV. Piekļūšana informācijas un tehniskajiem resursiem

1. ITN uztur IS dokumentāciju, kas apraksta vismaz:
   1. IS vai to komponenšu drošu konfigurāciju, instalēšanu un darbību;
   2. IS drošības mehānismu izmantošanu un uzturēšanu;
   3. administratīvo / priviliģēto funkciju izmantošanu.
2. Sistēmas dokumentācijai Pārzinis nosaka atbilstošu klasifikācijas līmeni un nodrošina šīs informācijas vai datu atbilstošu aizsardzību un glabāšanu.
3. IS pieejas datiem un tehniskajiem resursiem piešķir tikai un vienīgi tiem darbiniekiem, kuriem tas nepieciešams tiešo darba pienākumu veikšanai.

# V. Informācijas resursu rezerves kopiju izgatavošana un glabāšana

1. ITN nodrošina IS resursu rezerves kopiju veidošanu tām IS un to resursiem, kas ir izvietoti uz institūciju serveriem / darba stacijām.
2. Rezerves kopiju ārējos datu nesējus glabā attālināti no oriģinālajiem datiem, lai novērstu oriģināla un kopijas vienlaicīgas bojāejas iespēju liela apjoma negadījuma situācijā.
3. ITN nosaka vietu, kur tiks glabātas rezerves kopijas uz ārējā datu nesēja.
4. ITN nodrošina institūciju informācijas resursu atjaunošanu no rezerves kopijām.
5. ITN vismaz reizi gadā veic pārbaudi par IS atjaunošanas iespējām no rezerves kopijām.

# VI. Datu nesēju lietošana, pārvietošana, glabāšana un iznīcināšana

1. ITN marķē visus ārējos datu nesējus, kuros ir klasificēta informācija atbilstoši Pārziņa  
   noteiktajai informācijas klasifikācijai.
2. Marķējumā norāda vismaz:
   1. informācijas klasifikācijas līmeni;
   2. informācijas identifikatoru;
   3. izņēmums - datu nesējus pieļaujams nemarķēt, ja tie atrodas slēgtā serveru telpā.
3. Datu nesēju (t.sk. CD, DVD, USB Flash, ārējais cietais disks, vai tml.) fizisko aizsardzību nodrošina katrs IS lietotājs, nodrošinot, ka tie tiek glabāti drošās vietās, lai novērstu trešo personu piekļuvi.
4. Transportējot datu nesējus ārpus Pārziņa kontrolētās zonas, Pārzinis nodrošina atbildību par datu nesēja transportēšanu, kā arī atbilstošu pierakstu veikšanu.
5. ITN organizē un nodrošina elektronisko datu nesēju iznīcināšanu saskaņā ar Pārziņa noslēgto ārpakalpojuma līgumu par īpašo kategoriju atkritumu utilizēšanu un iznīcināšanas rezultātu uzskaiti. Iznīcināšanu veic ITN darbinieka klātbūtnē, izsniedzot atbilstošo dokumentāciju un nodrošinot **foto/video fiksācijas** iespēju.
6. Aizliegts jebkādus elektroniskos datu nesējus izmest sadzīves atkritumos.

# VII. Informācijas lietošana un glabāšana, kas nepieciešama piekļuvei IS informācijai un tehniskajiem resursiem

1. IS lietotājs nedrīkst nodot citiem Pārziņa darbiniekiem un trešajām personām lietotāja rekvizītus (lietotāja vārdu, paroli). Rekvizītus drīkst izmantot tikai konkrētais lietotājs (fiziska persona), kuram tie piešķirti. Autorizētam lietotājam regulāri (konkrētā IS noteiktā laika posmā) jāmaina lietošanas parole.
2. IS lietotājs nedrīkst izdarīt darbības, kas būtu vērstas pret IS drošību, izmantojot neparedzētas pieslēgšanās iespējas. Beidzot (pārtraucot) darbu IS lietotājam jāaizver pārlūkprogramma. IS lietotājs nedrīkst saglabāt lietošanas paroli, izmantojot pārlūkprogrammas iespējas.
3. IS lietotājs nedrīkst veikt nelegālu datu, sistēmas vai tās daļu kopēšanu (par nelegālām tiek uzskatītas visas tās darbības, kuru izpildei netiek izmantotas atļautās, uz ekrāna redzamās komandas, vai kuras tiek izpildītas automātiski, bez cilvēka līdzdalības informācijas pieprasījumu formēšanas procesā, neatkarīgi no šo darbību mērķa).
4. IS lietotājs nedrīkst saņemto informāciju pārveidot, publicēt, pārvadīt piedalīties tās nodošanā vai pārdošanā, reproducējot kopumā vai tās daļas. Jebkuras ar datiem veiktas apstrādes darbības, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu un izpaušanu, bloķēšanu vai dzēšanu drīkst veikt tikai likumdošanā vai Pārziņa iekšējos normatīvajos aktos noteiktajā kārtībā.
5. IS lietotājs nedrīkst no IS saņemto informāciju glabāt publiski pieejamās vietās.
6. Visas IS lietotāja darbības IS uzrauga un iegūto informāciju var izmantot drošības incidentu izmeklēšanā un iespējamo draudu laicīgai novēršanai.

# VIII. Prasības sistēmas informācijas resursu aizsardzībai

1. Pārziņa datortīklu, datoru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī IS lietotāju datoru uzstādīšanu un administrēšanu veic ITN.
2. ITN ir atbildīga par piemērotu un efektīvu aizsardzības sistēmas izveidi, lietojot atbilstošu maršrutēšanas un ugunsmūra sistēmu, kā arī nodrošinot pretvīrusu programmatūras uzstādīšanu un uzturēšanu uz Pārziņa datoriem.
3. ITN ir pienākums regulāri sekot līdzi ugunsmūra paziņojumiem un reaģēt uz vīrusu uzbrukumiem, nodrošinot konstatēto vīrusu iznīcināšanu un būtisko incidentu reģistrēšanu.
4. Ja tiek konstatēti ielaušanās mēģinājumi vai drošības incidenti, ITN veic to reģistrēšanu un izmeklēšanu, kā arī par tās rezultātiem informē personas datu aizsardzības speciālistu un Drošības incidentu novēršanas institūciju (CERT.lv).
5. Vīrusu darbības novēršanai veic šādus pasākumus:
   1. ITN veic pasākumus datoru vīrusu darbības novēršanai tehniskajos resursos, izmantojot šim nolūkam paredzētu programmatūru;
   2. ITN veic antivīrusu programmu pārraudzību, lai pārliecinātos par to darbību un jaunāko vīrusu definīciju failu esamību.
6. ITN izveido, veic izmaiņas un anulē IS lietotāju tiesības.
7. IS lietotājiem, kuri ir institūciju darbinieki, autorizēšanās rekvizītus (lietotājvārdu un sākotnējo paroli) izsniedz ITN, vai arī atbilstošās IS pakalpojumu sniedzējs. IS lietotājiem, kuri nav institūciju darbinieki, autorizēšanās rekvizītus (lietotājvārdu un sākotnējo paroli) izsniedz ITN pēc atbilstošā IS lietotāja identificēšanas.
8. Ja IS lietotājs, kas ir Pārziņa darbinieks, ir aizmirsis savu IS lietotāja paroli, viņš par to personīgi vai telefoniski informē ITN, kas identificē atbilstošo IS lietotāju, izveido jaunu pagaidu paroli un izsniedz lietotājam.
9. ITN nodrošina auditācijas pierakstu veidošanu datortīkla autorizācijai un par IS, kas ir izvietotas uz institūciju resursiem vai kuras ir institūcijas īpašumā. Auditācijas pierakstos iekļauj visus veiksmīgus un neveiksmīgus pieslēgšanās gadījumus, to datumus un laiku, kā arī šo IS lietotāju (t.sk. administratora) vārdus vai citu autentifikācijas līdzekli. ITN nodrošina auditācijas pierakstu integritāti un regulāri veido auditācijas pierakstu datu rezerves kopijas.
10. ITN nodrošina, ka pirms jaunas IS pieņemšanas ekspluatācijā tai ir veikti lokāli ielaušanās testi, kuru veikšanai var pieaicināt ārpakalpojumu sniedzējus vai ITN darbiniekus, kuri nav piedalījušies IS izstrādē.
11. Reģistru par iegādātiem un uzstādītiem informācijas tehniskajiem resursiem (t.sk. par darba stacijām, serveriem un perifērijas iekārtām) veic Grāmatvedības nodaļa. Vismaz reizi gadā tiek veikta šo resursu inventarizācija, pārliecinoties, vai reģistrs ir korekts.
12. ITN nodrošina Pārziņa datortīkla / informācijas sistēmas atbilstību šādām aizsardzības prasībām:
    1. iekšējo datortīklu nodala no interneta ar ugunsmūra palīdzību;
    2. datortīkliem un IS ir pretvīrusu aizsardzība;
    3. datortīklu / IS darba vides drošības apdraudējumu pastāvīga novēršana, izmantojot ielaušanās mēģinājumu noteikšanu un aizsardzības sistēmu;
    4. attālinātas piekļuves ierobežošana datortīklu / IS administrēšanai izmantojot tikai šifrētu pieslēgumu un daudzfaktoru autentifikāciju;
    5. atsevišķi savietojamās sistēmas un savietotāja uzlabojumu testēšana šīm vajadzībām izveidotā savietotāja fiziskā vai loģiskā līmenī un no savietojamās sistēmas nodalītā testa vidē;
    6. piekļuve datortīklu / IS administrēšanas un pārvaldības funkcionalitātei tikai tām personām, kurām datortīklu / IS esošā informācija atbilstošā apmērā ir nepieciešama darba pienākumu veikšanai;
    7. IS lietotāji, kas veic sistēmas administrēšanas darbu, izmanto īpašus lietotāju kontus (piemēram, sistēmas administratora konts), kas netiek izmantoti ikdienas darbību veikšanai;
    8. katrs IS lietotāja konts ir saistīts ar konkrētu fizisko personu. Pretējā gadījumā IS jābūt iestrādātiem tehniskiem līdzekļiem, kas novērš iespēju IS lietotājiem izmantot šādus kontus;
    9. IS lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī IS lietotāja autentifikācijas procesa ietvaros;
    10. IS lietotāja parole ievadīšanas brīdī lietotājam netiek pilnībā attēlota;
    11. IS lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā ir lietojama vienu reizi un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas;
    12. IS nav pieļaujama funkcionalitāte, kas atļauj IS lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;
    13. iekārtām, tai skaitā infrastruktūras iekārtām, kas nodrošina IS funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles;
    14. nodrošināta IS auditācijas pierakstu veidošana un uzglabāšana vismaz sešus mēnešus pēc ieraksta izdarīšanas;
    15. jebkura piekļuve IS ir izsekojama līdz konkrētam IS lietotāja kontam vai interneta protokola (IP) adresei;
    16. IS jābūt uzliktiem programmatūras visiem pieejamiem atjauninājumiem, iepriekš izvērtējot to nepieciešamību;
    17. visās institūciju valdījumā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos IS, jābūt iekļautai pretvīrusu funkcionalitātei;
    18. IS funkcionalitāte ir izpildāma ar minimāli iespējamām tiesībām;
    19. piecas secīgas reizes nepareizi ievadot IS lietotāja konta paroli, šis konts (izņemot IS administratora kontu) nekavējoties tiek bloķēts;
    20. ar IS administratora kontu piekļūt IS, izmantojot iekārtas, kas atrodas ārpus institūciju telpām, kā arī iekārtas, kas neatrodas institūciju valdījumā, iespējams tikai izmantojot daudzfaktoru autentifikāciju;
    21. fiziski piekļūt iekārtām, kas nodrošina IS darbību, atļauts vienīgi institūciju pilnvarotām personām;
    22. IS lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai IS lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību atrisinātu kļūdu;
    23. plūsma starp IS un tās IS lietotājiem, kā arī starp IS un citām IS tiek kontrolēta, piemēram, izmantojot ugunsmūri;
    24. datortīkla pakalpojumi, kas netiek izmantoti IS darbības nodrošināšanai, ir atslēgti;
    25. veicot IS izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu IS glabāto datu integritātei;
    26. IS izvietošana ārpakalpojuma sniedzēja nodrošinātos resursos atļauta tikai tad, ja pakalpojuma sniedzējs ir juridiska persona, kas reģistrēta Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, un sistēmā glabātā informācija atrodas vienīgi Eiropas Savienības vai Eiropas Ekonomikas zonas valstu teritorijā.

# IX. Prasības sistēmas tehnisko resursu aizsardzībai pret fiziskas iedarbības radītu sistēmas drošības apdraudējumu

1. IS serveri, datortīkla un to saistīto aprīkojums tiek ekspluatēts ierobežotas pieejas telpās (turpmāk - serveru telpas), kurām iespēja piekļūt ir ITN, nodrošinot aizsardzību pret neautorizētu personu iespēju serverus izslēgt, pārvietot, bojāt un nesankcionēti mainīt to konfigurāciju.
2. Serveru telpām jābūt aprīkotām ar:
   1. ugunsgrēka signalizācijas iekārtu;
   2. ugunsdzēšamo aparātu;
   3. gaisa kondicionēšanas iekārtu;
   4. nepārtrauktās barošanas avotu (UPS);
   5. apsardzes signalizāciju.
3. Serveru telpās pieeja tiek nodrošināta:
   1. Carnikava, Stacijas iela 5, piekļuve tikai ITN darbiniekiem;
   2. Carnikava, Stacija iela 7, piekļuve ITN darbiniekiem, aģentūras "Carnikavas komunālserviss" elektriķiem, TET inženieriem;
   3. Carnikava, Garā iela 20, piekļuve ITN darbiniekiem, aģentūras "Carnikavas komunālserviss" elektriķiem, signalizācijas apkalpojošam uzņēmumam;
   4. Carnikava, Nākotnes iela 1, piekļuve ITN darbiniekiem, pamatskolas apsaimniekotājam, aģentūras "Carnikavas komunālserviss" elektriķiem, signalizācijas apkalpojošam uzņēmumam, BMS sistēmas apkalpojošajam uzņēmumam;
   5. Ādaži, Gaujas iela 33A, piekļuve ITN un centrālās administrācijas administrācijas darbiniekiem.
4. Personām, kuras nav noteiktas 60. punktā, aizliegts ieiet serveru telpās.
5. Nepiederošas personas, t.sk. ārpakalpojumu sniedzēji, serveru telpās drīkst uzturēties tikai ITN darbinieka klātbūtnē.
6. Pazūdot elektrībai, ITN ir pienākums maksimāli īsā laikā organizēt elektrības padeves traucējumu novēršanu, ziņojot pašvaldības aģentūras “Carnikavas komunālserviss” galvenajam enerģētiķim vai saimniecības pārzinim traucējumus un nodrošināt pieslēgumu no cita enerģijas avota vai arī ja tas nav iespējams un serveriem nav nodrošināta izslēgšanās automātiski, uzsākt manuālu serveru izslēgšanu.
7. Informācijas sistēmas lietotāju darba stacijas atrodas ierobežotas pieejas telpās, kā arī uz tām ir uzstādīts nepārtrauktās barošanas avots (UPS), ja elektroenerģijas padeves traucējumu risks ir nepieņemami liels.

# X. Kārtība, kādā novēro sistēmas drošības apdraudējuma tuvošanās pazīmes

1. Par tehniskajiem resursiem atbildīgā persona organizē regulāru IS auditācijas pierakstu uzraudzību un analīzi, lai konstatētu incidentus.
2. Par tehniskajiem resursiem atbildīgā persona periodiski organizē IS lokālus ielaušanās testus. Vājās vietas tiek uzraudzītas un novērstas.
3. Par tehniskajiem resursiem atbildīgā persona organizē, ka vismaz reizi gadā tiek veikta informācijas tehnoloģiju drošības pārbaude (t.i. izmantotās IS drošības dokumentācijas un pasākumu atbilstības pārbaude) un atbilstoši tās rezultātiem tiek organizēta atklāto trūkumu novēršana.

# XI. Drošības incidentu atklāšana un pārvaldīšana

1. IS drošības apdraudējuma pazīmes nosaka, veicot nepārtrauktu tās resursu uzraudzību, kas nodrošina automātisku paziņošanu, potenciālā apdraudējuma iespējamībai sasniedzot noteiktus parametrus.
2. Par atklātajām IS ievainojamībām, vai, ja notikusi ļaunprātīga ielaušanās sistēmā, iejaukšanās vai nesankcionēta piekļuve personas datiem, IS lietotājs nekavējoties informē par tehniskajiem resursiem atbildīgo personu vai ITN.
3. Darba laikā lietotājam ir tiesības lūgt ITN atbalstu IS un ar to saistītu resursu lietošanā. Ja atbalsts vajadzīgs nekavējoties un ārpus darba laika, lietotājs nosūta jautājumu SMS vai e-pastā. Izvērtējot iespējamos riskus IS drošībai, par tehniskajiem resursiem atbildīgā persona vai ITN lemj par nekavējošu atbildes reakciju, vai nākamajā darba dienā, informējot par to lietotāju.
4. Par tehniskajiem resursiem atbildīgā persona vai ITN nodaļa, izvērtē notikumu un gadījumos, ja noticis **drošības incidents, kas apdraud IT integritāti, pieejamību vai konfidencialitāti, nekavējoties informē CERT (Informācijas tehnoloģiju drošības incidentu novēršanas institūciju)** t. 67085888 (ziņojumu pieņemšana 24 x 7, CERT.LV darba laiks - darba dienās) [cert@cert.lv](mailto:cert@cert.lv), [cert@cert.gov.lv](mailto:cert@cert.gov.lv).
5. Ja risks skar personu datus, nekavējoties jāinformē datu aizsardzības speciālists pašvaldības oficiālajā e-pastā, ar norādi *“Personas datu aizsardzības speciālistam”*.

# XII. Sistēmas darbības kārtība, ja informācijas vai tehniskie resursi nav pieejami pilnā apjomā

1. Sistēmas bojājumu novērtējumu veic par tehniskajiem resursiem atbildīgā persona.
2. Par tehniskajiem resursiem atbildīgā persona informē IS lietotājus par laiku, kādā tiks atjaunota IS darbība.

# XII. Sistēmas tehnisko resursu maiņas kārtība

1. Ja Pārzinis ir pieņēmis lēmumu mainīt IS, vai ar to saistītos tehniskos resursus, tas vismaz 2 nedēļas iepriekš informē IS lietotājus.
2. IS vai tehnisko resursu maiņa tiek veikta iespējami mazāk ietekmējot ikdienas gaitu institūcijās.
3. Ja nepieciešams, ITN nodrošina apmācības vai tehnisko atbalstu jauno IS vai tehnisko resursu lietošanā.

# XIII. Darbinieku apmācība un zināšanu pārbaude sistēmas drošības jomā

1. Pārzinis nodrošina, ka vismaz reizi gadā par tehniskajiem resursiem atbildīgā persona apmeklē Drošības incidentu novēršanas institūcijas organizētu apmācību informācijas tehnoloģiju drošības jautājumos.
2. Pārzinis nodrošina, ka ne retāk kā reizi gadā tiek veikta darbinieku instruktāža informācijas tehnoloģiju drošības jautājumos.
3. ITN, tā pilnvarota persona vai ārējs konsultants veic IS lietotāju apmācību IS drošības jomā, izskaidrojot tiem IS drošības pamatprincipus un drošības pasākumus IS un datu drošībai.

# XIV. Ieviešamo sistēmas jauninājumu ietekmes uz tās drošību izvērtēšana

1. Pirms atjauninājumu uzstādīšanas IS:
   1. pārliecinās, ka atjauninājumi nemazina sistēmas drošības līmeni vai zudumu  
      iespējams kompensēt ar adekvātām kontrolēm, kas mazina risku;
   2. pārmaiņas veic organizēti un atbilstoši iestādes IS drošības politikas  
      uzstādījumiem;
   3. par tehniskajiem resursiem atbildīgā persona un ITN ir informēti par uzstādāmajām pārmaiņām.

# XV. Sistēmas pierakstu datņu veidošana, uzglabāšana, apstrāde un dzēšana

1. IS jābūt konstruktīvi un programmatiski aizsargātai ar aizsardzības risinājumiem pret satura dzēšanu vai pārrakstīšanu. Piekļuve IS pierakstu datnēm ir tikai par tehniskajiem resursiem atbildīgai personai un ITN darbiniekiem, kam piešķirtas attiecīgas pilnvaras.
2. Jebkāda datu dzēšana atļauta tikai ar par tehniskajiem resursiem atbildīgās personas rīkojumu.

# XVI. Nobeiguma jautājumi

1. Šos noteikumus pārskata reizi gadā, kā arī:
   1. ja izmaiņas IS var ietekmēt IS drošību;
   2. ja ir mainījušies vai atklāti jauni IS drošības apdraudējumi;
   3. ja pieaug IS drošības incidentu skaits vai noticis nozīmīgs incidents;
   4. ja izmaiņas iestādes struktūrā skar IS drošības vadības organizāciju;
   5. ja izdarīti grozījumi normatīvajos aktos, kas regulē IS darbību.
2. Ar šo noteikumu parakstīšanu spēkā spēku zaudē:
   1. Carnikavas novada domes 2018. gada 25. aprīļa noteikumi Nr. INA/2018/15 “Iekšējie informācijas sistēmu drošības noteikumi”;
   2. Ādažu novada domes 2020. gada 25. augusta noteikumi Nr. 12 “Informācijas sistēmu drošības noteikumi”.

Pašvaldības domes priekšsēdētāja K.Miķelsone

*Sadale: @ ITN, PSN, IDR*