**LATVIJAS REPUBLIKA**
**TĒRVETES NOVADA DOME**
Reģ.Nr.90001465562
"Zelmeņi", Tērvetes pagasts, Tērvetes novads, LV-3730, tālr.63726012, fakss 63726012,
e-pasts:tervetesnd@zemgale.lv

**TĒRVETES NOVADA TĒRVETES PAGASTĀ**

APSTIPRINĀTI
ar Tērvetes novada domes
2016.gada 28. aprīļa
sēdes lēmumu (protokols Nr.7, 13. §)

# Tērvetes novada domes Informācijas tehnoloģiju drošības noteikumi

Izdoti saskaņā ar
Informācijas tehnoloģiju drošības likuma
8.panta ceturto daļu,
likuma "Par pašvaldībām" 43. panta
pirmās daļas 2. punktu

## 1.Vispārīgie jautājumi

1.1. Tērvetes novada domes (turpmāk – TND) Informācijas tehnoloģiju (IT) drošības noteikumi (turpmāk – noteikumi) izstrādāti saskaņā ar Informācijas tehnoloģiju drošības likumu.

1.2. Noteikumi domāti Tērvetes novada pašvaldības administrācijai un pašvaldības iestādēm (turpmāk – iestādes).

1.3. Noteikumi nosaka kārtību, kādā iestādes nodrošina tām piederošo informācijas un tehnisko resursu (turpmāk – resursu) aizsardzību.

1.4. Noteikumu mērķis ir:

1.4.1. apliecināt TND vadības apņemšanos nodrošināt iestādē resursu drošību, lai uzturētu to integritāti, pieejamību un konfidencialitāti,

1.4.2. nodrošināt iestādēs vienādu un sistemātisku pieeju informācijas tehnoloģiju drošības jautājumu risināšanai,

1.4.3. panākt iestāžu darbinieku izpratni par informācijas tehnoloģiju drošības jautājumiem,

1.4.4. būt par pamatu procedūru, instrukciju un citu nepieciešamo drošības dokumentu izstrādē un ieviešanā.

1.5. Noteikumu ievērošana ir obligāta visiem TND darbiniekiem.

## 2. Noteikumos lietotie termini

2.1. **Informācijas resursi** – sistēmprogrammas, lietojumprogrammas, sistēmu un datu faili un cita informācija, ko izmanto informācijas apstrādei, pārraidei, glabāšanai un citu funkciju veikšanai.

2.2. **Tehniskie resursi** – datori, tīkla aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas apstrādei, pārraidei un glabāšanai.

2.3. **Informācijas sistēma (IS)** – informācijas un tehnisko resursu kopums.

2.4. **Resursu turētājs** – TND izpilddirektors vai ar izpilddirektora rīkojumu iecelts iestādes darbinieks, kurš atbild par IT drošības pārvaldību.

2.5. **IT drošības pārzinis** – TND IT administrators vai ārpakalpojuma sniedzējs, kurš nodrošina IT drošības pārvaldību.

2.6. **Resursu aizbildnis** – resursu turētāja vai ārpakalpojuma sniedzēja norīkota persona, kura atbild par resursu funkcionēšanu un/vai saturu.

2.7. **Resursu lietotājs** – iestādes darbinieks, kurš izpilda noteiktus pienākumus, atbilstoši kuriem darbiniekam ir piešķirtas tiesības lietot noteiktus resursus.

2.8. **Informācijas integritāte** – raksturo, cik lielā mērā informācija ir pilnīga, patiesa, precīza un aktuāla.

2.9. **Informācijas pieejamība** – raksturo, vai lietotāji var piekļūt nepieciešamajai informācijai ne vēlāk kā noteiktā laikā pēc informācijas pieprasīšanas brīža.

2.10. **Informācijas konfidencialitāte** – raksturo, cik lielā mērā informācija ir pieejama tikai šīs informācijas saņemšanai paredzētajiem lietotājiem.

2.11. **Informācijas vērtība** – informācijas nozīmīgums iestādes funkciju veikšanai.

2.12. **Drošības incidents** – notikums vai nodarījums, kura rezultātā tiek apdraudēta informācijas resursu integritāte, pieejamība vai konfidencialitāte.

2.13. **Auditācijas pieraksti** - analīzei pieejams resursu veikto darbību (piekļūšana, datu ievade, mainīšana, dzēšana, izvade) atspoguļojums elektroniskas informācijas veidā.

2.14. **Drošības dokumenti** – dokumentu kopums, kas apraksta iestādes resursu lietošanas kārtību.

2.15. **Risku pārvaldīšana** – Informācijas sistēmu risku identificēšana, novērtēšana, samazināšana un kontrolēšana, kuras ietvaros tiek veikta informācijas sistēmu risku ierobežošana līdz iestādei pieņemamam līmenim.

2.16. **Ārpakalpojuma sniedzējs** - trešā persona, kas uz līguma pamata nodrošina iestādes IT drošības pārvaldību vai citas funkcijas.

## 3. Ārpakalpojuma pārvaldība

3.1. Iestādes IT drošības pārvaldību, attīstību un/vai drošību var nodrošināt ārpakalpojuma sniedzējs.

3.2. Iestāde veic ārpakalpojumu uzraudzību un atbild par ārpakalpojuma sniedzēja veikumu kā par savu.

3.3. Ārpakalpojuma līgumā jāiekļauj IT drošības likumā noteiktie pienākumi.

## 4. Resursu pārvaldība

4.1. Resursu turētājs norīko **IT drošības pārzini**, kura pienākums ir:

4.1.1. organizēt iestādes IT drošības noteikumu izstrādi,

4.1.2. nodrošināt izmaiņu pārvaldību,

4.1.3. uzturēt (apstiprināt) aktuālas izmaiņas drošības dokumentos.

4.2. Resursu turētājs norīko visiem vai atsevišķiem resursiem **resursu aizbildni,** kura pienākums ir:

4.2.1. nodrošināt resursu normālu (pareizu) darbību,
4.2.2. nodrošināt resursu lietotāju pārvaldību,
4.2.3. pildīt citus iestādes IT drošības noteikumos uzliktos pienākumus,
4.2.4. veikt kopā ar resursu turētāju risku aktualizāciju.
4.2.5. **Resursu lietotājiem** ir pienākums ievērot iestādē apstiprinātos IT drošības noteikumus.

## 5. Informācijas resursu klasifikācija

5.1. Resursu turētājs sadarbībā ar IT administratoru veic visu informācijas resursu klasifikāciju ar mērķi novērtēt to nozīmību pēc **konfidencialitātes, vērtības un pieejamības** (pielikumā).

5.1.1. **Informācijas konfidencialitātes** līmeni nosaka, ņemot vērā kaitējumu, kas varētu tikt nodarīts iestādei, ja informācijai piekļūst nepilnvarotas personas.

5.1.1.1. **Publiska informācija (P)** – nav svarīga konfidencialitātes aspektā, tā ir brīvi pieejama iestādes darbiniekiem, jebkurai personai vai organizācijai, kas to ir pieprasījusi. Šīs informācijas izplatīšana neietekmē iestādi negatīvā veidā.

5.1.1.2. **Ierobežotas pieejamības informācija (I)** – ir svarīga konfidencialitātes aspektā, tās pazīmes noteiktas Informācijas atklātības likuma 5., 6., un 7. pantā. Šī informācija ir pieejama tikai iestādes darbiniekiem, kuriem ir piešķirtas šādas tiesības.

5.1.2. **Informācijas vērtības (V)** līmeni nosaka atkarībā no kaitējuma, kas varētu būt nodarīts iestādei, ja netiktu nodrošināta informācijas resursu integritāte, pēc šādas skalas:

- V1 - augstas vērtības informācija,
- V2 - vidējas vērtības informācija,
- V3 - zemas vērtības informācija.

5.1.3. **Informācijas pieejamības** līmeņus nosaka atkarībā no iestādes darbības jomas, ņemot vērā kaitējumu, kas varētu tikt nodarīts iestādei vai tās klientiem, ja netiktu nodrošināta resursu pieejamība. Informācijas pieejamības līmeni nosaka pēc šādas skalas:

- P1- informācija pieejama 24 stundas diennaktī, 7 dienas nedēļā,
- P2 - informācija pieejama iestādes darba laikā.

5.2. Resursi, kuriem nav piešķirts neviens no konfidencialitātes, vērtības vai pieejamības līmeņiem, tiek uzskatīti par **neklasificētiem** un tiem nav jāveic risku analīze.

## 6. Tīklu infrastruktūra

Iestādes resursu turētājs nodrošina pietiekamu fizisko aizsardzību tīkla aparatūrai un kabeļiem, tos izvietojot tādējādi, lai tiem nevarētu nesankcionēti, nemanīti vai aiz nejaušības piekļūt, pieslēgties vai kā citādi bojāt.

## 7. Darbstaciju fiziskā aizsardzība

7.1. Darbstacijas lieto atbilstoši ražotāja noteiktajām prasībām.

7.2. Iestādē lieto elektroenerģijas nepārtrauktas piegādes iekārtas, ja elektroenerģijas piegādes traucējumu radītais risks ir nepieņemami liels.

## 8. Portatīvo iekārtu fiziskā aizsardzība

Portatīvos datorus lieto atbilstoši ražotāja noteiktajām prasībām.

## 9. Datu nesēju fiziskā aizsardzība

9.1. Datu nesējus, kas satur informācijas resursus, lietot un pārvietot bez īpaša laika ierobežojuma drīkst tikai resursu turētāja pilnvaroti darbinieki, kuriem ir pieeja informācijas resursiem. Informācijas resursi, kurus nav nepieciešams lietot vai pārvietot, tiek glabāti iestādes telpās tam paredzētās vietās. Ja ir nepieciešams iznīcināt datu nesējus, to iznīcināšanu uzrauga vai nodrošina IT drošības pārzinis.

9.2. Resursu lietotājiem datu nesējus ar klasificētiem informācijas resursiem aizliegts atstāt nedrošās, publiski pieejamās vietās.

9.3. Ja datu nesēju, kas satur klasificētus informācijas resursus, ir paredzēts iznīcināt, tad to izdara tādā veidā, lai nebūtu iespējams veikt uz tā esošo datu atjaunošanu.

## 10. Klasificētie resursi

10.1. Nepieciešamības gadījumā resursu turētājs veic papildu fiziskās aizsardzības pasākumus atkarībā no resursu klasifikācijas.

10.2. Resursu turētājs sistemātiski veic informācijas sistēmas fiziskās aizsardzības pasākumus, nepieļaujot situāciju, ka informācijas resursi atrastos ārpus ierobežotas pieejamības telpām bez resursu turētāja pilnvarotu iestādes darbinieku uzraudzības. Resursu turētājs regulāri veic fiziskās aizsardzības pasākumu pārbaudi.

## 11. Piekļuves kontrole

11.1. Katram resursu lietotājam tiek piešķirts lietotāja vārds un parole, kā arī noteiktas piekļuves tiesības. Lietotājs ir atbildīgs par piešķirtā lietotāja vārda un paroles lietošanu, saglabāšanu un neizpaušanu.

11.2. Resursu turētajam vai tā pilnvarotai personai ir jāinformē IT drošības pārzini par tiem darbiniekiem un studējošajiem, kuri pārtrauc darba vai studiju attiecības ar TND. IT drošības pārzinis pēc šīs informācijas saņemšanas nekavējoties anulē visas attiecīgā lietotāja piekļuves tiesības iestādes informācijas sistēmas resursiem.

11.3. Lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa lietotāja vārdu. Lietotāja autentiskumu nosaka, lai pārliecinātos, ka lietotāja vārda izmantotājs ir sankcionētais tā turētājs. Autentiskuma noteikšanai tiek izmantotas paroles. Pēc lietotāja vārda un paroles ievadīšanas lietotājs var izmantot informācijas resursu atbilstoši noteiktajām piekļuves tiesībām.

11.4. Par paroli nedrīkst izmantot personu identificējošus datus (piemēram, personas datus, automašīnas numuru, radu vārdus vai uzvārdus, vārdus, kas saistīti ar darbavietu vai kas bieži tiek tajā lietoti).

11.5. Lietotāji paši ir atbildīgi par savu paroļu drošu glabāšanu.

11.6. Lietotājam pirmo reizi autorizējoties sistēmās, parole ir jānomaina.

11.7. Par paroli jāizvēlas pietiekami sarežģīta simbolu kombinācija. Paroles garumam ierobežotas pieejamības resursiem ir jābūt vismaz 8 (astoņiem) simboliem. Administratoru parolēm jābūt 10 (desmit) simbolu garām. Lietotāja vārdiem un parolēm dažādos resursos ir jāatšķiras.

11.8. Lietotājam regulāri, ne retāk kā 1 (vienu) reizi gadā jāmaina lietošanas parole resursiem, kas klasificēti ar augstas konfidencialitātes līmeni.

11.9. Lietotājam parole ir jāiegaumē. Rakstiskā veidā paroles atļauts glabāt tikai aizslēgtā seifā ar ierobežotu pieeju vai izmantot speciāli šim nolūkam paredzētus rīkus.

11.10. Lietotājam ir aizliegts izpaust jebkuru piešķirto paroli, kā arī citu konfidenciālu informāciju, kas saistīta ar IT resursu izmantošanu. Par katru darbību, kas veikta datoru tīklā, datu bāzēs, kā arī citās informatīvās sistēmās, ir atbildīgs izmantotā lietotāja vārda un paroles īpašnieks.

11.11. Izmantojot TND IT resursus publiskās vietās, lietotajam ir jāpārliecinās, ka, beidzot darbu, sistēma ir pieejama tikai no jauna autentificējoties –lietotājam ievadot lietotāja vārdu un paroli.

11.12. Ja lietotājs konstatē, ka kāds cits ir uzzinājis viņa paroli, lietotājs to nekavējoties nomaina un par to nekavējoties ziņo IT drošības pārzinim.

11.13. Aizliegts mēģināt uzzināt citu lietotāju paroles. IT drošības pārzinim, instalējot sistēmu, jānomaina noklusētās paroles.

## 12. Datu rezerves kopiju veidošana

12.1. Regulāri veic svarīgāko koplietošanas informācijas resursu un programmatūru rezerves datu kopēšanu. Rezerves datu kopēšanu nodrošina IT drošības pārzinis, un to biežums un apjoms tiek saskaņots ar resursu turētāju.

12.2. IT drošības pārzinis pārbauda, ka rezerves kopiju veidošanas process ir beidzies sekmīgi.

12.3. Reizi gadā IT drošības pārzinis pārbauda iespēju no rezerves kopijām atjaunot informācijas resursu datus.

12.4. Rezerves datu kopijas tiek glabātas tikai šim mērķim paredzētā datu nesējā.

## 13. Vīrusu kontrole

13.1. IT drošības pārzinis nosaka kārtību un veic pasākumus datorvīrusu darbības novēršanai informācijas sistēmās.

13.2. Vīrusu darbības novēršanai lieto speciāli šim nolūkam paredzētu programmatūru. Vīrusu definīciju failus nekavējoties atjauno, tiklīdz izstrādātājs tos piedāvā.

13.3. IT drošības pārzinis regulāri veic antivīrusu programmas pārraudzību, lai pārliecinātos par tās darbību un jaunāko vīrusu definīciju failu esamību.

## 14. Personālo un portatīvo datoru aizsardzība

14.1. Portatīvajos datoros, kuri tiek lietoti ārpus iestādes darba telpām, glabā tikai to informāciju, kas nepieciešama noteiktajā laikā noteiktajam datora lietotājam.

14.2. Personālajā datorā uzstāda un lieto tikai to programmatūru un tādā konfigurācijā, ko ir noteicis resursu turētājs. IT drošības pārzinis personālā datora funkcionalitāti ierobežo līdz darba vajadzībām nepieciešamo funkciju līmenim.

14.3. Lietotājam atstājot datoru bez uzraudzības, to slēdz, lietojot ekrānsaudzētāju ar paroli, speciālu slēgšanas funkciju vai citu metodi, kas ļauj turpināt darbu ar šo datoru vienīgi tad, ja ir veikta lietotāja autentifikācija.

## 15. Datortīklu aizsardzība

15.1. IT drošības pārzinis izstrādā un uztur datortīkla shēmu, kurā parādīta datortīklā savienotā aparatūra un nodrošinātie pakalpojumi.

15.2. Datu plūsmā starp lokālo datortīklu un ārējo datortīklu atļauj tikai tos pakalpojumus, kas ir nepieciešami iestādes funkciju izpildei.

15.3. IT drošības pārzinis pārbauda visu ārējo savienojumu eksistenci un pārliecinās, ka pastāv tikai tie savienojumi, kuri atbilst iestādes darbības vajadzībām, un ka darbojas rezerves savienojumi.

15.4. Pieslēgšanos iestādes informācijas sistēmām no loģiski attālas vietas aizsargā, lietojot kriptogrāfijas līdzekļus kopā ar lietotāja vārdu tā, lai droši noteiktu lietotāja autentiskumu.

15.5. IT drošības pārzinis pēc nepieciešamības iesaka papildu loģiskās aizsardzības pasākumus atkarībā no informācijas resursu klasifikācijas.

15.6. IT drošības pārzinim ir pienākums reaģēt uz vīrusu uzbrukumiem, nodrošinot konstatēto vīrusu iznīcināšanu un būtisko incidentu reģistrēšanu. Gadījumā, ja tiek konstatēti virtuālās ielaušanās mēģinājumi vai citi būtiski incidenti, IT drošības pārzinis veic to reģistrēšanu un izmeklēšanu, kā arī par tās rezultātiem informē resursu turētāju.

## 16. TND sadarbība ar ārējiem informācijas tehnoloģiju pakalpojumu sniedzējiem

16.1. Ja TND izvēlas resursa uzturēšanu uzticēt ārējam pakalpojumu sniedzējam, tam jānodrošina drošības līmenis, kas nav zemāks par šajos noteikumos noteikto.

16.2. TND nosaka informācijas izpaušanas ierobežojumus.

16.3. Ārpakalpojuma līgumā jāiekļauj Informācijas tehnoloģiju drošības likumā noteiktie pienākumi.

16.4. Saskaņojot ar resursu turētājiem, piešķir pieejas tiesības informācijas resursiem ārējiem informācijas tehnoloģiju pakalpojumu sniedzējiem tikai to pienākumu veikšanai nepieciešamajā apjomā.

16.5. Visas izmaiņas (sistēmas informācijas resursu izveidošana, papildināšana, mainīšana, apstrāde, pārraidīšana, glabāšana, atjaunošana un iznīcināšana) notiek atbilstoši TND IT izmaiņu pārvaldības prasībām.

**17. Drošības incidentu pārvaldība**

17.1. Incidentu pārvaldību veic ar mērķi samazināt drošības incidenta ietekmi uz iestādes normālu darbību.

17.2. IT drošības pārzinis identificē drošības incidentu pēc jebkura no minētajiem kritērijiem:

- notiek uzbrukums resursiem no ārpuses,
- notiek svarīgu resursu atteice,
- apgrūtināta iestādes normāla darbība,
- apgrūtināta būtisku pakalpojumu sniegšana.

17.3. Drošības incidenta gadījumā IT drošības pārzinis:

- informē Informācijas tehnoloģiju drošības incidentu novēršanas institūciju CERT.LV,
- saglabā pierādījumus,
- atjauno informācijas sistēmas darbību,
- reģistrē drošības incidentu žurnālā.

Domes priekšsēdētāja Dace Reinika

APSTIPRINĀTS
ar 2016.gada 28.aprīļa sēdes lēmumu (protokols Nr.7, 13.§)

# RESURSU KLASIFIKĀCIJA UN AIZBILDŅI

| Nr | Resurss | Informācijas sistēma | Informācijas vērtība | Inform.konfidencialitāte | Informāc. Pieejamība | Resursu aizbildnis (saturs) | Resursu aizbildnis (funkcionēšana) |
|---|---|---|---|---|---|---|---|
| 1 | Lietvedība | Lietvedības dokumenti elektroniskā formā | V2 | PI | P2 | Sekretāre I.Meija | IT administrators A.Narvaišs |
| 2 | Personāla daļa | Personāla daļas dokumenti elektroniskā formā | V1 | I | P2 | Personāla speciāliste S.Hibšmane | Ārpakalpojuma sniedzējs SIA ZZ Dats, IT administrators A.Narvaišs |
| 3 | Grāmatvedība | Grāmatvedības sistēmas | V1 | I | P2 | Galv.grāmatv. A.Anuža | Ārpakalpojuma sniedzējs SIA ZZ Dats (tīkla progr.), IT administrators A.Narvaišs (lokālās progr.) |
| 4 | Iestādes resursi | Iestādes darbības nodrošināšanai nepieciešamie dokumenti elektron.formā | V2 | PI | P2 | Lietotāji | IT administrators A.Narvaišs |
| 5 | IT daļa | Iestādes darbinieku IT sistēmu pieejas tiesību saraksts, u.c. | V1 | I | P2 | IT administrat. A.Narvaišs | IT administrators A.Narvaišs |
| 6 | Valsts Inform.sistēma | Valsts informācijas sistēmas, ar kurām iestāde apmainās ar informāciju | V1 | I | P2 | Lietotāji | IPS ( par datu komunikāciju) un VIS pārzinis (par VIS darbību) |
| 7 | Iestādes interneta vietne | Informācija par iestādi interneta tīmekļa vietnē | V2 | P | P1 | Sab.attiecību speciālisti | Ārpakalpojuma sniedzējs LU MII |

*V1 - augstas vērtības informācija,*

*V2 - vidēja vērtības informācija,*

*V3 - zema vērtības informācija*

*P – publiska informācija - brīvi pieejama jebkurai personai*

*I – ierobežotas pieejamības informācija*

*O – neklasificēti resursi*

P1 – *informācija pieejama 24 stundas diennaktī, 7 dienas nedēļā*

*P2 - informācija pieejama iestādes darba laikā.*