BABĪTES NOVADA PAŠVALDĪBAS DOME

Reģ. Nr. 90000028870
Centra iela 4, Piņķi, Babītes pagasts, Babītes novads, LV-2107
tālr. 26120706, 67914650, fakss 67914435, e-pasts dome@babite.lv, www.babite.lv
Babītes novada Babītes pagastā

A P S T I P R I N Ā T I
ar Babītes novada
pašvaldības domes
2015.gada 27.maija
lēmumu (protokols
Nr.8, 24.§)

N O T E I K U M I

2015.gada 27.maijā **Nr.6**

Babītes novada pašvaldības informācijas tehnoloģiju drošības noteikumi

Vispārīgie jautājumi

1.1. Noteikumi nosaka kārtību, kādā Babītes novada pašvaldība (turpmāk – Pašvaldība) un tās iestādes (turpmāk tekstā – Iestāde) nodrošina tai piederošo informācijas un tehnisko resursu aizsardzību.
1.2. Informācijas tehnoloģiju (turpmāk tekstā - IT) drošības noteikumi (turpmāk – Noteikumi) izstrādāti saskaņā ar Informācijas tehnoloģiju drošības likumu.
1.3. Noteikumi ietver minimālās prasības. Iestāde var noteikt stingrākus drošības pasākumus.
1.4. Noteikumu mērķis ir:
1.4.1. apliecināt Pašvaldības un tās Iestāžu vadības apņemšanos nodrošināt Iestādēs informācijas un tehnisko resursu drošību, lai uzturētu to integritāti, pieejamību un konfidencialitāti;
1.4.2. nodrošināt Iestādēs vienādu un sistemātisku pieeju IT drošības jautājumu risināšanai;
1.4.3. panākt Iestāžu darbinieku izpratni par IT drošības jautājumiem;
1.4.4. būt par pamatu procedūru, instrukciju un citu nepieciešamo drošības dokumentu izstrādē un ieviešanā.
1.5. Saskaņā ar Informācijas tehnoloģiju drošības likumu Pašvaldībā kopumā IT drošības pārvaldību nodrošina Pašvaldības domes priekšsēdētājs, bet Pašvaldības iestādē – iestādes vadītājs.
1.6. Noteikumu ievērošana ir obligāta visiem Pašvaldības darbiniekiem.

Noteikumos lietotie termini

2.1. **Informācijas resursi** – informācijas sistēmu sistēmprogrammas, lietojumprogrammas, sistēmu un datu faili un cita informācija, ko izmanto informācijas apstrādei, pārraidei, glabāšanai un citu funkciju veikšanai.
2.2. **Tehniskie resursi** – datori, serveri, 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** – Iestādes vadītājs vai ar vadītāja rīkojumu iecelts Iestādes darbinieks, kurš atbild par IT drošības pārvaldību Iestādē.
2.5. **IT drošības pārzinis** – ar Pašvaldības domes priekšsēdētāja rīkojumu iecelts darbinieks, kurš nodrošina IT drošības pārvaldību Pašvaldībā kopumā saskaņā ar Informācijas tehnoloģiju drošības likumu.
2.6. **Resursu aizbildnis** – Resursu turētāja norīkota persona, kura atbild par resursu funkcionēšanu un/vai saturu Iestādē.
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** – kaitīgs 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** – IS risku identificēšana, novērtēšana, samazināšana un kontrolēšana, kuras ietvaros tiek veikta IS risku ierobežošana līdz Iestādei pieņemamam līmenim.

Resursu pārvaldība

3.1. **IT drošības pārzinim** ir šādi pienākumi:
3.1.1. organizēt Pašvaldības IT drošības noteikumu izstrādi;
3.1.2. nodrošināt izmaiņu pārvaldību;
3.1.3. uzturēt aktuālas izmaiņas drošības dokumentos;
3.1.4. pildīt Informācijas tehnoloģiju drošības likuma 8.panta 3.daļā minētos pienākumus.
3.2. Resursu turētājs norīko visiem vai atsevišķiem resursiem **Resursu aizbildni,** kura pienākums ir:
3.2.1. nodrošināt resursu normālu (pareizu) darbību;
3.2.2. nodrošināt resursu lietotāju pārvaldību;
3.2.3. pildīt citus Iestādes IT drošības noteikumos uzliktos pienākumus;

3.2.4. veikt kopā ar **Resursu turētāju** risku aktualizāciju.

3.3. **Resursu lietotājiem** ir pienākums ievērot Pašvaldībā apstiprinātos IT drošības noteikumus.

Serveru fiziskā aizsardzība

4.1. **Resursu turētājs** nodrošina, ka visi serveri tiek ekspluatēti slēdzamās telpās ar ierobežotu pieejamību, kuru fiziskā aizsardzība nodrošina tikai pilnvarotu personu piekļuvi vai arī serveru fizisko aizsardzību, lai tos nevarētu izslēgt, pārvietot, bojāt un nesankcionēti mainīt to konfigurāciju. Serveru telpas izvieto ēkas vietās, kurās ir mazāka apdraudejumu īstenošanās iespējamība.

4.2. Nepiederošas personas serveru telpās drīkst uzturēties tikai pilnvarotu personu pavadībā.

4.3. Serveru telpām ir ierobežota fiziskā piekļuve. Tiesības piekļūt serveru telpām nosaka **IT drošības pārzinis**, uzturot pilnvaroto personu sarakstu. Sarakstā iekļaujamas tikai tās personas, kam nepieciešama fiziska piekļuve serveriem.

4.4 . Atstājot serveru telpas, pilnvarotajām personām jāpārliecinās, ka durvis un logi ir cieši aizvērti.

4.5. Sistēmu uzturot, **Resursu aizbildņiem** ir jāseko IT resursa izstrādātāja vai ražotāja izvirzīto prasību ievērošanai, piemēram, nodrošinot pietiekamu atmiņas un diska apjomu, atbilstošu temperatūru un gaisa mitrumu serveru telpās.

4.6. Atkarībā no iespējamo zaudējumu apmēriem **Resursu turētājs** nodrošina serveru un serveru telpu pietiekamu aizsardzību pret fiziskiem apdraudējumiem (t.sk. neatbilstošiem klimatiskajiem apstākļiem, ugunsgrēku, plūdiem, elektroenerģijas piegādes pārtraukumiem, tīšiem bojājumiem), nepieciešamības gadījumā ierīkojot ugunsdzēsības signalizāciju, automātiskās ugunsdzēšanas sistēmu, uzstādot alternatīvās strāvas piegādes iekārtas un gaisa dzesēšanas iekārtas.

Tīklu Infrastruktūra

5.1. **Resursu turētājs** nodrošina pietiekamu fizisko aizsardzību tīkla aparatūrai un kabeļiem, tos izvietojot tādejādi, lai tiem nevarētu nesankcionēti, nemanīti vai aiz nejaušības piekļūt, pieslēgties vai kā citādi bojāt.

Darbstaciju fiziskā aizsardzība

6.1. Darbstacijas lieto atbilstoši ražotāja noteiktajām prasībām.

6.2. Lietot elektroenerģijas nepārtrauktas piegādes iekārtas, ja elektroenerģijas piegādes traucējumu radītais risks ir nepieņemami liels.

Portatīvo iekārtu fiziskā aizsardzība

7 .1. Portatīvos datorus lieto atbilstoši ražotāja noteiktajām prasībām.

Datu nesēju fiziskā aizsardzība

8.1. 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 Pašvaldības administrācijas telpās tam paredzētās vietās. Ja ir nepieciešams iznīcināt datu nesējus, to iznīcināšanu uzrauga vai nodrošina **IT drošības pārzinis**.

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

8.3. 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.

Klasificētie resursi

9.1. Nepieciešamības gadījumā **Resursu turētājs** veic papildu fiziskās aizsardzības pasākumus atkarībā no resursu klasifikācijas.

9.2. **Resursu turētājs** sistemātiski veic informācijas sistēmas fiziskās aizsardzības pasākumus, nepieļaujot situāciju, ka informācijas resursi atrastos ārpus ierobežotas pieejamības telpām bez resursu turētāja pilnvarotu darbinieku uzraudzības.

9.3. **Resursu turētājs** regulāri veic fiziskās aizsardzības pasākumu pārbaudi.

Piekļuves kontrole

1.7. 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.

1.8. **Resursu turētajam** vai tā pilnvarotai personai ir jāinformē **Resursu aizbildni** par tiem darbiniekiem, kuri pārtrauc darba attiecības ar Iestādi. **Resursu aizbildņi** pēs šīs informācijas saņemšanas nekavējoties anulē visas attiecīgā lietotāja piekļuves tiesības informācijas sistēmas resursiem.

1.9. 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 resursus atbilstoši noteiktajām piekļuves tiesībām.

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

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

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

1.13. Par paroli jāizvēlas pietiekami sarežģīta simbolu kombinācija.

1.14. Paroles garumam resursiem, kas klasificēti ar informācijas konfidencialitātes līmeni K2 (vidēja vērtības informācija), ir jābūt vismaz 8 (astoņiem) simboliem.

1.15. Paroles garumam resursiem, kas klasificēti ar konfidencialitātes līmeni K3 (augstas vērtības informācija), ir jābūt vismaz 10 (desmit) simboliem. Administratoru parolēm piekļuvei servera informācijas resursiem jābūt 12 (divpadsmit) simbolu garām.

1.16. Lietotāju vārdiem un parolēm starp konfidencialitātes līmeņiem K2 un K3 resursos ir jāatšķiras.

1.17. Lietotājam regulāri, ne retāk kā 1 (vienu) reizi gadā jāmaina lietošanas parole

resursiem, kas klasificēta ar konfidencialitātes līmeni K2. Lietotājam regulāri, ne retāk kā 1 (vienu) reizi 3 (trīs) mēnešos jāmaina lietošanas parole resursiem, kas klasificēti ar konfidencialitātes līmeni K3. K3 konfidencialitātes līmeņa resursu aizbildņiem ir jānodrošina automātisks paroles maiņas pieprasījums.

1.18. Lietotāju paroles uz serveriem var glabāt tikai šifrētā veidā.

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

1.20. 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 informācijas sistēmās ir atbildīgs izmantotā lietotāja vārda un paroles īpašnieks.

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

1.22. Ja lietotājs konstatē, ka kāds cits ir uzzinājis viņa paroli, lietotājs to nekavējoties nomaina un par to nekavējoties ziņo resursu aizbildņiem.

1.23. Aizliegts mēģināt uzzināt citu lietotāju paroles.

1.24. Resursu aizbildņiem, instalējot sistēmu, jānomaina noklusētās paroles.

Datu rezerves kopiju veidošana

1.25. Regulāri jāveic svarīgāko informācijas resursu un programmatūru rezerves datu kopēšanu. Rezerves datu kopēšanu nodrošina **Resursu aizbildņi** un to biežums un apjoms tiek saskaņots ar **Resursu turētāju.**

1.26. Vismaz reizi dienā tiek veidota inkrementālā dublējumkopija resursu datnēm. **Resursu aizbildņi** pārbauda, ka rezerves kopiju veidošanas process ir beidzies sekmīgi.

1.27. Reizi gadā **Resursu aizbildņi** pārbauda iespēju no rezerves kopijām atjaunot informācijas resursu datus.

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

Vīrusu kontrole

1.29. **Resursu aizbildņi** nosaka kārtību un veic pasākumus datorvīrusu darbības novēršanai informācijas sistēmās.

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

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

Darbstaciju aizsardzība

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

1.33. Personālajā datorā uzstāda un lieto tikai to programmatūru un tādā konfigurācijā, ko ir noteicis **Resursu turētājs. Resursu aizbildnis** personālā datora funkcionalitāti ierobežo līdz darba vajadzībām nepieciešamo funkciju līmenim.

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

Datortīklu aizsardzība

1.35. **Resursu aizbildnis** datu plūsmā starp lokālo datortīklu un ārējo datortīklu atļauj tikai tos pakalpojumus, kas ir nepieciešami Pašvaldības funkciju izpildei, šim nolūkam lietojot ugunsmūra sistēmu.
1.36. Pieslēgšanos Pašvaldības informācijas sistēmām no loģiski attālas vietas aizsargā, lietojot kriptogrāfijas līdzekļus kopā ar lietotāja vārdu tā, lai droši noteiktu lietotāja autentiskumu.
1.37. **IT drošības pārzinis** pēc nepieciešamības iesaka papildu loģiskās aizsardzības pasākumus atkarībā no informācijas resursu klasifikācijas.

Pašvaldības sadarbība ar ārējiem IT pakalpojumu sniedzējiem

1.38. Ja Iestāde izvēlas resursa uzturēšanu uzticēt ārējam pakalpojumu sniedzējam, tam jānodrošina drosības līmenis, kas nav zemāks par šajos Noteikumos noteikto.
1.39. Iestāde nosaka informācijas izpaušanas ierobežojumus.
1.40. Ārpakalpojuma līgumā jāiekļauj IT drošības likumā noteiktie pienākumi.
1.41. Saskaņojot ar **Resursu turētājiem**, piešķir pieejas tiesības ìnformācijas resursiem ārējiem IT pakalpojumu sniedzējiem tikai to pienākumu veikšanai nepieciešamajā apjomā.
1.42. Visas izmaiņas (sistēmas informācijas resursu izveidošana, papildināšana, mainīšana, apstrāde, pārraidīšana, glabāšana, atjaunošana un iznīcināšana) notiek atbilstoši Pašvaldības IT izmaiņu pārvaldības prasībām.
1.43. Ārpakalpojumu sniedzēju normatīvajos aktos noteiktajā kārtībā reģistrē Datu valsts inspekcijā, kā datu operatoru.

Informācijas resursu klasifikācija

1.44. Iestāde veic visu informācijas resursu klasifikāciju ar mērķi novērtēt to nozīmību pēc **konfidencialitātes, vērtības un pieejamības.**
1.45. Informācija var būt **publiska** vai **ierobežotas pieejamības.**
1.46. **Informācijas konfidencialitātes** līmeni nosaka, ņemot vērā kaitējumu, kas varētu tikt nodarīts Iestādei, ja informācijai piekļūst nepilnvarotas personas.
1.47. **Publiska informācija (P)** - ir informācija, kas nav svarīga konfidencialitātes aspektā, ir brīvi pieejama Iestādes darbiniekiem un jebkurai personai vai organizācijai, kas to pieprasījusi. Šīs informācijas izplatīšana neietekmē iestādi negatīvā veidā.
1.48. **Ierobežotas pieejamības informācija (I)** – ir informācija, kas ir svarīga konfidencialitātes aspektā un tās pazīmes ir noteiktas Informācijas atklātības likuma 5., 6. un 7.pantā, tā ir brīvi pieejama tikai Iestādes darbiniekiem, kuriem ir piešķirtas šādas tiesības.

1.49. **Informācijas vērtības (V)** līmeni nosaka atkarībā no kaitējuma, kas varētu būt nodarīts Iestādei, ja tiktu nodrošināta informācijas resursu integritāte, pēc šādas skalas:
1.49.1. V1 – augstas vērtības informācija,
1.49.2. V2 – vidējas vērtības informācija,
1.49.3. V3 – zemas vērtības informācija.

1.50. **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:
1.50.1. PI – informācija pieejama 24 stundas diennaktī, 7 dienas nedēļā;
1.50.2. P2 – informācijas pieejamība Iestādes darba laikā.

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

1.52. Informācijas resursu klasifikācijai var izmantot tabulu, kur **V** – informācijas vērtība, **K** – informācijas konfidencialitāte, **P** – informācijas pieejamība:

Nr.	Resurss	Informācijas sistēma	V	K	P

Risku analīze

1.53. Risku analīzi veic ar mērķi izvērtēt resursu apdraudējumu un iespējamās sekas apdraudējuma iestāšanās gadījumā.

1.54. Risku pārvaldīšanu veic, ņemot vērā informācijas klasifikāciju, un risku pārvaldīšanas pasākumus nosaka, samērojot drošības pasākumu izmaksas ar iespējamiem zaudējumiem.

1.55. Atbildīgais par risku analīzes veikšanu ir **Resursu turētājs**, kurš organizē risku analīzi, piesaistot struktūrvienību vadītājus.

1.56. Struktūrvienību vadītāju pienākums ir nodrošināt pēc iespējas pilnīgu un precīzu risku identificēšanu un novērtēšanu.

1.57. Risku analīzi veic ne retāk kā vienu reizi gadā.

1.58. Resursu apdraudējuma iestāšanās varbūtību nosaka, izmantojot skalu:
1.58.1. A1 – maza apdraudējuma iestāšanās varbūtība – vērtība 1,
1.58.2. A2 – vidēja apdraudējuma iestāšanās varbūtība – vērtība 2,
1.58.3. A3 – liela apdraudējuma iestāšanās varbūtība – vērtība 3.

1.59. Katra apdraudējuma iestāšanās rezultātā resursiem radīto kaitējumu nosaka, izmantojot skalu:
1.59.1. RK1 – mazs kaitējums – vērtība 1,
1.59.2. RK2 – vidējs kaitējums – vērtība 2,
1.59.3. RK3 – liels kaitējums – vērtība 3.

1.60. Risku aprēķināšanu veic:
risks= apdraudējuma varbūtība x resursa apdraudējuma kaitējums
jeb **R=AV x RK**.

1.61. Tabulā apkopo iespējamos resursu apdraudējumus, atzīmējot to K – konfidencialitāti, P – pieejamību, I – integritāti, AV – apdraudējuma varbūtību, RK – resursiem radīto kaitējumu, R – aprēķināto risku.

Nr.	Apdraudējums	Apraksts	K	P	I	AV	RK	R

Risku pārvaldība

Risku mazināšanas pasākumu tabulā ieteicamas apkopot tos riskus, kuriem drošības risks ir 6 vai vairāk.

Nr.	Drauds	Papildus drošības pasākumi	Ieviešanas termiņš	Izmaksas	Izpildītājs

Izmaiņu pārvaldība

1.62. **IT drošības pārzinis**:
- 1.62.1. ne retāk kā reizi gadā veic un dokumentē:
  - 1.62.1.1. informācijas resursu klasifikāciju,
  - 1.62.1.2. resursu risku analīzi,
  - 1.62.1.3. atklāto trūkumu novēršanu;
- 1.62.2. pēc nepieciešamības organizē Iestāžu darbinieku apmācību;
- 1.62.3. apstiprina un atceļ lietotājiem pieejas tiesības resursiem, fiksējot to resursu pieejas žurnālā;
- 1.62.4. organizē datu rezerves kopiju veidošanu;
- 1.62.5. nodrošina resursu konfigurāciju pārvaldību;
- 1.62.6. nodrošina atsevišķu konkrētai Iestādei būtisku resursu pārvaldību;
- 1.62.7. nodrošina auditācijas pierakstu veikšanu;
- 1.62.8. veic drošības incidentu pārvaldību.

Drošības incidentu pārvaldība

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

1.64. **IT drošības pārzinis** identificē drošības incidentu pēc jebkura no minētajiem kritērijiem:
- 1.64.1. notiek uzbrukums resursiem no ārpuses,
- 1.64.2. notiek svarīga resursu atteice,
- 1.64.3. apgrūtināta Iestādes normāla darbība,
- 1.64.4. apgrūtināta būtisku pakalpojumu sniegšana.

1.65. Drošības incidenta gadījumā **IT drošības pārzinis**:
- 1.65.1. informē Informācijas tehnoloģiju drošības incidentu novēršanas institūciju CERT.LV,
- 1.65.2. saglabā pierādījumus,
- 1.65.3. atjauno informācijas sistēmas darbību,
- 1.65.4. reģistrē drošības incidentu žurnālā.

Pašvaldības domes priekšsēdētājs Andrejs Ence