LATVIJAS REPUBLIKA
DAUGAVPILS PILSĒTAS DOME

Reģ. Nr. 90000077325, K. Valdemāra iela 1, Daugavpils, LV-5401, tālrunis 65404344, 65404365, fakss 65421941
e-pasts: info@daugavpils.lv www.daugavpils.lv

RĪKOJUMS

Daugavpilī

2015.gada 4.jūnijā Nr. 144

Par grozījumu izdarīšanu Daugavpils pilsētas domes Informācijas tehnoloģiju drošības noteikumos

Pamatojoties uz likuma "Par pašvaldībām" 62.panta 6.punktu, izpildot Informācijas tehnoloģiju drošības likuma 8.panta ceturto daļu, nodrošinot kontroli par Daugavpils pilsētas domes (turpmāk - Dome) darbinieku rīcībā esošajām informācijas resursu lietotāju piekļuves tiesībām, izdarīt ar Domes 2014.gada 16.janvāra rīkojumu Nr.18 apstiprinātajos noteikumos "Daugavpils pilsētas domes informācijas tehnoloģiju drošības noteikumi" (turpmāk – Noteikumi) šādus grozījumus:

1. Izteikt Noteikumu tiesisko pamatu šādā redakcijā:
   "Izdoti saskaņā ar Informācijas tehnoloģiju drošības likuma 8.panta ceturto daļu";
2. Izteikt Noteikumu 10.2.apakšpunktu šādā redakcijā:
   „ 10.2. Domes struktūrvienību vadītāji, atbilstoši to padotībā esošo informācijas resursu lietotāju piekļuves tiesībām, nodrošina saistību rakstu sagatavošanu informācijas resursu lietotājiem, kuriem attiecīgajā struktūrvienībā noteikta pieeja informācijas resursiem, un to iesniegšanu Domes personāla speciālistam. Domes personāla speciālists nodrošina autorizēto informācijas resursu lietotāju saistību rakstu glabāšanu resursu lietotāja personīgajā lietā un trīs darba dienu laikā nodrošina informācijas sniegšanu ārējiem informācijas resursu turētājam, ar kuru noslēgts līgums, gadījumos, ja informācijas resursu lietotājs, kā autorizētais informācijas resursu lietotājs caur saistību rakstu, ir atstādināts no darba pienākumu veikšanas vai ar viņu ir pārtrauktas darba tiesiskās attiecības, kā rezultātā resursu lietotājs vairs nav informācijas resursu lietotājs.";
3. Papildināt Noteikumus ar 10.2.[1] apakšpunktu šādā redakcijā:
   „10.2.[1] Domes struktūrvienību vadītāji vienas darba dienas laikā ar rakstveida pieprasījumu e-pasta formā informē resursu aizbildņus un Domes personāla speciālistu par struktūrvienībai pieejamo informācijas resursu lietotāju maiņu, jaunu pieeju izveidi vai atcelšanu u.c. ar informācijas resursiem saistītos jautājumos, atbilstoši Domes informācijas resursu lietotāju piekļuves tiesību un atbildīgo personu sarakstam, kuru aktualizē un kontrolē resursu aizbildņi.";
4. Aizstāt Noteikumu 10.11.apakšpunktā vārdus "reizi gadā" ar vārdiem un ciparu "reizi 60 (sešdesmit) dienās";
5. Izteikt Noteikumu 11.1.apakšpunktu šādā redakcijā:

"11.1. Svarīgāko informācijas resursu un programmatūru rezerves datu kopēšana notiek regulāri katru darba dienu.";

6. Izteikt Noteikumu 12.1.1.apakšpunktu šādā redakcijā:
   "12.1.1. resursu aizbildņi nosaka programmnodrošinājuma kārtību serverī pretvīrusu aizsardzībai;";
7. Izteikt Noteikumu 14.1.1.apakšpunktu šādā redakcijā:
   "14.1.1. resursu aizbildnis izstrādā un uztur datortīkla shēmu (pielikums Nr.1), kurā parādīta datortīklā savienotā aparatūra;"
8. Aizstāt Noteikumu 14.1.2.apakšpunktā vārdus "tos pakalpojumus, kas ir nepieciešami" ar vārdiem "tās operācijas, kas ir nepieciešamas";
9. Domes Vispārējai nodaļai iepazīstināt Domes darbiniekus ar Noteikumu grozījumu tekstu.
10. Kontroli par rīkojuma izpildi uzdot Domes lietu pārvaldniekam.
11. Atzīt par spēku zaudējušu Daugavpils pilsētas domes 2008.gada 5.janvāra rīkojumu Nr.34 "Par atbildīgās personas nozīmēšanu".

Daugavpils pilsētas domes priekšsēdētājs J.Lāčplēsis

LATVIJAS REPUBLIKA
DAUGAVPILS PILSĒTAS DOME

Reģ. Nr. 90000077325, K. Valdemāra iela 1, Daugavpils, LV-5401, tālrunis 65404344, 65404365, fakss 65421941
e-pasts: info@daugavpils.lv www.daugavpils.lv

APSTIPRINĀTI
ar Daugavpils pilsētas domes
priekšsēdētāja 2014.gada 16.janvāra
rīkojumu Nr.18

Grozījumi ar:
04.06.2015. rīkojumu Nr.144

Daugavpils pilsētas domes Informācijas tehnoloģiju drošības noteikumi

Izdoti saskaņā ar Informācijas tehnoloģiju drošības likuma 8.panta ceturto daļu"
(grozīts ar 04.06.2015. rīkojumu Nr.144)

1. Vispārīgie jautājumi

1.1. Noteikumi nosaka kārtību, kādā Daugavpils pilsētas dome (turpmāk – Dome nodrošina tai piederošo informācijas un tehnisko resursu (turpmāk – resursi) aizsardzību.

1.2. Informācijas tehnoloģiju (turpmāk – IT) drošības noteikumi (turpmāk – noteikumi) izstrādāti saskaņa ar Informācijas tehnoloģiju drošības likumu (turpmāk – likums).

1.3. Noteikumi ietver minimālās prasības. Informācijas sistēmas resursu turētājs ar rīkojumu laicīgi var noteikt stingrākus drošības pasākumus.

1.4. Noteikumu mērķis ir:

1.4.1. nodrošināt iestādes resursu drošību, lai uzturētu to integritāti, pieejamību un konfidencialitāti;

1.4.2. nodrošināt vienādu un sistemātisku pieeju IT drošības jautājumu risināšanā;

1.4.3. panākt darbinieku izpratni par IT drošības jautājumiem;

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

1.5. Noteikumu ievērošana ir obligāta IT resursu turētājam, pārzinim, aizbildņiem un lietotājiem.

2. Noteikumos lietotie termini

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

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

2.3. **Resursu turētājs** – Domes izpilddirektors.

2.4. **IT drošības pārzinis** - ar rīkojumu iecelts darbinieks vai nolīgts ārpakalpojumu sniedzējs, kurš nodrošina IT drošības pārvaldību (likuma izpratnē atbildīgā persona).

2.5. **Resursu aizbildnis** (datortīkla administrators un programmēšanas inženieris) - resursu turētāja vai ārpakalpojumu sniedzēja norīkota persona, kura ir atbildīga par resursu funkcionēšanu.

2.6. **Resursu lietotājs** – Domes darbinieks, kurš izpilda noteiktus pienākumus un apstrādā noteiktu informāciju atbilstoši piešķirtām tiesībām lietot noteiktus informācijas resursus.

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

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

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

2.10. **Informācijas vērtība** - informācijas nozīmīgums iestādes funkciju veikšanai.

2.11. **Drošības incidents** - kaitīgs notikums vai nodarījums, kas apdraud informācijas resursu integritāti, pieejamību vai konfidencialitāti.

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

2.13. **Drošības dokumenti** - dokumentu kopums, kas apraksta iestādes resursu lietošanas kārtību.

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

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

3. Resursu pārvaldība

3.1. Resursu turētājs norīko IT drošības pārziņi, kura pienākumi ir:

3.1.1. organizēt iestādes IT drošības noteikumu izstrādi;

3.1.2. nodrošināt izmaiņu pārvaldību;

3.1.3. uzturēt aktuālās izmaiņas drošības dokumentos.

3.2. Resursu turētājs, visiem vai atsevišķiem resursiem apstiprina resursu aizbildni, kura pienākumi ir:

3.2.1. nodrošināt resursu pareizu darbību;

3.2.2. nodrošināt resursu lietotāju pārvaldību;

3.2.3. pildīt citus iestādes IT drošības noteikumos uzliktos pienākumus;

3.2.4. kopā ar resursu turētāju un/vai IT drošības pārziņu veikt risku aktualizāciju.

3.3. Resursu lietotājiem ir pienākums ievērot iestādē apstiprinātos IT drošības noteikumus.

4. 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 nodrošina serveru fizisko aizsardzību, lai tos nevarētu izslēgt, pārvietot, bojāt un nesankcionēti mainīt to konfigurāciju. Serveru telpas izvieto ēkas vietās, kurās ir mazāka apdraudējumu īstenošanās iespējamība.

4.2. Nepiederošas personas, t.sk. ārējie pakalpojumu sniedzēji, serveru telpās drīkst uzturēties tikai pilnvarotu personu pavadībā.

4.3. Serveru telpām ir ierobežota fiziska 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.

5. Tīklu infrastruktūra

5.1. 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.

6. 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.

7. Portatīvo iekārtu fiziskā aizsardzība

7.1. Portatīvos datorus lieto atbilstoši ražotāja noteiktajām prasībām.

8. 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 Domes 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.

9. Klasificētie resursi

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

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

9.3. Domes resursu turētājs regulāri veic fiziskās aizsardzības pasākumu pārbaudi.

10. Piekļuves kontrole

10.1. 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.

10.2. Domes struktūrvienību vadītāji, atbilstoši to padotībā esošo informācijas resursu lietotāju piekļuves tiesībām, nodrošina saistību rakstu sagatavošanu informācijas resursu lietotājiem, kuriem attiecīgajā struktūrvienībā noteikta pieeja informācijas resursiem, un to iesniegšanu Domes personāla speciālistam. Domes personāla speciālists nodrošina autorizēto

informācijas resursu lietotāju saistību rakstu glabāšanu resursu lietotāja personīgajā lietā un trīs darba dienu laikā nodrošina informācijas sniegšanu ārējiem informācijas resursu turētājam, ar kuru noslēgts līgums, gadījumos, ja informācijas resursu lietotājs, kā autorizētais informācijas resursu lietotājs caur saistību rakstu, ir atstādināts no darba pienākumu veikšanas vai ar viņu ir pārtrauktas darba tiesiskās attiecības, kā rezultātā resursu lietotājs vairs nav informācijas resursu lietotājs;

(grozīts ar 04.06.2015. rīkojumu Nr.144)

10.2.[1] Domes struktūrvienību vadītāji vienas darba dienas laikā ar rakstveida pieprasījumu e-pasta formā informē resursu aizbildņus un Domes personāla speciālistu par struktūrvienībai pieejamo informācijas resursu lietotāju maiņu, jaunu pieeju izveidi vai atcelšanu u.c. ar informācijas resursiem saistītos jautājumos, atbilstoši Domes informācijas resursu lietotāju piekļuves tiesību un atbildīgo personu sarakstam, kuru aktualizē un kontrolē resursu aizbildņi;

(papildināts ar 04.06.2015. rīkojumu Nr.144)

10.3. 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.

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

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

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

10.7. Par paroli jāizvēlas pietiekami sarežģīta simbolu kombinācija.

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

10.9. 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.

10.10. Lietotāja vārdiem un parolēm starp konfidencialitātes līmeņiem K2 (*vidēja vērtības informācija,*) un K3 (augstas vērtības informācija) resursos ir jāatšķiras.

10.11. Lietotājam regulāri, ne retāk kā 1 (vienu) reizi 60 (sešdesmit) dienās jāmaina lietošanas parole resursiem, kas klasificēta ar konfidencialitātes līmeni K2 (vidēja vērtības informācija). Lietotājam regulāri, ne retāk kā 1 (vienu) reizi 3 (trīs) mēnešos jāmaina lietošanas parole resursiem, kas klasificēti ar konfidencialitātes līmeni K3 (augstas vērtības informācija). K3 (augstas vērtības informācija) konfidencialitātes līmeņa resursu aizbildņiem ir jānodrošina automātisks paroles maiņas pieprasījums.

(grozīts ar 04.06.2015. rīkojumu Nr.144)

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

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

10.14. 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.

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

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

10.17. Aizliegts mēģināt uzzināt citu lietotāju paroles.

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

11. Datu rezerves kopiju veidošana

11.1. Svarīgāko informācijas resursu un programmatūru rezerves datu kopēšana notiek regulāri katru darba dienu.

(grozīts ar 04.06.2015. rīkojumu Nr.144)

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

11.3. Reizi gadā resursa aizbildni pārbauda iespēju no rezerves kopijām atjaunot informācijas resursu datus.

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

12. Vīrusu kontrole

12.1. Vīrusu kontrole informācijas resursos:

12.1.1. resursu aizbildņi nosaka programmnodrošinājuma kārtību serverī pretvīrusu aizsardzībai;

(grozīts ar 04.06.2015. rīkojumu Nr.144)

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

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

13. Darbstaciju aizsardzība

13.1. Personālo un portatīvo datoru aizsardzība:

13.1.1. portatīvajos datoros, kuri tiek lietoti ārpus Domes darba telpām, glabā tikai to informāciju, kas nepieciešama noteiktajā laikā noteiktajam datora lietotājam;

13.1.2. 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;

13.1.3. 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.

14. Datortīklu aizsardzība

14.1. Datortīklu aizsardzība:

14.1.1. resursu aizbildnis izstrādā un uztur datortīkla shēmu (pielikums Nr.1), kurā parādīta datortīklā savienotā aparatūra;

(grozīts ar 04.06.2015. rīkojumu Nr.144)

14.1.2. datu plūsmā starp lokālo datortīklu un ārējo datortīklu atļauj tikai tās operācijas, kas ir nepieciešamas Domes funkciju izpildei, šim nolūkam lietojot ugunsmūra sistēmu;

(grozīts ar 04.06.2015. rīkojumu Nr.144)

14.1.3. resursu aizbildnis pārbauda visu ārējo savienojumu eksistenci un pārliecinās, ka pastāv tikai tie savienojumi, kuri atbilst Dome darbības vajadzībām, un ka darbojas rezerves savienojumi;

14.1.4. pieslēgšanos Domes informācijas sistēmām no loģiski attālas vietas aizsargā, lietojot kriptogrāfijas līdzekļus kopā ar lietotāja vārdu tā, lai droši noteiktu lietotāja autentiskumu.

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

15. DPD sadarbība ar ārējiem IT pakalpojumu sniedzējiem

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

15.2. Dome nosaka informācijas izpaušanas ierobežojumus.

15.3. Ārpakalpojuma līgumā jāiekļauj IT drošības likumā noteiktie pienākumi.

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

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

15.6. Ārpakalpojumu sniedzēju normatīvajos aktos noteiktajā kārtībā kārtībā reģistrē Datu valsts inspekcijā, kā datu operatoru.

Daugavpils pilsētas domes priekšsēdētājs *(personiskais paraksts)* J.Lāčplēsis