Liepājas pilsētas pašvaldības administrācija

Rožu iela 6, Liepāja, LV-3401, tālrunis: 63 404 750, e-pasts: pasts@liepaja.lv, www.liepaja.lv

APSTIPRINĀTS
ar Liepājas pilsētas pašvaldības izpilddirektora
2019. gada 4. marta rīkojumu Nr. 59/2.1.1

Sistēmas drošības politika elektronisko pieteikumu sistēmai pieteikumi.liepaja.lv

Izdots saskaņā ar Ministru kabineta
2015. gada 28. jūlija noteikumi Nr. 442 "Kārtība, kādā
tiek nodrošināta informācijas un komunikācijas tehnoloģiju
sistēmu atbilstība minimālajām drošības prasībām" 8. punktu

1. Sistēmas raksturojums un analīze drošības jomā

1.1. Drošības politika izstrādāta Liepājas pilsētas pašvaldības Elektronisko pieteikumu sistēmai PIETEIKUMI.LIEPAJA.LV.

1.2. Saskaņā ar Ministru kabineta 2015. gada 28. jūlija noteikumiem Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" sistēma ir noteiktas kā pamata drošības sistēmas.

1.3. Sistēmas funkcijas ir pieteikumu iesniegšana, apstrāde, vērtējumu apkopošana, realizācijas atskaišu iesniegšana un rezultātu publicēšana pašvaldības līdzfinansējuma saņemšanai saskaņā ar Liepājas pilsētas domes apstiprinātiem normatīvajiem aktiem.

1.4. Sistēmas lietotāji:

1.4.1. Pieteikumu iesniedzēji - nevalstiskās organizācijas, mazie un vidējie komersanti, kā arī citas fiziskās un juridiskās personas, kuri atbilst izsludināto konkursu/aptauju nosacījumiem.

1.4.2. Pašvaldības darbinieki, kuri veic konkursu/aptauju administrēšanu, vērtēšanu un rezultātu apkopošanu.

1.4.3. Sistēmai ir šādas lietotāju grupas:

1.4.3.1. Sistēmas administrators – administrē lietotājus, veido konkursus/aptaujas, ir iespēja labot iesniegtos datus, ja tas nepieciešams;

1.4.3.2. Konkursa lietotāji – iesniedz pieteikumus;

1.4.3.3. Konkursa projektu vadītāji - redz/rediģē tikai savus ievadītos vai administratora piesaistītos projektus/aptaujas, vienam projektam iespējams piesaistīt divus projekta vadītājus;

1.4.3.4. Konkursa vērtētāji - pieejami vērtēšanai projekta vadītāja/administratora piešķirtie projekti lasīšanas režīmā, vienam projektam var būt līdz 10 projekta vērtētāji.

1.5. Sistēmai nav saistīto sistēmu.

1.6. Sistēma atbilst Latvijas Republikas tiesību aktiem informācijas drošības jomā.
1.7. Sistēmas uzturēšanu un datu glabāšanu nodrošina ārpakalpojumu sniedzējs SIA „IT Līderis".

2. Sistēmas drošības politikas mērķi un pamatnostādnes

2.1. Nodrošināt tādu informācijas tehnoloģiju vidi, lai Sistēma būtu aizsargāta pret ārējiem un iekšējiem drošības apdraudējumiem.
2.2. Apliecināt organizācijas vadības atbalstu Sistēmas drošības nodrošināšanai atbilstoši iestādes vajadzībām, saistošajiem normatīvajiem aktiem un drošības normām.
2.3. Sistēmas drošības politika ir saistoša visiem Sistēmas lietotājiem, kā arī SIA "IT Līderis".

3. Sistēmas drošības politikas uzdevumi

Sistēmas drošības politikai ir šādi uzdevumi:
3.1. nodrošināt informācijas pieejamību (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas);
3.2. nodrošināt informācijas integritāti (pilnīgas un nemainītas informācijas saglabāšanu);
3.3. nodrošināt informācijas konfidencialitāti (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot);
3.4. aizsargāt Sistēmas informācijas resursus;
3.5. aizsargāt Sistēmas tehniskos resursus;
3.6. noteikt Sistēmas drošības apdraudējumus;
3.7. novērtēt Sistēmas drošības riskus;
3.8. atklāt Sistēmas drošības incidentus;
3.9. atjaunot Sistēmas darbību pēc Sistēmas drošības incidentiem.

4. Sistēmas drošības pārvaldības organizācijas principi

4.1. Liepājas pilsētas pašvaldībā ir noteikts un regulāri tiek pilnveidots dokumentu un pasākumu kopums, kuru īstenošana nodrošina Sistēmas drošības politikas mērķa sasniegšanu.
4.2. Liepājas pilsētas pašvaldībā veicina katra darbinieka izpratni par pienākumiem risku un darbības nepārtrauktības pārvaldīšanā un informācijas un tehnoloģisko resursu aizsardzības nodrošināšanā, veicot darbinieku regulāru izglītošanu.
4.3. Liepājas pilsētas pašvaldībā nodrošina pastāvīgu drošības politikas īstenošanas koordinēšanu un pārraudzīšanu.
4.4. Gadījumos, kad Liepājas pilsētas pašvaldības darbinieki neievēro Drošības politikas izvirzītās prasības, Liepājas pilsētas pašvaldības vadība var ierosināt disciplinārās atbildības procesu saskaņā ar esošajiem normatīvajiem aktiem.
4.5. Iestādē ir skaidri definēts un izprasts atbildības sadalījums par Sistēmas drošību.
4.6. Liepājas pilsētas pašvaldības izpilddirektors:
  4.6.1. atbild par Sistēmas drošību;
  4.6.2. nosaka un apstiprina Sistēmas drošības politiku;
  4.6.3. nodrošina nepieciešamos līdzekļus un atbalstu Sistēmas drošības politikas ieviešanai, uzturēšanai un pilnveidošanai;
  4.6.4. nosaka pienākumu un atbildības sadalījumu attiecībā uz Sistēmas drošību:
4.7. Atbildīgā persona par Sistēmu drošības pārvaldību ir Liepājas pilsētas pašvaldības drošības pārvaldnieks.
4.8. IKT resursu turētājs šī dokumenta izpratnē rīkojas ar IKT resursiem pašvaldības uzdevumā. IKT resursi ir tehnisku un tehnoloģisku resursu kopums informācijas aprites nodrošināšanai – programmatūras, serveri, datu glabāšanas iekārtas, datori, datu pārraides tīkli un tīkla aparatūra, biroja un mobilās ierīces un citi tehniskie resursi, kurus izmanto Pašvaldības funkciju izpildei.

4.9. IKT resursu turētājs Sistēmai ir Liepājas pilsētas pašvaldības administrācijas Informācijas tehnoloģiju daļa.
4.10. Sistēmas informācijas resursu turētājs ir persona, kura savas kompetences ietvaros ir atbildīga par Informācijas resursiem un rīkojas ar tiem Pašvaldības uzdevumā, veicot Institūcijas kompetencē esošās funkcijas un uzdevumus
4.11. Sistēmas informācijas resursu turētāji ir:
4.11.1. Nevalstisko organizāciju sociālās iekļaušanas veicināšanas projektu līdzfinansēšanas konkursiem - Vides, veselības un sabiedrības līdzdalības daļa;
4.11.2. Veselības veicināšanas projektu konkursiem - Vides, veselības un sabiedrības līdzdalības daļa;
4.11.3. Nevalstisko organizāciju līdzfinansēšanas projektu konkursiem - Vides, veselības un sabiedrības līdzdalības daļa;
4.11.4. Mazo un vidējo komercsabiedrību projektu līdzfinansēšanas konkursiem - Attīstības pārvalde.
4.12. Atbildīgā persona par Sistēmas drošības pārvaldību:
4.12.1. organizē Sistēmas risku analīzi;
4.12.2. nodrošina nepieciešamo Sistēmas drošības dokumentu uzturēšanu un īstenošanu;
4.12.3. veic noteikto drošības prasību ievērošanas uzraudzību un drošības incidentu izmeklēšanu;
4.12.4. nodrošina darbinieku apmācību informācijas drošības jomā.
4.13. IKT resursu turētājs:
4.13.1. atbild par Sistēmas tehnisko resursu iegādi, izstrādi, darbību un uzturēšanu;
4.13.2. nodrošina Sistēmas tehniskos un loģiskos aizsardzības pasākumus;
4.13.3. atbild par Sistēmas pieejas tiesību pārvaldību;
4.13.4. sadarbībā ar ārpakalpojuma sniedzēju “IT Līderis” veic Sistēmas darbības atjaunošanas pasākumus, ja Sistēmas darbība ir traucēta.
4.14. Sistēmas informācijas resursu turētājs:
4.14.1. atbild par piekļuves kontroli informācijas resursam;
4.14.2. pieprasa Sistēmas lietotāju tiesības un definē lomas Pašvaldības darbiniekiem;
4.14.3. klasificē viņa turējumā esošos informācijas resursus;
4.14.4. nosaka drošības prasības informācijas resursam.
4.15. Lietotāji:
4.15.1. iepazīstas un apņemas ievērot informācijas drošības jomā pieņemto iekšējo normatīvo aktu prasības;
4.15.2. ziņo par Sistēmā identificētajiem riskiem, informācijas drošības notikumiem un incidentiem Liepājas pilsētas pašvaldības administrācijas informācijas tehnoloģiju daļai – e-pasts: it@liepaja.lv, tālrunis: 63 404 760.

5. Sistēmas drošības principi

5.1. Sistēmas lietotāju konti:
5.1.1. Sistēmas lietotāji, kas veic Sistēmas administrēšanas darbu, izmanto tam īpašus lietotāju kontus (turpmāk – Sistēmas administratora konti);
5.1.2. katrs lietotāja konts ir saistīts ar konkrētu fizisko personu;
5.1.3. Sistēmas administratora kontus aizsargā tā, lai novērstu iespēju lietotājiem tos izmantot.
5.2. Prasības parolēm:
5.2.1. Sistēmas piekļuve ir aizsargāta ar lietotāja vārdu un paroli;
5.2.2. Sistēmas lietotāja paroles garums nav mazāks par deviņām rakstu zīmēm un satur vismaz vienu lielo latīņu alfabēta burtu un mazo latīņu alfabēta burtu, kā arī ciparu vai speciālu simbolu;
5.2.3. Sistēmas lietotāja paroles aizliegts glabāt nešifrētā veidā;

5.2.4. Sistēmas lietotāja parole ievadīšanas brīdī netiek pilnībā attēlota lietotājam;
5.2.5. Sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir vienreiz lietojama;
5.2.6. Sistēmā nav funkcionalitātes, kas atļauj Sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada.

5.3. Izsekojamība:
5.3.1. Sistēmas auditācijas pierakstus veido un uzglabā vismaz 6 mēnešus pēc ieraksta izdarīšanas;
5.3.2. jebkura piekļuve sistēmai ir izsekojama līdz konkrētam Sistēmas lietotāja kontam vai interneta protokola (IP) adresei.

5.4. Atjauninājumi:
5.4.1. IKT resursu turētājs sadarbībā ar atbildīgo par Sistēmas drošības pārvaldību veic pieejamo programmatūras atjauninājumu izvērtēšanu un nepieciešamības gadījumā - testēšanu;
5.4.2. Sistēmai nodrošina visus pieejamos nepieciešamos programmatūras atjauninājumus.

6. Sistēmas aizsardzības pasākumi

6.1. Visās Liepājas pilsētas pašvaldības valdījumā esošajās gala lietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, uzstāda pretvīrusu aizsardzības sistēmu.
6.2. Sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamo tiesību kopu.

7. Sistēmas drošības risku (pieejamības, integritātes un konfidencialitātes risku) pieņemamais līmenis

7.1. Atbildīgais par Sistēmas drošības pārvaldību ne retāk kā reizi gadā veic Sistēmas drošības risku analīzi.
7.2. Risku analīzes ietvaros sadarbībā ar Liepājas pilsētas pašvaldības administrācijas IT daļu tiek veikts izvērtējums vai risku ierobežošanas un darbības nepārtrauktības nodrošināšanas izmaksas ir samērojamas ar iespējamiem zaudējumiem, kas varētu rasties šo risku īstenošanās vai Iestādes darbības pārtraukšanas gadījumos.

8. Sistēmas drošības kritēriji

8.1. Sistēmas nepārtrauktās darbības laiks:
8.1.1. Sistēmai jābūt pieejamai darba dienās, laikā no 8:00 līdz 20:00;
8.1.2. Sistēmas darbības atjaunošanas laiks - Sistēmas darbība jāatjauno ne vēlāk kā 8 stundas pēc darbības pārtraukuma.

8.2. Nosacījumi, pie kuriem ikdienas procedūras aizstājamas ar krīzes pārvaldības procedūrām:
8.2.1. ja Sistēmas darbības atjaunošanas laiks pārsniedz pieļaujamo;
8.2.2. ja Sistēmā konstatēts datu zudums;
8.2.3. ja Sistēma ilgāk par 12 stundām nav pieejama no ārējā tīkla.

9. Lietotāja personu datu apstrāde

9.1. Reģistrējoties Sistēmā, iegūto Lietotāja personas datu pārzinis ir Pašvaldība un apstrādā tos ar mērķi nodrošināt efektīvu un ērtu pieteikumu aizpildīšanas, iesniegšanas un izvērtēšanas procesu.
9.2. Tiesiskais pamats Lietotāja personas datu apstrādei ir Sistēmas drošības politikas izpilde saskaņā ar Vispārīgās datu aizsardzības regulas 6. panta 1. punkta b) apakšpunktu.
9.3. Pašvaldība Lietotāja personas datu apstrādi veiks un datus glabās ne ilgāk kā 5 gadus pēc pēdējās Lietotāja veiktās aktivitātes Sistēmā.
9.4. Lietotājam kā datu subjektam ir tiesības:

9.4.1. pieprasīt Pašvaldībai piekļūt Lietotāja kā datu subjekta apstrādātajiem personas datiem, lūgt neprecīzo personas datu labošanu vai dzēšanu, iesniedzot rakstisku pamatojumu lūgumam,

9.4.2. likumā noteiktajos gadījumos lūgt personas datu apstrādes ierobežošanu, kā arī iebilst pret apstrādi,

9.4.3. iesniegt sūdzību par nelikumīgu personas datu apstrādi Datu valsts inspekcijā.

9.5. Lietotājam par viņa personas datu apstrādes jautājumiem ir tiesības vērsties pie Pašvaldības personas datu aizsardzības speciālista. Kontaktinformācija – tālrunis: 63 422 331, e-pasta adrese: das@liepaja.lv.

10. Noslēguma jautājumi

10.1. Politiku pārskata vismaz reizi gadā, kā arī šādos gadījumos:

10.1.1. ja izmaiņas Sistēmā var ietekmēt Sistēmas drošību;

10.1.2. ja ir mainījušies vai atklāti jauni Sistēmas drošības apdraudējumi;

10.1.3. ja pieaug Sistēmas drošības incidentu skaits vai noticis nozīmīgs Sistēmas drošības incidents.

10.2. Ja, pārskatot politiku, konstatēta atbilstoša nepieciešamība, to aktualizē.

IT daļas vadītāja Iveta Lapiņa