|  |  |  |  |
| --- | --- | --- | --- |
| APSTIPRINĀTS  Valsts kases 2015. gada 10. jūlijā  iepirkuma komisijas sēdē,  protokols Nr. 2 | | | |
| **Uzaicinājums** | | | |
| Rīgā | | | |
| 10.07.2015. |  | Nr. | VK/2015/12 |

**Uzaicinājums iesniegt piedāvājumu**

1. **Iepirkuma priekšmets**

Sekundārā datu centra telpu noma (CPV kods – 72300000-8 „Datu pakalpojumi”).

1. **Pasūtītājs un iepirkuma identifikācijas numurs:**
   1. Pasūtītājs un rekvizīti:

Valsts kase

Smilšu ielā 1

Reģ. Nr. 90000597275

Tālruņa Nr. +371 67094222

Faksa Nr. +371 67094220

[kase@kase.gov.lv](mailto:kase@kase.gov.lv);

* 1. Iepirkuma identifikācijas numurs:

VK/2015/12.

1. **Iepirkuma metode**

Publiskais iepirkums saskaņā ar Publisko iepirkumu likuma (turpmāk – PIL) 8.2 pantu.

1. **Paredzamā līgumcena**

41 999,00 EUR (bez PVN).

1. **Piedāvājuma iesniegšanas vieta**

5.1. Piedāvājums jāiesniedz līdz 2015. gada 21.jūlijam plkst. 11.00 Valsts kases Birojā A308.kab., Smilšu ielā 1, Rīgā, LV-1919 vai pa pastu, kontaktpersona – Informātikas departamenta Infrastruktūras uzturēšanas daļas vadītājs Andris Rutkis, tālrunis 67094256, e-pasta adrese: [andris.rutkis@kase.gov.lv](mailto:andris.rutkis@kase.gov.lv) un Informātikas departamenta Infrastruktūras uzturēšanas daļas vadītāja vietnieks Jānis Lazdāns, tālrunis 67094316, e-pasta adrese: [janis.lazdans@kase.gov.lv](mailto:janis.lazdans@kase.gov.lv) .

5.2. Piedāvājumu, kas iesniegts vai piegādāts pēc uzaicinājuma 5.1.apakšpunktā norādītā termiņa, neatvērtu nosūta atpakaļ tā iesniedzējam.

1. **Piedāvājuma noformēšana**
   1. Piedāvājums jāiesniedz aizlīmētā aploksnē vai cita veida necaurspīdīgā iepakojumā divos ( 2) eksemplāros ( viens oriģināleksemplārs un viena kopija elektroniskā formātā).
   2. Uz aploksnes jābūt norādei:
      1. piedāvājums iepirkuma procedūrai **„Sekundārā datu centra telpu noma”**;
      2. identifikācijas Nr. VK/2015/12;
      3. pretendenta nosaukums, juridiskā adrese, tālruņa un faksa numurs;
      4. Neatvērt līdz 2015. gada 21. jūlijam plkst. 11.00.
   3. Piedāvājuma oriģināleksemplāru noformē un iesniedz kā vienu sējumu ar uzrakstu „ORIĢINĀLS”. Sējumam pievieno satura rādītāju, visas lapas sanumurē un cauršauj ar diegu vai caurauklo ar auklu, kuras galus sasien mezglā, mezglu pielīmējot sējuma pēdējai lapai ar papīra uzlīmi. Uz papīra uzlīmes raksta apliecinājuma tekstu, norādot: sējumā sanumurēto un cauršūto (cauraukloto) lapu skaits, norādīts ar cipariem un vārdiem. Apliecinājuma tekstu ar parakstu apliecina persona, kura cauršuva (cauraukloja) sējumu, parakstā iekļaujot personas parakstu, tā atšifrējumu un ziņas, kas ļauj nepārprotami identificēt šo personu, kā arī norāda apliecinājuma izdarīšanas datumu.
   4. Piedāvājuma kopiju elektroniskā formātā (vienreiz rakstāmā CD) noformē MS Office, MS Project, Adobe Acrobat vai OpenOffice/LibreOffice nolasāmā formātā. Uz CD norāda pretendenta nosaukumu un iepirkuma identifikācijas numuru.
   5. Visus izdevumus, kas saistīti ar piedāvājuma sagatavošanu un iesniegšanu, sedz pretendents.
2. **Piedāvājuma derīguma termiņš**

Pretendenta iesniegtā piedāvājuma derīguma termiņš ir līdz iepirkuma līguma noslēgšanai, bet ne mazāk kā 60 (sešdesmit) dienas, skaitot no iepirkuma procedūrā noteiktās piedāvājumu iesniegšanas dienas.

1. **Nosacījumi pretendentu dalībai iepirkuma procedūrā:**

8.1.   Iepirkuma procedūras piedāvājumam jābūt par visu iepirkuma priekšmeta apjomu.

8.2.  Iepirkuma procedūras piedāvājumam jābūt latviešu valodā. Svešvalodā sagatavotiem piedāvājuma dokumentiem jāpievieno pretendenta paraksta tiesīgas personas apliecināts tulkojums latviešu valodā.

1. **Prasības pretendentiem, iesniedzamie pretendentu atlases dokumenti un pārbaudāmās ziņas:**
   1. **Prasības pretendentiem:**
      1. Pasūtītājs izslēdz pretendentu no turpmākās dalības iepirkuma procedūrā, kā arī neizskata pretendenta piedāvājumu, ja:
         1. pasludināts pretendenta maksātnespējas process (izņemot gadījumu, kad maksātnespējas procesā tiek piemērota sanācija vai cits līdzīga veida pasākumu kopums, kas vērsts uz parādnieka iespējamā bankrota novēršanu un maksātspējas atjaunošanu), apturēta vai pārtraukta tā saimnieciskā darbība, uzsākta tiesvedība par tā bankrotu vai tas tiek likvidēts;
         2. pretendentam Latvijā vai valstī, kurā tas reģistrēts vai kurā atrodas tā pastāvīgā dzīvesvieta, ir nodokļu parādi, tajā skaitā valsts sociālās apdrošināšanas obligāto iemaksu parādi, kas kopsummā kādā no valstīm pārsniedz 150 EUR.
      2. Pretendenta vidējais gada finanšu apgrozījums iepriekšējo triju (3) gadu (2012., 2013., 2014. vai iepriekšējo triju gadu laikā, par kuriem bija jāiesniedz gada pārskats vai ienākumu deklarācija) (pretendentiem, kas dibināti vēlāk – gada finanšu vidējais apgrozījumu skaita par faktiski nostrādāto laiku) laikā vismaz 2 reizes pārsniedz piedāvājuma cenu. Ja piedāvājumu iesniedz piegādātāju apvienība, visu apvienības dalībnieku finanšu apgrozījumu skaita kopā.
      3. Pretendentu atlases prasības attiecas uz piegādātāju apvienības vai personālsabiedrības kā pretendenta dalībniekiem.
   2. Prasības attiecībā uz pretendenta pieredzi un tehniskajām spējām:
      1. Pretendentam iepriekšējo trīs gadu laikā ir iegūta pieredze datu centra pakalpojumu sniegšanā, vienlaikus nodrošinot vismaz trīs klientiem informācijas sistēmu un tās infrastruktūras ar augstām pieejamības prasībām (pieejamība nav zemāka par 99,90%) izmitināšanu. Minētajā periodā infrastruktūras ar augstām pieejamības prasībām (pieejamība nav zemāka par neplānoto dīkstāvju kopsummu 43 minūtes summāri mēnesī) izmitināšana ir tikusi nodrošināta nepārtraukti ne mazāk kā gadu (uzaicinājuma 6. pielikums).
      2. Pretendents var nodrošināt vismaz 2 (divi) specializētus datu centrus, kas atbilst Ministru kabineta 2012. gada 19. jūnija noteikumos Nr.421 „Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības” (http://likumi.lv/ta/id/249580-valsts-informacijas-sistemu-savietotaju-un-integreto-valsts-informacijas-sistemu-aizsardzibas-prasibas) noteiktajām prasībām savietotāja uzturētājam, un, kas izvietoti divās dažādās ģeogrāfiskās vietās, kā arī Pretendents var nodrošināt Pasūtītāja tehnisko resursu (serveri, disku masīvi, datu rezerves kopēšanas iekārtas, ugunsmūri, slodzes balansētāji, komutatori, u.c.) pārvietošanu starp šiem datu centriem, iepriekš par to vienojoties ar Pasūtītāju.
      3. Pretendents atbilst visām „**Datu centra pakalpojumu sniedzēja pašnovērtējuma tabulā”** izvirzītajām prasībām. Detalizēta informācija par pašnovērtējuma tabulā izvirzītajām prasībām sniegta uzaicinājuma 2. pielikumā.
   3. Iesniedzamie pretendentu atlases dokumenti un pārbaudāmās ziņas:
      1. Pretendenta pieteikums iepirkuma procedūrai (uzaicinājuma 1.pielikums). Pieteikumu paraksta pretendenta vadītājs vai vadītāja pilnvarota persona (jānorāda pilns vārds, uzvārds un amats). Pieteikumā norāda pretendenta nosaukumu un rekvizītus, kā arī apliecina, ka:
         1. iepirkuma procedūras uzaicinājuma nosacījumi ir skaidri un saprotami, pretendents tiem piekrīt un garantē to izpildi;
         2. parakstot iepirkuma līgumu, piegādātājs piekrīt šī iepirkuma līguma publicēšanai pasūtītāja mājaslapā saskaņā ar Publisko iepirkumu likuma 8.2 panta trīspadsmito daļu.
      2. Pārbaudāmās ziņas:
         1. PIL 8.2 panta piektās daļas 1. un 2. punktā minēto apstākļu esamību (uzaicinājuma 9.1.1.1. un 9.1.1.2. apakšpunkts) iepirkuma komisija pārbauda tikai attiecībā uz pretendentu, kuram būtu piešķiramas līguma slēgšanas tiesības atbilstoši noteiktajām prasībām un kritērijiem.
         2. Lai pārbaudītu, vai pretendents nav izslēdzams no dalības iepirkumā PIL 8.2 panta piektās daļas 1. vai 2.punktā (uzaicinājuma 9.1.1.1. un 9.1.1.2. apakšpunkts) minēto apstākļu dēļ, iepirkuma komisija:
         3. attiecībā uz pretendentu (neatkarīgi no tā reģistrācijas valsts vai pastāvīgās dzīvesvietas), izmantojot Ministru kabineta noteikto informācijas sistēmu, Ministru kabineta noteiktajā kārtībā iegūst informāciju:
            1. par PIL 8.2 panta piektās daļas 1.punktā minētajiem faktiem — no Uzņēmumu reģistra,
            2. par PIL 8.2 panta piektās daļas 2.punktā minēto faktu — no Valsts ieņēmumu dienesta un Latvijas pašvaldībām. Iepirkuma komisija minēto informāciju no Valsts ieņēmumu dienesta un Latvijas pašvaldībām ir tiesīga saņemt, neprasot pretendenta piekrišanu;
            3. attiecībā uz ārvalstī reģistrētu vai pastāvīgi dzīvojošu pretendentu papildus pieprasa, lai tas iesniedz attiecīgās ārvalsts kompetentās institūcijas izziņu (izsniegtu ne agrāk kā vienu mēnesi pirms iesniegšanas dienas), kas apliecina, ka uz to neattiecas PIL 8.2 panta piektajā daļā noteiktie gadījumi. Termiņu izziņu iesniegšanai iepirkuma komisija nosaka ne īsāku par 10 (desmit) darbdienām pēc pieprasījuma izsniegšanas vai nosūtīšanas dienas. Ja attiecīgais pretendents noteiktajā termiņā neiesniedz minēto izziņu, iepirkuma komisija to izslēdz no dalības iepirkumā.
            4. Atkarībā no PIL 8.2 panta septītās daļas 1.punkta „b” apakšpunktam (uzaicinājuma 9.3.3.1.2. apakšpunkts) veiktās pārbaudes rezultātiem pasūtītājs:
            5. neizslēdz pretendentu no dalības iepirkumā, ja konstatē, ka saskaņā ar Ministru kabineta noteiktajā informācijas sistēmā esošo informāciju pretendentam nav nodokļu parādu, tajā skaitā valsts sociālās apdrošināšanas obligāto iemaksu parādu, kas kopsummā pārsniedz 150 EUR;
            6. informē pretendentu par to, ka tam konstatēti nodokļu parādi, tajā skaitā valsts sociālās apdrošināšanas obligāto iemaksu parādi, kas kopsummā pārsniedz 150 EUR, un nosaka termiņu — 10 (desmit) darbdienas pēc informācijas izsniegšanas vai nosūtīšanas dienas — konstatēto parādu nomaksai un parādu nomaksas apliecinājuma iesniegšanai. Pretendents, lai apliecinātu, ka tam nav nodokļu parādu, tajā skaitā valsts sociālās apdrošināšanas obligāto iemaksu parādu, kas kopsummā pārsniedz 150 EUR, iesniedz attiecīgi pretendenta vai tā pārstāvja apliecinātu izdruku no Valsts ieņēmumu dienesta elektroniskās deklarēšanas sistēmas vai pašvaldības izdotu izziņu par to, ka attiecīgajai persona laikā pēc pasūtītāja nosūtītās informācijas saņemšanas dienas nav nodokļu parādu, tajā skaitā valsts sociālā apdrošināšanas obligāto iemaksu parādu, kas kopsummā pārsniedz 150 EUR. Ja noteiktajā termiņā minētie dokumenti nav iesniegti, pasūtītājs pretendentu izslēdz no dalības iepirkumā.
      3. Ja pretendents paredzējis piesaistīt apakšuzņēmējus, par katru apakšuzņēmēju jāiesniedz:
         1. apakšuzņēmēja paraksttiesīgas amatpersonas parakstīts apliecinājums par to, ka apakšuzņēmējs piekrīt sadarbībai projekta realizācijā;
         2. dokumenti, kas nepārprotami norāda apakšuzņēmēja veicamo darbu vai piegādājamo preču apjomu;
         3. dokuments, no kura būtu secināms, ka persona, uz kuras iespējām pretendents balstās, lai apliecinātu iepirkuma dokumentos noteikto kvalifikācijas prasību izpildi, pretendenta rīcībā nodos konkrētos resursus līguma izpildes nodrošināšanai.
      4. Klientu atsauksmes par katru informācijas sistēmu, kura apliecina Pretendenta atbilstību nolikuma 9.2.1. punkta prasībām.
      5. Pretendenta atbilstība visām „**Datu centra pakalpojumu sniedzēja pašnovērtējuma tabulā”** izvirzītajām prasībām.
2. **Tehniskais piedāvājums**
   1. Tehniskajā piedāvājumā Pretendentam jāiekļauj:
      1. apliecinājumu (uzaicinājuma 7. pielikums) izpildīt uzaicinājuma tehniskajā specifikācijā (uzaicinājuma 3. pielikums) noteiktās prasības;
      2. pakalpojuma sniegšanas nosacījumu apraksts, kas sevī ietver :
         1. prasības izvietotajām iekārtām;
         2. fiziskās piekļuves procedūras noteikumus un kārtību;
         3. statņu izvietošanas un pieslēgumu shēmu Pakalpojumu sniedzēja Datu centrā;
         4. iekārtu pieņemšanas un nodošana kārtību;
         5. bojājumu pieteikšanas un novēršanas aprakstu;
         6. citu informāciju, kas ir būtiska nozīme pakalpojuma sniegšanā.
3. **Finanšu piedāvājums**
   1. Finanšu piedāvājumu pretendents sagatavo atbilstoši iepirkuma uzaicinājuma nosacījumiem un iepirkuma tehniskajā specifikācijā izvirzītajām prasībām.
   2. Finanšu piedāvājumā cenu norāda eiro bez pievienotās vērtības nodokļa atbilstoši Finanšu piedāvājuma formai (uzaicinājuma 4. pielikums).
4. **Iepirkuma līguma izpildes laiks**

12.1. Iepirkuma līguma (turpmāk tekstā – Līgums) darbības termiņš ir 36 (trīsdesmit seši) mēneši no Līguma noslēgšanas dienas.

1. **Piedāvājumu vērtēšana un lēmuma pieņemšana**
   1. Pretendentu novērtēšanā un salīdzināšanā iepirkuma komisija izskata piedāvājuma atbilstību iepirkuma procedūras uzaicinājumā norādītajām prasībām.
   2. Ja piedāvājums piegādes un pakalpojumu līgumam ir nepamatoti lēts, iepirkuma komisija pirms šā piedāvājuma iespējamās noraidīšanas rakstveidā pieprasa detalizētu paskaidrojumu par būtiskajiem piedāvājuma nosacījumiem.
   3. Piedāvājumus, kas neatbilst iepirkuma procedūras uzaicinājuma prasībām, iepirkuma komisija noraida kā neatbilstošu un tālāk neizskata.
   4. Iepirkuma komisija izvēlas piedāvājumu ar viszemāko cenu, kas atbilst uzaicinājumā norādītajām prasībām.
   5. Iepirkumu komisija pirms lēmuma pieņemšanas veiks pretendenta Datu centru pārbaudi klātienē, iepriekš saskaņojot laikus.
   6. Iepirkuma komisija informē visus pretendentus par iepirkumā izraudzīto pretendentu vai pretendentiem triju darbdienu laikā pēc lēmuma pieņemšanas, kā arī lēmumu ievieto mājaslapā internetā: [www.kase.gov.lv](http://www.kase.gov.lv/) sadaļā “Publiskie iepirkumi”.
   7. Ne vēlāk kā dienā, kad stājas spēkā attiecīgi iepirkuma līgums vai tā grozījumi, pasūtītājs savā mājaslapā internetā ievieto attiecīgi iepirkuma līguma vai tā grozījumu tekstu, atbilstoši normatīvajos aktos noteiktajai kārtībai ievērojot komercnoslēpuma aizsardzības prasības. Iepirkuma līguma un tā grozījumu teksts ir pieejams pasūtītāja mājaslapā internetā vismaz visā iepirkuma līguma darbības laikā, bet ne mazāk kā 36 mēnešus pēc līguma spēkā stāšanās dienas.

|  |  |
| --- | --- |
| Iepirkuma “ Sekundārā datu centra telpu noma” komisijas priekšsēdētājs | A. Rutkis |

*Rutkis 67094256*

1. pielikums

iepirkuma procedūras uzaicinājumam

“ Sekundārā datu centra telpu noma”

iepirkuma identifikācijas Nr. VK/2015/12

Pieteikums dalībai iepirkumā

Pretendents, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ reģ. Nr. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(nosaukums)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(juridiskā adrese, faktiskā adrese)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(tālruņa numurs, faksa numurs, e-pasta adrese)

tā\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_personā\_\_\_\_\_\_\_\_\_\_\_

(personas, kurai ir tiesības pārstāvēt Pretendentu, vārds, uzvārds un amats)

1. Iepazinušies ar iepirkuma procedūras “ Sekundārā datu centra telpu noma” (iepirkuma identifikācijas Nr. VK/2015/12) uzaicinājumu, piesakām dalību šajā iepirkumā.
2. Piekrītam ievērot iepirkuma procedūras uzaicinājuma prasības.
3. Atzīstam sava piedāvājuma spēkā esamību līdz iepirkuma uzaicinājumā noteiktajam piedāvājuma derīguma termiņa beigām.
4. Apliecinām, ka, parakstot iepirkuma līgumu, piegādātājs piekrīt šī iepirkuma līguma publicēšanai pasūtītāja mājaslapā saskaņā ar Publisko iepirkumu likuma 8.2 panta trīspadsmito daļu.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /

(Pretendenta vai tā pilnvarotās personas paraksts) (paraksta atšifrējums)

Vieta \_\_\_\_\_\_\_\_\_\_\_

Datums \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. pielikums

iepirkuma procedūras uzaicinājumam

“ Sekundārā datu centra telpu noma”

iepirkuma identifikācijas Nr. VK/2015/12

**Datu centra pakalpojumu sniedzēja pašnovērtējuma tabula datu centra pakalpojuma nodrošināšanai**

Datu centra pakalpojuma sniedzēja pašnovērtējums balstās uz ENISA *(European Union Agency for Network and Information Security)* izstrādāto mākoņpakalpojumu sniedzēju drošības atbilstības vērtējuma metastruktūrietvaru.

|  |  |  |  |
| --- | --- | --- | --- |
| ***Vērtējuma objekts*** | ***Prasība*** | ***ENISA vadlīnijas (detalizēts skaidrojums)*** | ***Pretendenta apliecinājums par atbilstību/ neatbilstību prasībai\**** |
| 1. Informācijas drošības politika | Pakalpojumu sniedzējs uztur informācijas drošības politiku | SO1 |  |
| 1. Risku vadība | Pakalpojumu sniedzējs uztur atbilstošu pārvaldības un riska vadības ietvaru, lai identificētu Pakalpojumu sniedzēja darbības drošības riskus un veiktu pasākumus to novēršanai. | SO2 |  |
| 1. Drošības lomas | Pakalpojumu sniedzējs nodala un piešķir vajadzībām atbilstošas drošības lomas, pienākumus un atbildības. | SO3 |  |
| 1. Attiecības ar piegādātājiem | Pakalpojumu sniedzējs izstrādā un uztur drošības politiku ar prasībām attiecībā uz līgumiem ar saviem piegādātājiem, lai nodrošinātos, ka atkarība no piegādātājiem neatstātu negatīvu ietekmi uz Pakalpojumu sniedzēja sniegto pakalpojumu drošību | SO4 |  |
| 1. Blakus informācijas pārbaude | Pakalpojumu sniedzējs veic atbilstošas likumos atļautas blakus informācijas pārbaudes attiecībā par personāla uzticamību (darbiniekiem, darbuzņēmējiem un trešajām pusēm), ja šāda uzticība nepieciešama veicamo darba pienākumu dēļ. | SO5 |  |
| 1. Zināšanas par drošību un mācības | Pakalpojumu sniedzējs veic pārbaudes, vai personālam ir pietiekamas zināšanas drošības jomā.  Pakalpojumu sniedzējs savam personālam nodrošina regulāras mācības par drošības jautājumiem | SO6 |  |
| 1. Personāla mainība | Pakalpojumu sniedzējs izstrādā un uztur atbilstošus personāla mainības un tā lomu un pienākumu izmaiņu pārvaldības procesu. | SO7 |  |
| 1. Fiziskā un vides drošība | Pakalpojumu sniedzējs izstrādā, uztur un realizē datu centra fiziskās, kā arī vides drošības politikas. | S09 |  |
| 1. Atbalsta resursu drošība | Pakalpojumu sniedzējs izstrādā un uztur atbilstošu atbalsta resursu (elektrība, degviela, siltums u.tml.) esamību un pietiekamību | SO10 |  |
| 1. Piekļuves kontrole tīklam un informācijas sistēmām | Pakalpojumu sniedzējs izstrādā un uztur atbilstošu politiku un pasākumus piekļuvei Datu centra resursiem | SO11 |  |
| 1. Infrastruktūras un informācijas sistēmu integritāte | Pakalpojumu sniedzējs izstrādā un uztur savas infrastruktūras, platformu un pakalpojumu integritāti un pasargā tos no vīrusiem, kodu iefiltrēšanas un citas ļaunprātīgas programmatūras, kas var izmainīt sistēmu funkcionalitāti | SO12 |  |
| 1. Darbības procedūras | Pakalpojumu sniedzējs izstrādā un uztur procedūras, kas nosaka, kā tā personāls strādā ar infrastruktūru un informācijas sistēmām. | SO13 |  |
| 1. Izmaiņu vadība | Pakalpojumu sniedzējs izstrādā un uztur izmaiņu kārtību attiecībā uz infrastruktūras un informācijas sistēmu pārvaldību. | SO14 |  |
| 1. Resursu pārvaldība | Pakalpojumu sniedzējs izstrādā un uztur resursu pārvaldības procedūras un konfigurācijas kontroles attiecībā uz infrastruktūru un informācijas sistēmām | SO15 |  |
| 1. Drošības incidentu atklāšana un pasākumi to novēršanai | Pakalpojumu sniedzējs izstrādā procedūras incidentu atklāšanai un atbilstošai to novēršanai | SO16 |  |
| 1. Ziņošana par drošības incidentiem | Pakalpojumu sniedzējs izstrādā un uztur atbilstošas procedūras ziņošanai un paziņojumiem par drošības incidentiem | SO18 |  |
| 1. Darbības nepārtrauktība | Pakalpojumu sniedzējs izstrādā un uztur ārkārtas rīcības plānus un darbības nodrošināšanas stratēģiju Datu centra pakalpojumu nepārtrauktības nodrošināšanai | SO19 |  |
| 1. Ārkārtas situāciju seku novēršanas spēja | Pakalpojumu sniedzējs izstrādā un uztur atbilstošus ārkārtas situāciju seku novēršanas resursus, lai atjaunotu Datu centra sniegtos pakalpojumus dabas un/vai citu lielu katastrofu gadījumā | SO20 |  |
| 1. Monitorings un reģistrēšanas process | Pakalpojumu sniedzējs izstrādā un uztur Datu centra pakalpojumu uzraudzības (tehniskā monitoringa) un notikumu reģistrēšanas sistēmas | SO21 |  |
| 1. Sistēmas testi | Pakalpojumu sniedzējs izstrādā un izpilda galveno Datu centra pakalpojumu uzturošās infrastruktūras un informācijas sistēmu testēšanas procedūras | SO23 |  |
| 1. Drošības novērtējums | Pakalpojumu sniedzējs izstrādā un izpilda atbilstošas svarīgāko resursu drošības novērtējuma veikšanas procedūras | SO24 |  |
| 1. Atbilstības pārbaude | Pakalpojumu sniedzējs izstrādā atbilstības politiku un atbilstoši tai veic normatīvajos aktos paredzētās pārbaudes | SO25 |  |
| 1. Datu centra datu drošība | Pakalpojumu sniedzējs izstrādā un uztur atbilstošus mehānismus klientu datu aizsardzībai Datu centra pakalpojumu ietvaros |  |  |
| 1. Datu centra saskarņu drošība | Pakalpojumu sniedzējs izstrādā un uztur atbilstošu politiku Datu Centra pakalpojumu saskarņu drošībai |  |  |
| 1. Datu centra programmatūras drošība | Pakalpojumu sniedzējs izstrādā un uztur programmatūras drošības politiku |  |  |
| 1. Datu centra savietojamība un pārnesamība | Pakalpojumu sniedzējs lieto standartus, kas ļauj klientiem koordinēti lietot citus Datu centra pakalpojumus un/vai, ja nepieciešams, migrēt pie citiem Datu centru operatoriem, kas piedāvā līdzīgus pakalpojumus. |  |  |
| 1. Datu Centra monitoringa uzraudzības process | Pakalpojumu sniedzējs nodrošina klientiem piekļuvi attiecīgajiem darījumu un darbības snieguma žurnāliem, lai klienti nepieciešamības gadījumā varētu izpētīt konkrētus jautājumus vai incidentus. |  |  |

\* Pretendents katrā ailē sniedz informāciju, vai nodrošina prasības izpildi, aizpildot to ar vārdiem “Tiek nodrošināts” vai “Netiek nodrošināts”.

Pretendenta uzņēmuma vadītājs vai vadītāja pilnvarota persona:

|  |  |
| --- | --- |
| **Vārds, uzvārds, amats** |  |
| **Paraksts un zīmogs** |  |
| **Datums** |  |

**ICT iepirkuma drošības vadlīnijas**

*ICT iepirkuma drošības vadlīnijas elektronisko sakaru operatoriem*

2014.gada decembris

**2. Drošības vadlīnijas pakalpojumu pārdevējiem**

**2.1. Pārvaldība un risku vadība**

**SO1: Informācijas drošības politika / SO2: Pārvaldība un risku vadība**

|  |
| --- |
| ***Drošības riski*** |
| Pakalpojumu sniedzēja nespēja saskaņot savas darbības drošības jomā ar Pakalpojumu ņēmēja drošības mērķiem. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam ir pilnībā jāizprot un jāintegrē Pakalpojumu ņēmēja drošības mērķi. * Izvēlētajam Pakalpojumu sniedzējam ir jābūt informācijas drošības politikai, nodrošinot tā produktu un pakalpojumu drošību un elastību, un jāatbilst Pakalpojumu ņēmēja augsta līmeņa drošības mērķiem. * Pakalpojumu sniedzējiem jānodrošina Pakalpojumu ņēmējam analīzei tā attiecīgās iekšējās informācijas drošības politikas pierādījumi, nodrošinot ņēmēja produktu un pakalpojumu drošību un elastību. |
| ***Drošības riski*** |
| Pakalpojumu sniedzējs nespēj nodrošināt atbilstību Pakalpojumu ņēmēja drošības mērķiem komunikācijas abu pušu starpā un neizpratnes trūkuma dēļ attiecībā uz Pakalpojumu sniedzēja veicamajām darbībām. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam jāparaksta līgums, kurā paredzētas specifiskas Pakalpojumu ņēmēja noteiktas un ar tā drošības mērķiem saskaņotas drošības prasības. Drošības prasībām jābūt skaidrām, precīzām, īstenojamām un izmērāmām. * Pakalpojumu ņēmējs definē drošības prasības risku novērtēšanas laikā. * Pakalpojumu ņēmējam ir jābūt iespējai pieprasīt drošības prasību aktualizēšanu, ņemot vērā jebkādus Pakalpojumu ņēmēja sistēmu ietekmējošus testus/uzdevumus vai atgadījumus un /vai līdzīgus Pakalpojumu sniedzēja produktus vai pakalpojumus. Aktualizētās drošības prasības Pakalpojumu sniedzējam ir jāīsteno bezierunu kārtībā. |

|  |
| --- |
| ***Drošības riski*** |
| Pakalpojumu ņēmējs nespēj izpildīt nacionālo tiesību aktu vai sekundāro tiesību aktu prasības Pakalpojumu sniedzēja atbalsta neesamības dēļ. |
| ***Drošības prasības*** |
| * Pakalpojumu ņēmējam jāspēj lūgt Pakalpojumu sniedzējam ievērot pakalpojumu ņēmējam saistošos tiesību aktu vai sekundāro tiesību aktu prasības, nepalielinot izmaksas. |

**SO3: Drošības lomas un atbildība**

|  |
| --- |
| ***Drošības riski*** |
| Skaidri un/vai pareizi nesadalītas lomas un atbildība drošības risku pārvaldībā starp Pakalpojumu sniedzēju un ņēmēju, kas rada:   * neskaidrību un nesaprašanos pušu starpā draudu vai incidentu gadījumā; * nepareizu drošības prasību īstenošanu; * atbildības trūkumu gadījumos, kad tiek pārkāptas tādas drošības prasības, kas nav atzītas Pakalpojumu sniedzēja organizācijā. |
| ***Drošības prasības*** |
| * Līgumā skaidri definēt un noteikt atbildību, lai izvairītos no neskaidrības, pārpratumiem vai ļaunprātīgas izmantošanas. * Pakalpojumu sniedzēja organizācijā ir jānozīmē viena atbildīgā persona, kura visā līguma darbības laikā nodrošinās, ka: * drošības riski un prasības ir pilnībā izprasti; * ir atbilstoši procesi un ar pakalpojuma ņēmēju ir panākta vienošanās par minimālo pieņemamo atlikušā riska līmeni, ko ir atbilstoši akceptējusi katra puse; * drošības riski tiek pārvaldīti un ir atbilstoši procesi, par ko tiek paziņots Pakalpojumu ņēmējam; * Pakalpojumu ņēmējam tiek nodrošināts atbilstošs atbalsts, izmantojot attiecīgu palīdzības komandu vai citas līgumā noteiktās iespējas; * tiek ievēroti līguma nosacījumi. * Ir nepieciešams skaidri definēt tos nepārvaramas varas apstākļus, kas pakalpojuma sniedzēju atbrīvo no atbildības, lai izvairītos no Pakalpojumu sniedzēja ļaunprātīgām darbībām. |

**SO4: Attiecības ar piegādātājiem**

|  |
| --- |
| ***Drošības riski*** |
| Pakalpojumu ņēmēja pakļautība papildu drošības riskiem, ja pakalpojuma sniedzējs, lai nodrošinātu Pakalpojumu ņēmējam produktus vai pakalpojumus, izmanto lejupējus apakšuzņēmējus. Šie draudi ietver turpmāk minētos (bet ne tikai):   * nav informācijas par lejupējiem apakšuzņēmējiem; * pakalpojuma sniedzējs pienācīgi neuzrauga un neveic tā apakšuzņēmēju efektīvu kontroli.   Drošības prasību nepiemērošana Pakalpojumu sniedzēja apakšuzņēmējiem. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam jāsniedz informācija par esošajiem un/vai potenciālajiem apakšuzņēmējiem, kas tiek/tiks izmantoti produktu un pakalpojumu nodrošināšanai Pakalpojumu ņēmējam. Šīs informācija tiks iekļauta Pakalpojumu ņēmēja veiktajā riska novērtējumā un tiks ņemtas vērā, definējot drošības prasības. * Apakšuzņēmējam jānodrošina tie paši vai līdzvērtīgi drošības pasākumi, kas ir attiecināmi uz pakalpojuma sniedzēju. * Pakalpojuma sniedzējs ir vienīgais atbildīgais par tā apakšuzņēmēju veiktajām darbībām, tas atbild par drošības pārvaldību tā apakšuzņēmēju vidū un garantē drošības prasību efektīvu darbību, lai nodrošinātu atbilstību Pakalpojumu ņēmēja drošības mērķiem. |

**2.2. Cilvēkresursu drošība**

**SO5: Blakus informācijas pārbaude**

|  |
| --- |
| ***Drošības riski*** |
| Apzinātas vai neapzinātas Pakalpojumu sniedzēja darbinieku veiktas produktu vai sistēmu izmaiņas, tostarp kļūdainas izmaiņas vai uzlabojumi, konfigurācijas kļūdas, slikta uzturēšana, darbinieku ļaunprātīgas darbības u.tml. |
| ***Drošības prasības*** |
| * Jānodrošina Pakalpojumu sniedzēja darbinieku sertifikāti, kas apliecinātu viņu atbilstošo pieredzi drošības risku pārvaldībā. * Ja to pieļauj tiesību aktu normas un ja tas ir pamatojams ar sniegtā pakalpojumu būtiskumu, Pakalpojumu sniedzējam jāveic attiecīgās pārbaudes, lai piefiksētu visa veida noziedzīgus notikumus tā darbinieku pagātnē, lai izvairītos no ļaunprātīgām un apzinātām produktu vai sistēmu izmaiņām. Ar pārbaudes rezultātiem ir jāiepazīstina Pakalpojumu ņēmējs. |

**SO6: Zināšanas par drošību un mācības**

|  |
| --- |
| ***Drošības riski*** |
| Pakalpojuma sniedzējs nenodrošina pietiekamu skaitu prasmīgu un apmācītu resursu efektīvai risku pārvaldībai. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzēja darbiniekiem ir jāiziet atbilstošas apmācības, lai ieviestu un pielietotu praksē Pakalpojumu ņēmēja noteiktās drošības prasības. * Pakalpojumu sniedzējam ir jānodrošina pietiekami pierādījumi par tā darbinieku apgūto mācību programmu. * Ja Pakalpojumu ņēmējs pieprasa, Pakalpojumu sniedzējam ir jābūt nepieciešamajam kvalificētajam personālam (piem., ar ISO, ISACA html. Sertifikātiem). * Noteiktai daļai Pakalpojumu sniedzēja darbinieku ir regulāri jāapmeklē apmācības, lai attīstītajā tehnoloģiju vidē ar mainīgo praksi drošības jomā būtu informēti par aktuālākajiem jautājumiem. * Pakalpojumu sniedzējam jāveic attiecīgas pārbaudes, lai pārliecinātos par to, ka tā darbiniekiem ir pietiekamas drošības un tehniskās zināšanas, prasmes un kvalifikācija, lai izvairītos no neapzinātām produktu vai sistēmu izmaiņām. Ar pārbaudes rezultātiem ir jāiepazīstina Pakalpojumu ņēmējs. |

**SO7: Personāla mainība**

|  |
| --- |
| ***Drošības riski*** |
| Jauna personāla vai personāla maiņas dēļ Pakalpojumu sniedzējam traucēta un neefektīva drošības risku pārvaldība, rezultātā novirzoties no līguma specifikācijām. |
| ***Drošības prasības*** |
| * Visiem Pakalpojumu sniedzēja vai lejupējo apakšuzņēmēju darbiniekiem, kam ir piešķirta piekļuve konfidenciālai informācijai vai personas datiem Pakalpojuma izpildes laikā, pie sava darba devēja ir jāparaksta līgums par konfidencialitātes ievērošanu vai informācijas neizpaušanu. Pakalpojumu sniedzējam arī jāparedz parakstītajā līgumā punkti par konfidencialitāti un personas datu aizsardzību. * Par visām personāla izmaiņām atbilstoši līgumam ir jāinformē Pakalpojumu ņēmējs. * Par personāla maiņu attiecībā uz konkrēto pakalpojumu jāvienojas ar Pakalpojuma ņēmēju. * Zināšanu nodošanas procesu definē un veic Pakalpojuma pārdevējs un tie darbinieki, kuri tiek aizstāti. * Pakalpojumu sniedzējam ir savlaicīgi jāatsauc to darbinieku piekļuves tiesības Pakalpojumu ņēmēja informācijas sistēmām, kuri vairs ar tām nestrādās. |

**2.3. Sistēmu un telpu drošība**

**SO9: Fiziskā un vides drošība**

|  |
| --- |
| ***Drošības riski*** |
| Vājo vai neesošo Pakalpojumu sniedzēja nodrošināto loģisko piekļuves kontroļu rezultātā var rasties neapzinātas vai apzinātas produktu vai sistēmas izmaiņas |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam ir jābūt specifiskiem drošības procesiem, kas nodrošina tā produktu vai sistēmu fizisko drošību un nepieļauj nesankcionētu piekļuvi tā fiziskajām telpām un infrastruktūrai, ieskaitot (bet ne tikai): * drošības pasākumus ražošanas vietās; * drošības pasākumus uzglabāšanas telpās; * drošības pasākumus darba telpās; * drošības pasākumus attiecībā uz transporta vai piegādes aprīkojumu. * Ar pārbaudes rezultātiem ir jāiepazīstina Pakalpojumu ņēmējs. * Pakalpojumu sniedzējam regulāri jāuzrauga pasākumu ievērošana. * Pakalpojumu sniedzējam periodiski jānovērtē procesu efektivitāte un, kad nepieciešams, tie jāpārskata, it īpaši pēc incidentiem un testiem/uzdevumiem, kas ietekmē Pakalpojumu ņēmēja sistēmas un/vai līdzīgus Pakalpojumu ņēmēja produktus vai pakalpojumus. |

**SO10: Atbalsta resursu drošība**

|  |
| --- |
| ***Drošības riski*** |
| Nepietiekami atbalsta resursi (elektrība, degviela dīzeļģeneratoram, siltums, aukstums u. tml.) var traucēt Pakalpojuma sniedzēja spēju sniegt pakalpojumu |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējs izstrādā un uztur atbilstošu atbalsta resursu (elektrība, degviela, siltums, aukstums u.tml.) esamību un pietiekamību. * Pakalpojuma sniedzējam ir atbalsta resursu piegādes politika, kura paredz alternatīvus resursu piegādes kanālus * Pakalpojumu sniedzējs pielieto industriālo standartu atzītus drošības risinājumus stabilai resursu piegādei * Pakalpojumu sniedzējs regulāri pārskata resursu piegādes metodes un iespējas, atjaunina tās, ņemot vērā resursu tehnoloģisko attīstību un iepriekšējos drošības incidentus |

**SO11: Piekļuves kontrole tīklam un informācijas sistēmām**

|  |
| --- |
| ***Drošības riski*** |
| Vājo vai neesošo Pakalpojumu sniedzēja nodrošināto fiziskās piekļuves kontroļu rezultātā var rasties neapzinātas vai apzinātas produktu vai sistēmas izmaiņas |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam ir jābūt specifiskām loģiskās piekļuves kontrolēm, lai nodrošinātu tā produktu vai sistēmu drošību un nepieļautu nesankcionētu piekļuvi tā tīkliem un informācijas sistēmām, ieskaitot (bet ne tikai): * lietotāju identifikāciju un autentikāciju; * unikālo ID; * pienākumu sadali; * priviliģētās piekļuves grupas. * Ar pārbaudes rezultātiem par loģiskajām piekļuves kontrolēm jāiepazīstina Pakalpojumu ņēmējs. * Pakalpojumu sniedzējam periodiski jānovērtē procesu efektivitāte un, kad nepieciešams, tie jāpārskata, it īpaši pēc incidentiem un testiem/uzdevumiem, kas ietekmē Pakalpojumu ņēmēja sistēmas un/vai līdzīgus Pakalpojumu sniedzējs produktus vai pakalpojumus elektronisko sakaru nozarē. * Piekļuvei sensitīvajiem tīkliem un informācijas sistēmām jābūt ierobežotai un pieejamai tikai tiem Pakalpojumu sniedzēja darbiniekiem, kuriem tas nepieciešams darba uzdevumu veikšanai. * Pakalpojumu sniedzējam regulāri jāpārskata to personu saraksts (un tām piešķirtās tiesības un privilēģijas), kurām piešķirta piekļuve tīkliem un informācijas sistēmām. * Pakalpojumu sniedzējam jāveic aktivitāšu žurnāla pārskats, lai atzīmētu jebkādas nestandarta darbības. Šo pārskatīšanu jāveic trešajai personai (piem., neatkarīgam kvalitātes pārskatītājam Pakalpojumu sniedzēja organizācijā). * Pakalpojumu sniedzējam. jāveic Sistēmas darbību izsekošana un visu tās bojāšanas mēģinājumu, izmaiņu vai nesankcionētas piekļuves reģistrēšana |

**SO12: Tīkla un informācijas sistēmu integritāte**

|  |
| --- |
| ***Drošības riski*** |
| Tāda ļaunprātīga satura kā vīrusi, kodi vai ļaunprātīga programmatūra ievietošana, kas rada produkta vai sistēmas integritātes un/vai funkcionalitātes izmaiņas. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam jāpārbauda produkta vai sistēmas integritāte, pirms tās integrēšanas Pakalpojumu ņēmēja infrastruktūrā, veicot atbilstošu skenēšanu un testēšanu. * Ar testēšanas/skenēšanas procedūrām un rezultātiem jāiepazīstina Pakalpojumu ņēmējs. * Viltotu vienumu gadījumā Pakalpojumu sniedzējam jāveic atbilstoši pasākumi to nomaiņai, nodrošinot Pakalpojumu ņēmējam nepārtrauktu pakalpojumu, saglabājot tādu pašu drošības līmeni. |

**2.3. Darbību pārvaldība**

**S013: Darbības procedūras**

|  |
| --- |
| ***Drošības riski*** |
| Pakalpojuma pārdevējs neveic ikdienas darbības atbilstoši Pakalpojumu ņēmēja drošības prasībām. |
| ***Drošības prasības*** |
| * Līguma ietvaros Pakalpojumu sniedzējam jānoslēdz ar Pakalpojuma ņēmēju Pakalpojumu līmeņa vienošanās (Service Level Agreement – SLA), kur izmērāmās vienībās ir noteikts, kādus pakalpojumus Pakalpojumu sniedzējam jāsniedz. Tajā ir noteikts: * Minimālais Pakalpojumu ņēmējam pieņemamais pakalpojumu līmenis. * Minimālais Pakalpojumu ņēmējam pieņemamais atlikušā riska līmenis (kad ir veiktas kontroles). Par šo minimālo Pakalpojumu ņēmējam pieņemamo atlikušā riska līmeni jāvienojas ar Pakalpojumu ņēmēja augstākā līmeņa vadību. * Uz drošību vērstie Galvenie darbības indikatori (Key Performance Indicators – KPI), pēc kuriem Pakalpojumu ņēmējs novērtēs Pakalpojumu sniedzējs sniegumu. KPI jābūt precīziem un izmērāmiem. * Pakalpojumu sniedzēja snieguma vērtējuma regularitāte, kad Pakalpojumu ņēmējs vēlreiz izskata SLA. * Pakalpojumu sniedzējam jāsniedz visi pamatojošie dati, protokoli vai pārskati, kas Pakalpojumu ņēmējam atvieglo snieguma novērtējumu. Papildus Pakalpojumu sniedzējam jāsniedz Pakalpojumu ņēmējam informācija, lai tas varētu pilnībā saprast datus, protokolus vai pārskatus. * Attiecībā pret Pakalpojuma pārdevēju ir jāpiemēro soda sankcijas, ja ir konstatētas nepilnības vai nobīdes no SLA. Attiecībā uz ļoti svarīgām sistēmām jāvienojas par lielākām soda sankcijām. |

**SO14: Izmaiņu vadība**

|  |
| --- |
| ***Drošības riski*** |
| Nav izdevies veikt izmaiņas (piem., atjaunināšanas kļūme), kā dēļ Pakalpojumu ņēmēji daļēji vai pilnībā nevar sniegt pakalpojumus pārmaiņu vadības procesu neesamības vai to neefektivitātes dēļ.  Neefektīvas drošības prasības vāju izmaiņu vadības procesu vai to neesamības dēļ vidē, kas attīstās līdz ar konstantām tehnoloģiskajām pārmaiņām. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam ir jāuztur izmaiņu vadības procesi. Var īstenot dažādus procesus atkarībā no nepieciešamo izmaiņu veida: * jaunatklāta vājā vieta, kā dēļ jāpieņem papildu drošības pasākumi; * programmatūras atjaunināšana; * aparatūras nomaiņa. * Izmaiņu vadības procesā jābūt iekļautai precīzai un efektīvai testēšanai (sk. SO23). Precīzāk, Pakalpojumu sniedzējam pirms to integrēšanas reālajā vidē ir jātestē visas programmatūras vai aparatūras izmaiņas. Par rezultātiem jāinformē Pakalpojumu ņēmējs. * Par izmaiņu iniciēšanas pienākumu un papildu izmaksām jāvienojas iepriekš un tie jāparedz līgumā. * Pakalpojumu sniedzējam jāuzņemas atbildība par izmaiņām, kas saistītas ar: * visām Pakalpojumu sniedzēja ierosinātajām izmaiņām; * citām līgumā paredzētām izmaiņām (piem., atjauninājumiem) * variācijām pakalpojumu līmenī Pakalpojumu sniedzēja dēļ; * jaunatklātām vājajām vietām Pakalpojumu sniedzēja produktā vai sistēmā. * Pakalpojumu sniedzēja koriģējošās darbības pēc drošības incidenta. |
|  |
| ***Drošības riski*** |
| Pakalpojuma Pārdevējs neuztur stabilu drošības līmeni un pārejas procesā, kad līguma ar Pakalpojuma ņēmēju darbības laiks ir beidzies, neievēro drošības prasības. |
| ***Drošības prasības*** |
| * Ir jābūt ārkārtas rīcības plānam, ja gadījumā kāda no pusēm vēlas izbeigt saistības pirms līguma darbības beigām. * Pakalpojumu sniedzējam jādefinē un jāvienojas ar Pakalpojuma ņēmēju par pārejas plānu, nodrošinot drošības pārvaldību līdz nodošanai Pakalpojumu ņēmējam vai citam Pakalpojumu sniedzējam ir pabeigta. * Pakalpojumu sniedzējam jānodod visi ar produktu vai pakalpojumu saistītie dokumenti, procedūras, konfigurācijas, ieraksti u.c., kas nepieciešami, lai nodrošinātu raitu turpmāku pakalpojumu sniegšanu Pakalpojumu ņēmējam. * Pakalpojumu sniedzējam jāatdod vai jāiznīcina visi Pakalpojumu ņēmēja informāciju saturošie faili, ieraksti un dokumenti. * Ja ar Pakalpojuma ņēmēju ir vienošanās par kādas informācijas paturēšanu, ir jāvienojas par īpašiem drošības pasākumiem un Pakalpojumu sniedzējam tie jāīsteno, lai nodrošinātu konfidencialitāti un Pakalpojumu ņēmēja datu aizsardzību. |

**SO15: Resursu pārvaldība**

|  |
| --- |
| ***Drošības riski*** |
| Nav savlaicīga nomaiņas plāna un efektīvas loģistikas funkcijas gadījumā, ja daži komponenti, produkti vai sistēmas salūzt ātrāk vai noveco, tādējādi padarot elementa nomaiņu \*vai atjaunināšanu\*\* neiespējamu, rezultātā radot traucējumus Pakalpojumu ņēmēja darbībā.  \*Pakalpojuma Pārdevēji var neturpināt kādu produktu ražošanu, jo tehnoloģijas attīstās ļoti strauji. Komponenti, produkti vai sistēmas var nebūt pieejami Pakalpojumu ņēmējam. Nomaiņa nebūs iespējama.  \*\* Tā kā tehnoloģijas attīstās ļoti strauji, atjauninājumi var nebūt savietojami ar novecojušo sistēmu vai infrastruktūru. Atjauninājumi nebūs iespējami. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam ir jāuztur izmaiņu vadības procesi (piem., programmatūras atjauninājumi, aparatūras nomaiņa u.c.) (skat. SO14). * Pakalpojumu sniedzējam ir jāparedz laiks posms, kurā tā produkti vai sistēmas kļūs novecojuši. * Pakalpojumu sniedzējam jāveic regulāras tā produktu un sistēmu pārbaudes, lai atklātu novecošanas pazīmes jau agrīnā stadijā. * Pakalpojumu sniedzējam jāizstrādā un jāievieš nomaiņas vai atjaunināšanas plāns, ņemot vērā savietojamu produktu, rezerves daļu un tādu atjauninājumu pieejamību, kas ir savietojami ar esošo infrastruktūru, lai nodrošinātu nepārtrauktu pakalpojumu sniegšanu Pakalpojumu ņēmējam. * Pakalpojumu sniedzējam jāsniedz pierādījumi tam, ka tam ir efektīva loģistikas funkcija, ar ko tiek pārvaldīti tā komponenšu krājumi, produkti un sistēmas, un nodrošināta to vai atbilstošu aizvietotāju pieejamība saprātīgos termiņos. * Pakalpojumu sniedzējam jāgarantē visu būtisko sastāvdaļu, produktu un sistēmu nomaiņa vai atjaunināšana ar Pakalpojuma ņēmēju līgumā saskaņotā termiņā, lai nepieļautu pārtraukumus Pakalpojumu ņēmēja pakalpojumos (atsauce uz SO19). * Pakalpojumu sniedzējam jāinformē Pakalpojumu ņēmējs par produkta atjauninājuma pieejamību. * Pakalpojumu sniedzējam jāsniedz atbalsts nomaiņas vai atjaunināšanas gadījumā. * Abām pusēm līgumā jāvienojas par minimālo laiku, kādā attiecībā uz produktu tiks nodrošināts Pakalpojumu sniedzējs atbalsts. |

**2.5. Incidentu pārvaldība**

**SO16: Incidentu pārvaldības kārtība**

|  |
| --- |
| ***Drošības riski*** |
| Plašāka mēroga pakalpojumu traucējumu ietekme neefektīvas incidentu pārvaldības dēļ. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam ir jābūt kārtībai par rīcību ārkārtas situācijās darbam incidentu situācijās un/vai jāsniedz atbalsts Pakalpojumu ņēmējam incidentu pārvaldīšanai. Kārtībā ir jāparedz scenāriji atkarībā no incidentu veida, pušu lomas un pienākumi, krīzes vadības process u.c. * Pakalpojumu sniedzējam ir jābūt pakalpojuma nepārtrauktības nodrošināšanas plānam (skat. SO19) un ārkārtas situāciju seku likvidēšanas plānam (skat. SO20), lai minimizētu incidenta ietekmi uz Pakalpojumu ņēmēja pakalpojumu pieejamību. * Pakalpojumu sniedzējam jāievēro SLA minētais un ar Pakalpojuma ņēmēju saskaņotais maksimālais laiks labojumu veikšanai un maksimālais laiks darbības atjaunošanai. * Pakalpojumu sniedzējam ir jāizvērtē katrs incidentu pārvaldības gadījums, un Pakalpojumu ņēmējam ir jābūt iespējai iepazīties ar pārskatu (SO18). * Ja tas nepieciešams incidentu pārvaldības uzlabošanai, Pakalpojumu sniedzējam ar Pakalpojuma ņēmēju ir jāvienojas par dažiem uzlabojumiem (piem., labākas darbplūsmas, jauni saziņas veidi u.tml.) un tie jāievieš (skat. SO18). |

**SO18: Ziņošana par incidentiem un komunikācija**

|  |
| --- |
| ***Drošības riski*** |
| Savlaicīgi nenosūtīts agrīnās brīdināšanas ziņojums Pakalpojumu ņēmējam par visām nestandarta situācijām, aizdomām par incidentiem vai aizdomām par situāciju tuvu kļūmei, kas rada sliktu incidentu pārvaldību un traucējumus pakalpojumu sniegšanā.  Informācijas trūkums par agrākiem incidentiem, aizdomām par incidentiem, situācijām tuvu kļūmei, aizdomām par situācijām tuvu kļūmei vai nestandarta situācijām, kas radušies Pakalpojumu ņēmēja infrastruktūrā. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam jāīsteno procesi, lai precīzi un savlaicīgi ziņotu pakalpojumu Ņēmējam par visiem drošības incidentiem un drošības noteikumu pārkāpumiem tā produktos vai pakalpojumos, vai visiem datu noplūdes gadījumiem, kas saistīti ar pakalpojumu sniedzēju, kā arī par visiem līgumā vai tiesību aktos noteikto drošības prasību pārkāpumiem. * Pakalpojumu sniedzējam nestandarta situāciju, aizdomu par incidentu vai aizdomu par situāciju tuvu kļūmei gadījumā nekavējoties jāuzsāk agrīnā brīdināšana; * Pakalpojumu sniedzējam jāziņo par visiem agrākiem incidentiem, aizdomām par incidentiem, situācijām tuvu kļūmei, aizdomām par situācijām tuvu kļūmei vai nestandarta situācijām, kas radušies Pakalpojumu ņēmēja infrastruktūrā. * Vienojoties ar Pakalpojuma ņēmēju, varētu noteikt dažus sliekšņus, lai ziņoti tikai par specifiskām trauksmēm pēc to svarīguma pakāpes. * Pakalpojumu sniedzējam jāziņo Pakalpojumu ņēmējam par visiem incidentiem tā produktos vai pakalpojumos notikušajiem incidentiem, ja šos pašus produktus un pakalpojumus uz līguma pamata izmanto arī Pakalpojumu ņēmējs. * Pakalpojumu sniedzējam un Pakalpojumu ņēmējam jānosaka skaidra ārkārtas situāciju seku novēršanas kārtība, lai nodrošinātu labi definētu un efektīvu informācijas apriti. Tajā jāparedz abu pušu ārkārtas situāciju seku novēršanas kanāli un kontakti (galvenie un rezerves). * Pakalpojumu sniedzējam ir jāizmeklē agrākie incidenti, jāsniedz Pakalpojumu ņēmējam atbalsts to izmeklēšanā vai lūgt to izmeklēšanu veikt trešajām personām, lai atrastu galvenos to cēloņus. Par to var vienoties līgumā vai katrā gadījumā atsevišķi. * Ja tas nepieciešams, lai izvairītos no turpmākiem incidentiem, jāvienojas ar Pakalpojuma ņēmēju par koriģējošām darbībām, kas jāveic Pakalpojumu sniedzējam. |

**2.6. Darbības nepārtrauktības pārvaldība**

**SO19: Pakalpojumu nepārtrauktības nodrošināšanas stratēģija un ārkārtas rīcības plāni**

|  |
| --- |
| ***Drošības riski*** |
| Ir vāja pakalpojumu nepārtrauktības nodrošināšanas stratēģija, kas garantētu pakalpojumu pieejamību Pakalpojumu ņēmējam incidenta gadījumā, vai tās nav nemaz. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam ar rīkiem, prasmēm un resursiem vai procesiem jānodrošina Pakalpojumu ņēmēja pakalpojumu nepārtraukta darbība, nodrošinot minimālo SLA noteikto un Pakalpojumu ņēmēja apstiprināto pakalpojumu sniegšanas līmeni. Tas cita starpā var ietver: * rezerves daļas[[1]](#footnote-1); * rezervi; * rezerves personālu, lai nodrošinātu, ka vienmēr tiek uzturētas svarīgākās funkcijas. * Pakalpojumu sniedzējam ir jāsniedz pilna dokumentācija par darbības nepārtrauktības nodrošināšanas procesiem. * Precīzāk, ārpakalpojuma pakalpojuma Pakalpojumu sniedzējam ir jābūt pakalpojuma nepārtrauktības nodrošināšanas plānam, īpaši pievēršoties potenciālajiem strāvas padeves vai Interneta pieslēgumu traucējumiem. Tas ir ļoti būtiski, ņemot vērā to, ka strāvas padeves vai Interneta pieslēguma traucējumi pilnībā vai daļēji var izraisīt Pakalpojumu ņēmēja pakalpojumu nepieejamību. * Pakalpojumu sniedzējs darbības nepārtrauktības nodrošināšanas plānā ir jāņem vērā tā atkarība no apakšuzņēmējiem. * Pakalpojumu sniedzējam jāpārskata savs pakalpojumu nepārtrauktības nodrošināšanas plāns, ņemot vērā agrākos incidentus un agrāko pieredzi, un, ja nepieciešams, tas jāpārstrādā. |

**SO20: Ārkārtas situāciju seku novēršanas spēja**

|  |
| --- |
| ***Drošības riski*** |
| Ir vāja pakalpojumu darbības atjaunošanas spēja vai tās neesamība Pakalpojumu ņēmēja pakalpojumu darbības atjaunošanai dabas katastrofu, nopietnu pārkāpumu vai pilnīga pakalpojumu darbības pārtraukuma gadījumā. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam ar rīkiem, prasmēm, resursiem vai procesiem jānodrošina, ka Pakalpojumu ņēmēja pakalpojumu sniegšana var tikt atjaunota pēc nopietna incidenta minimālajā SLA noteiktajā darbības atjaunošanas termiņā. Tas cita starpā var ietvert: * rezerves daļas[[2]](#footnote-2); * rezervi; * rezerves personālu, lai nodrošinātu, ka vienmēr tiek uzturētas svarīgākās funkcijas. * Pakalpojumu sniedzējam darbības nepārtrauktības nodrošināšanas plānā ir jāņem vērā tā atkarība no apakšuzņēmējiem. * Pakalpojumu sniedzējam jāpārskata savs pakalpojumu nepārtrauktības nodrošināšanas plāns, ņemot vērā agrākos incidentus un agrāko pieredzi, un, ja nepieciešams, tas jāpārstrādā. * Ja to pieprasa Pakalpojumu ņēmējs, Pakalpojuma sniedzējs var piedalīties Pakalpojumu ņēmēja organizētās mācībās, lai sagatavotu to potenciāliem nopietniem darbības traucējumiem (vētrām, lielām dabas katastrofām, atsevišķiem būtiska tīkla aprīkojuma darbības traucējumiem u.tml.) |

**2.7. Monitorings, revīzija un testēšana**

**SO21: Monitorings un reģistrēšanas process**

|  |
| --- |
| ***Drošības riski*** |
| Neatklātas nestandarta situācijas, vīrusi vai ļaunprātīgas darbības neefektīva datu plūsmas vai iekārtu darbības monitoringa dēļ. |
| ***Drošības prasības*** |
| * Pakalpojumu sniedzējam jāveic regulārs monitorings visu nestandarta situāciju atklāšanai, kas var norādīt uz jautājumiem, kas saistīti ar Pakalpojumu ņēmēja tīkla un sistēmas pieejamību vai integritāti. * Pakalpojumu sniedzējam jāizmeklē visas nestandarta situācijas. * Par visām nestandarta situācijām nekavējoties jāziņo Pakalpojumu ņēmējam (atsauce uz SO18). |

**SO23: Tīkla un informācijas sistēmu testēšana**

|  |
| --- |
| ***Drošības riski*** |
| Neadekvāta, neefektīva un nepietiekama testēšana, kas izraisa Pakalpojumu sniedzējs produktu un pakalpojumu vājās vietas, disfunkciju vai citas kļūmes. |
| ***Drošības prasības*** |
| * Pirms to integrēšanas Pakalpojumu ņēmēja sistēmā Pakalpojumu sniedzējam atbilstoši līgumā noteiktajām specifikācijām ir jānovērtē produkta kvalitāte un drošība. Pakalpojumu ņēmējs var noteikt dažus pieņemšanas kritērijus, un produkta vai aprīkojuma pieņemšana var tikt atteikta, ja tie neatbilst Pakalpojumu ņēmēja skaidri līgumā noteiktām prasībām. Kārtība ir spēkā attiecībā uz jaunām komponentēm, programmu izmaiņām un atjauninājumiem. * Pakalpojumu sniedzējam jāveic attiecīgas pārbaudes, lai nodrošinātu regulāru, precīzu un efektīvu testēšanu un sniegtu garantiju, ka tā produkti un pakalpojumi darbojas kā nākas: * testēšana jāveic visā produkta/pakalpojuma dzīves ciklā: izstrādes stadijā, pirms un pēc tā integrēšanas tīklā un kad tiek veiktas izmaiņas vai atjauninājumi; * testēšana jāveic ar pareizo konfigurāciju – testa vidē, simulējot reālās konfigurācijas (vai aizvietotāju), ja iespējams; * testēšana jāveic ar iterāciju, lai, kur tas nepieciešams, pārdevējs varētu veikt kļūdu labojumus; * ir jāveic vairāki testēšanas veidi, tais skaitā (bet ne tikai) zināmu vājo vietu skenēšana, aizsardzības pret nesankcionētu piekļuvi testēšana, izejas koda analīze u.c. * Testēšanu var veikt Pakalpojuma sniedzējs, Pakalpojumu ņēmējs, trešā persona un/vai kopēja ekspertu komanda (ar Pakalpojumu ņēmēja un Pakalpojumu sniedzēja testētājiem). Ir jāvienojas un līgumā jānosaka puses, kas atbild par testēšanu. * Par testēšanas biežumu ir jāvienojas, un tas jānosaka līgumā. * Testēšanas plāni un metodoloģijas ir regulāri jāpārskata, ņemot vērā tehnoloģiskās izmaiņas, uzlabojumus un agrākos incidentus. * Pakalpojumu sniedzējam ir jāsagatavo vispārējs testēšanas pārskats, kurā jāparedz testēšanas kārtība, identificētās vājās vietas, visas nepieciešamās trūkumu novēršanas darbības un skaidra ārkārtas situāciju seku novēršanas kārtība situāciju risināšanai nākotnē. |

**SO24: Drošības novērtējums**

|  |
| --- |
| ***Drošības riski*** |
| Nepietiekama informācija par produktu vai sistēmu potenciālajām vājajām vietām pirms ārpakalpojumu Pakalpojumu sniedzēja vai piegādātāja izvēles.  Vājas preventīvās darbības iepriekš minētā novēršanai. |
| ***Drošības prasības*** |
| * Pirms nodibināt saistības Pakalpojumu sniedzējam jāsniedz Pakalpojuma ņēmējam dokumentācija par zināmajām produktu vai sistēmu vājajām vietām līdz ar to svarīgumu un varbūtību, ka tās tiks pakļautas riskam. * Pakalpojumu sniedzējam jāievieš process, lai nekavējoties paziņotu Pakalpojumu ņēmējam par visām jaunatklātajām un izpētāmajām vājajām vietām (atsauce uz SO18). * Pakalpojumu sniedzējam jāņem vērā aktuālie draudi un periodiski jāpārskata nozarē pastāvošie trauksmes signāli/standarti, lai izvērtētu visas iespējamās jaunās vājās vietas. |

**SO25: Atbilstības monitorings**

|  |
| --- |
| ***Drošības riski*** |
| Nevar gūt pārliecību par Pakalpojumu sniedzēja atbilstību drošības prasībām un nevar nodrošināt, ka Pakalpojuma ņēmējs pareizi pārvalda drošības riskus. Piemēram:   * nav kontroles pasākumu; * esošās kontroles nav saskaņotas ar Pakalpojumu ņēmēja mērķiem; * nobīdes no plānotajiem kontroles pasākumiem. |
| ***Drošības prasības*** |
| * Ir jāorganizē regulāras Pakalpojumu sniedzējs un Pakalpojumu ņēmēja tikšanās, lai novērtētu Pakalpojumu sniedzēja sniegumu drošības prasību piemērošanā. * Pakalpojumu sniedzējam jāapliecina, ka drošības riski tiek pārvaldīti un prasības tiek ievērotas, un jādarbojas atbilstoši ar Pakalpojuma ņēmēju noslēgtajam līgumam. Pusēm jāvienojas par apliecinājumu izpildes pārskata saturu, metodoloģiju un biežumu. Apliecinājumiem var izmantojot vairākas metodes: * Pakalpojuma sniedzējs var sniegt pārskatu par drošības statusu, riskiem, vājajām vietām un incidentiem (kā daļu no pārskata par pakalpojumiem). * Pakalpojuma sniedzējs var pieprasīt regulārus neatkarīgus tā pakalpojumu vai darba procesu un izmantojamo tehnoloģiju pārskatus, un pārskatus izsniedzamus Pakalpojumu ņēmējam ar rezultātiem un identificētajām koriģējošajām darbībām. Lūdzam ņemt vērā, ka šis pasākums Pakalpojumu sniedzējam ir dārgs, tāpēc parasti tas tiek piemērots, izvērtējot katru gadījumu atsevišķi. * Pakalpojumu ņēmējam var būt tiesības veikt Pakalpojumu sniedzējs tam sniegto pakalpojumu vai darba procesu auditu vai pārskatu, tajā skaitā attiecībā uz aprīkojumu, programmatūru, informāciju, ierakstus, datus vai ar tiem saistītām personām. To, ja nepieciešams, var veikt trešā persona. Lūdzam ņemt vērā, ka šis pasākums Pakalpojumu ņēmējam ir dārgs, tāpēc parasti tas tiek piemērots, izvērtējot katru gadījumu atsevišķi. * Par apliecinājumu var kalpot sertifikāti (piem., ISO 27001). |

3. pielikums

iepirkuma procedūras uzaicinājumam

“ Sekundārā datu centra telpu noma”

iepirkuma identifikācijas Nr. VK/2015/12

**Tehniskā specifikācija**

1. **Vispārējas prasības Datu centra pakalpojuma nodrošināšanai**
   1. Pasūtītājam ir tehniskie resursi (serveri, disku masīvi, datu rezerves kopēšanas iekārtas, ugunsmūri, slodzes balansētāji, komutatori, u.c.), uz kuriem Pasūtītājs izmitinās un darbinās informācijas sistēmas. Pasūtītājs vēlas savus tehniskos resursus izvietot specializētā datu centrā, kas atbilst Tehniskās specifikācijas visām prasībām (turpmāk – Datu centra pakalpojumi).
   2. Datu centra pakalpojumu ietvaros Izpildītājam jānodrošina iespēja Pasūtītājam:
      1. datu centrā nodrošināt serveru statni (*(42U), dimensions (HxDxW) 200.4 x 101.5 x 59.7 cm*), vai piedāvāt labāku (platāku) statni šeit minēto Pasūtītāja tehnisko resursu izvietošanai;
      2. saņemt specifikācijā prasīto, ar iespēju palielināt vai samazināt, garantētā datu kanāla pieslēguma ātrumu līdz Pasūtītāja ugunsmūrim;
      3. piegādāt elektrobarošanas jaudu ne mazāku par 10 kW (ar iespēju palielināt līdz 20 kW) uz statni pie pilna statnes aizpildījuma.
   3. Izpildītājs nodrošina Datu centra pakalpojumus atbilstoši Tehniskās specifikācijas prasībām, vienlaicīgi ievērojot un nodrošinot:
      1. Ministru kabineta 2012. gada 19. jūnija noteikumu Nr.421 „Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības” prasību izpildi.
2. **Prasības datu centra fiziskai aizsardzībai**

|  |  |
| --- | --- |
| **Pozīcija** | **Specifikācija un piezīmes** |
| * 1. Fiziskā drošība | * + 1. Fiziski nodalīta telpa, kuras perimetrs (sienas, griesti, grīda) nav ēkas ārējais perimetrs vai nepieguļ ēkas daļai, kurai pieeju nekontrolē pretendents. Telpai nedrīkst būt logi.     2. Telpai ir jābūt izvietotai ēkā tā, lai iekšēja avārija citā ēkas daļā (piemēram, ūdensvada, kanalizācijas vai apkures sistēmas cauruļu avārija) pēc iespējas mazāk ietekmētu serveru telpu. Telpai ir jābūt izbūvētai tā, lai ūdens ēkas iekšpusē varētu bez traucējumiem aizplūst, neappludinot serveru telpā izvietoto aprīkojumu. Starpstāvu pārsegums virs serveru telpas nepieļauj telpas applūšanas iespēju ugunsgrēka dzēšanas laikā.     3. Telpa aprīkota ar kustības detektoriem un trauksmes signālu automātiska nosūtīšana;     4. Tiek nodrošināta autonoma videonovērošana, kas ļauj identificēt telpā ienākošās un izejošās personas;     5. Statnes abas durvis ir aprīkotas ar mehāniskajām atslēgām un durvju atvēršanas sensoriem, kas pieslēgti pie centralizētās monitoringa sistēmas. Ir jānodrošina, ka statni var atvērt un iekļūt tajā tikai atslēdzot un atverot minētās durvis. Pēc Pasūtītāja pieprasījuma ir jābūt iespējai nomainīt statnes durvju atslēgas ar unikālu tikai Pasūtītājam pieejamu atslēgu.     6. Pieejas kontroles sistēma nodrošina pieeju datu centram tikai tiem Izpildītāja darbiniekiem, kuriem darba pienākumu izpildei nepieciešama fiziska piekļuve sistēmu infrastruktūrai;     7. Trešās personas, kurām nepieciešama piekļuve sistēmas apkalpošanai, telpās drīkst uzturēties tikai kopā ar 2.1.6. apakšpunktā minētajām personām.     8. Tiek nodrošināts speciāls apmeklētāju reģistrācijas žurnāls.     9. Ēkā, kurā atrodas telpa, un tas pieguļošās teritorijās ir nodrošināta diennakts fiziskā apsardze (vismaz viens apsardzes darbinieks). |
| * 1. Ugunsdrošība | * + 1. Telpas sienām un durvīm ir jānodrošina vismaz 30 minūšu uguns aizsardzība (E30 ugunsdrošības klase).     2. Telpā, kur tiek izvietoti Pasūtītāja resursi, tiek nodrošināta automātiska ugunsdzēšana, izmantojot automātiskās gāzes ugunsdzēsības sistēmas;     3. Ugunsgrēka gadījumā klimata nodrošināšanas sistēmai automātiski jābloķē gaisa pieplūdes un aizvadīšanas kanālus; pēc ugunsgrēka klimata sistēma nodrošina degšanas produktu izvadīšanu pa aizvadīšanas kanālu |
| * 1. Mikroklimats (statnē) | * + 1. Datu centram ir jānodrošina telpas klimata kontroli, kura nepārtraukti uztur serveru darbībai nepieciešamo optimālo temperatūru 18ºC-28ºC (statnes „aukstajā” zonā pie priekšējām durvīm) un relatīvais gaisa mitrums 35% - 60%; |
| * 1. Piekļuve | * + 1. Izpildītājs nodrošina Pasūtītāja pilnvarotām personām iespēju piekļūt datu centrā izvietotām iekārtām profilaktisko vai avārijas atjaunošanas darbu veikšanai 24h diennaktī darba dienās, kā arī brīvdienās un svētku dienās. |
| * 1. Atrašanās vieta | * + 1. Datu centri atrodas Rīgas pilsētas administratīvās teritorijas robežās ne tuvāk kā 5 km viens no otra. |
| * 1. Pierakstu uzglabāšana | * + 1. Elektronisko atslēgu, trauksmes signalizācijas, videonovērošanas, apmeklētāju reģistrācijas u.c. žurnāliem ir jābūt pieejamiem pēc Pasūtītāja pieprasījuma 3 gadus no ieraksta brīža. |

1. **Optisko šķiedru nomas pakalpojuma apraksts**

Pakalpojumu sniedzējs ierīko un iznomā Pasūtītājam fiziskās optiskās šķiedras optiskās šķiedras kabelī optiskajā līnijā atbilstoši sekojošiem tehniskajiem parametriem:

* 1. optiskā līnija tiks nodrošināta bez jebkāda veida aktīvās aparatūras, pakešu vai kadru komutācijas, optiskās vai jebkāda cita veida multipleksēšanas palīdzības;
  2. vienmodu 9/125 (single mode) optiskās šķiedras kabeļi atbilst ITU-T rekomendācijām;
  3. darba frekvences viļņa garums ir robežās λ=1310 nm – 1550 nm;
  4. optisko šķiedru vājinājums 20°C temperatūrā nepārsniedz sekojošos rādītājus:
     1. 0,5 dB/km pie viļņa garuma 1310 nm;
     2. 0,3 dB/km pie viļņa garuma 1550 nm.
  5. visi nepieciešamie optisko šķiedru metinājumi tiek veikti ar optisko šķiedru metināšanas tehnoloģiju;
  6. savienojot optiskās šķiedras tiek ievēroti ražotāja noteikto krāsu gammas atbilstoši standartam IEC 304;
  7. kabeļu instalācija ēkās, telpās tiek veikta saskaņā ar Elektronisko sakaru likumu, būvniecību regulējošiem normatīvajiem dokumentiem un materiālu ražotāja noteikto tehnisko specifikāciju un prasībām.

1. **Optikas savienojuma specifikācija:**

|  |  |
| --- | --- |
| **Pozīcija** | **Specifikācija un piezīmes** |
| * 1. Vispārīgi | Pakalpojuma ietvaros nepieciešams 2 optikas šķiedru savienojums starp Pasūtītāja primāro un sekundāro datu centru. Datu pārraides kanālu veidojošās iekārtas nodrošinās Pasūtītājs. |
| * 1. Pieejamība | Optikas škiedru savienojumam tiek nodrošināta pieejamība 99% mēnesī. |
| * 1. Statņu savienojumi Datu centra iekšpusē | Izpildītājam jānodrošina vienmodu/daudzmodu optiskā šķiedra un/vai Cat5/Cat6 komunikāciju, savienojums starp serveru statnēs izvietotajiem Pasūtītāja komutatoriem izveidošana un pievadīšana,  Visiem kabeļu savienojumiem jābūt marķētiem; |

1. **Prasības elektroenerģijas pieslēgumam**

|  |  |
| --- | --- |
| **Pozīcija** | **Specifikācija un piezīmes** |
| * 1. Prasības pieslēgumam | * + 1. Dublēts elektroenerģijas pievads Datu centrā(ēkā);     2. Katrs elektroenerģijas pievads ēkai tiek nodrošināts no savstarpēji neatkarīgiem transformatoriem. |
| * 1. Spriegums | * + 1. Stabilizēts (ar UPS iekārtām) un nepārtraukts (ar dīzeļģeneratora iekārtu) spriegums, kas tiek padots uz katras aparatūras statnes divām neatkarīgām elektrobarošanas kontaktu grupām (PDU);     2. Darba spriegums – 230V uz katru statnes barošanas paneļa (Power Distribution Unit) ligzdām;     3. Statņu energoapgādes shēma ir aizsargāta ar pārsprieguma novadītājiem. |
| * 1. Prasības rezervēšanai | * + 1. Pielietots nepārtrauktas barošanas risinājums (UPS), kas nodrošina elektrobarošanu visām Pasūtītāja iekārtām vismaz 30 minūtes no elektrobarošanas pieslēguma pārtraukuma iestāšanās brīža, pie pilnas datu centra maksimālās slodzes;     2. Dīzeļģenerators, kas automātiski uzsāk darbību ne ilgāk kā pēc 1 minūtes no elektroenerģijas zuduma brīža uz viena no pievadiem, kas caur pieslēgšanas iekārtām (ARI) savienots pie viena vai abiem elektrobarošanas pievadiem. |
| * 1. Uzskaite un norēķini | * + 1. Tiek nodrošināta iespēja veikt uzskaiti un norēķinu par patērēto elektroenerģiju gan ar datu centra maksā iekļautu patēriņa limitu vienai statnei gan atbilstoši skaitītāja rādījumiem un elektroenerģijas piegādātāja spēkā esošajiem tarifiem, par kuru izmaiņām Pakalpojumu sniedzējs informē Pasūtītāju vismaz 30 dienas iepriekš visā pakalpojuma sniegšanas periodā. |

1. **Prasības Datu centra pakalpojuma pieejamībai un atbildība**
   1. Apraksts. Datu centra pakalpojumiem jābūt pieejamiem un darbspējīgiem vismaz 99,90% mēnesī, neskaitot plānotās nepieejamības, par kurām Izpildītājs Pasūtītāju informē un saskaņo vismaz 5 darba dienas iepriekš.
   2. Definīcija. Datu centra pakalpojuma pieejamība – parametrs, kas procentos raksturo Datu centra pakalpojamu pieejamību (t.sk. novirzes no Datu centra pakalpojuma tehniskajiem un kvalitātes rādītājiem, atbilstoši Datu centra pakalpojumu pieejamības uzraudzības (monitoringa) sistēmas mērījumiem) apskatāmā laika periodā, kas ir vienāds ar kalendāro mēnesi. Datu centra pakalpojuma pieejamība tiek aprēķināta:

, kur

P – pakalpojuma pieejamība, procentos;

T – laiks, kurā pakalpojums netiek saņemts, min;

– kopējais pakalpojuma sniegšanas laiks, min.;

* 1. Parametra mērījumi un kontrole. Izmantojot Izpildītāja Datu centra pakalpojumu pieejamības uzraudzības (monitoringa) sistēmu (skat. 6.punktu), ar kuru iespējams kontrolēt Datu centra pakalpojuma kvalitāti un pieejamību.
  2. Bojājumu novēršana. Izpildītājs veic iespējamo bojājumu proaktīvu uzraudzību (uzraudzību nepārtraukti veic Izpildītāja tehniskais dienests). Atklājot bojājumu, Izpildītājs to iespējami īsā laikā novērš. Izpildītājs tehnisko atbalstu nodrošina 365 dienas gadā. Par bojājumu tiek uzskatītas arī novirzes no Datu centra pakalpojuma tehniskajiem un kvalitātes rādītājiem, kas tiešā veidā iespaido Pasūtītāja izvietotās aparatūras nodrošināšanai nepieciešamos parametrus atbilstoši Datu centra pakalpojumu pieejamības uzraudzības (monitoringa) sistēmas mērījumiem.
  3. Maksimālais laiks pilnīgai bojājuma novēršanai: 43 (četrdesmit trīs) minūšu laikā darba no attiecīgās problēmas konstatācijas vai reģistrācijas brīža.
  4. Atbildība. Pasūtītājam ir tiesības prasīt līgumsoda samaksu šādā apmērā un gadījumos:

*Tabula* 1*. Laiks virs bojājuma novēršanas limita pārsniegšanas līgumsods*

|  |  |
| --- | --- |
| **Laiks virs bojājuma novēršanas limita** | **Līgumsods** |
| Līdz 8(astoņām) stundām | 20% no mēneša maksas |
| Virs 8 (astoņām) stundām | 50% no mēneša maksas |

1. **Prasības pakalpojuma uzraudzības un pārvaldības nodrošinājumam**.
   1. Lai nodrošinātu Datu centra pakalpojuma uzraudzības, kvalitātes kontroli un Pasūtītāja atbalsta funkcijas, Izpildītājam jānodrošina Datu centra pakalpojuma uzraudzības un pārvaldības organizatoriskā struktūra (tehniskais dienests) un centralizēta infrastruktūras monitoringa sistēma, kuras ietvaros var nodrošināt Pasūtītāja personāla attālināta pieslēguma iespējas pie šīs sistēmas, lai nodrošinātu iespēju Pasūtītājam veikt infrastruktūras parametru kontroli.
   2. Izpildītāja uzraudzības un pārvaldības dienestam jānodrošina sekojošu funkciju izpildi:
      1. darbības režīmu 24 (divdesmit četras) stundas dienā un 7 (septiņas) dienas nedēļā;
      2. problēmu pieteikumu saņemšanu, reģistrāciju un izpildes atsekošanu.
   3. Izpildītājam jānodrošina Pasūtītāja atbildīgajām personām piekļuve (24 (divdesmit četras) stundas dienā un 7 (septiņas) dienas nedēļā), izmantojot WEB saskarni, Izpildītāja Datu centra pakalpojumu pieejamības uzraudzības (monitoringa) sistēmai, ar kuru iespējams kontrolēt Datu centra pakalpojuma kvalitāti un pieejamību.
   4. Datu centra pakalpojumu pieejamības uzraudzības (monitoringa) sistēmai jānodrošina vismaz šādu kvalitatīvo parametru uzraudzība:
      1. temperatūras un relatīvā gaisa mitruma parametri statnes „aukstajā” zonā;
      2. elektrobarošanas pieejamība un kvalitātes parametri uz aparatūras statnes barošanas kontaktiem (Power Distribution Unit jeb PDU);
      3. aparatūras statnes durvju (priekšās un aizmugures) atvēršanas laikus.
   5. Datu centra pakalpojumu pieejamības uzraudzības (monitoringa) sistēmai jānodrošina šī pielikuma 6.4. punktā minēto parametru datu uzkrāšanu un grafisku attēlošanu par periodu ne mazāku kā 6 (seši) kalendārie mēneši un jānodrošina periodisku (ne biežāk kā reizi mēnesī) atskaišu sagatavošanu par kvalitātes parametru nodrošināšanu.

4.pielikums

iepirkuma procedūras uzaicinājumam

“ Sekundārā datu centra telpu noma”

iepirkuma identifikācijas Nr. VK/2015/12

**Finanšu piedāvājums**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr.p.k. | Pakalpojums | Vienību skaits | Vienības cena EUR, bez PVN | Cena kopā EUR, bez PVN |
| 1. | Iekārtu izvietošana 1. statnei, 1 mēnesis. | 1x36 |  |  |
| 2. | Optikas šķiedras noma Smilšu 1(admin lit 4), Rīgā *Datu centrs* | 1x36 |  |  |
| **Paredzamā līgumcena kopā** | | | |  |

Pretendenta uzņēmuma vadītājs vai vadītāja pilnvarota persona:

|  |  |
| --- | --- |
| **Vārds, uzvārds, amats** |  |
| **Paraksts un zīmogs** |  |
| **Datums** |  |

5.pielikums

iepirkuma procedūras uzaicinājumam

“ Sekundārā datu centra telpu noma”

iepirkuma identifikācijas Nr. VK/2015/12

Apakšuzņēmēju saraksts[[3]](#footnote-3)

|  |  |  |
| --- | --- | --- |
| Apakšuzņēmēja nosaukums | Reģistrācijas numurs | Pakalpojuma daļa, kuru plānots nodot attiecīgajam apakšuzņēmējam (% no pakalpojuma vērtības) |
| 1. |  |  |
| 2. |  |  |

**Personu, uz kuru iespējām pretendents balstās, saraksts**

|  |  |  |
| --- | --- | --- |
| Personas nosaukums | Reģistrācijas numurs | Norāde uz iepirkuma nolikuma vai tehniskās specifikācijas prasību, kuras atbilstību nodrošina |
| 1. |  |  |
| 2. |  |  |

Pretendenta uzņēmuma vadītājs vai vadītāja pilnvarota persona:

|  |  |
| --- | --- |
| **Vārds, uzvārds, amats** |  |
| **Paraksts un zīmogs** |  |
| **Datums** |  |

6. pielikums

iepirkuma procedūras uzaicinājumam

“ Sekundārā datu centra telpu noma”

iepirkuma identifikācijas Nr. VK/2015/12

**Pretendenta pieredzes apraksts**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr.p.k. | Informācijas sistēma | Informācijas sistēmas pārzinis vai turētājs | Laika periods, kurā nodrošināta IS izmitināšana datu centrā | Pasūtītāja kontaktpersona līguma izpildes jautājumos |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| ... |  |  |  |  |

Ar šo apliecinām, ka:

1. pārskatā norādītajām informācijas sistēmām esam snieguši datu centra pakalpojumus vienlaikus nodrošinot šo informācijas sistēmu un tās infrastruktūras ar augstām pieejamības prasībām (pieejamība nav zemāka par 99,90%) izmitināšanu.
2. Minētajā periodā vienlaicīga šo informācijas sistēmu un to infrastruktūras ar augstām pieejamības prasībām (pieejamība nav zemāka par neplānoto dīkstāvju kopsummu 43 minūtes summāri mēnesī) izmitināšana ir tikusi nodrošināta nepārtraukti ne mazāk 12 mēnešus.
3. Pārskatā sniegtā informācija ***ir/ nav***uzskatāma par komercnoslēpumu.

Pretendenta uzņēmuma vadītājs vai vadītāja pilnvarota persona:

|  |  |
| --- | --- |
| **Vārds, uzvārds, amats** |  |
| **Paraksts un zīmogs** |  |
| **Datums** |  |

7.pielikums

iepirkuma procedūras uzaicinājumam

“ Sekundārā datu centra telpu noma”

iepirkuma identifikācijas Nr. VK/2015/12

**Apliecinājums izpildīt uzaicinājuma tehniskajā specifikācijā noteiktās prasības**

Ar šo apliecinām, ka pakalpojumu sniegsim atbilstoši iepirkuma tehniskajā specifikācijā noteiktajam.

Pretendenta uzņēmuma vadītājs vai vadītāja pilnvarota persona:

|  |  |
| --- | --- |
| **Vārds, uzvārds, amats** |  |
| **Paraksts un zīmogs** |  |
| **Datums** |  |

1. 5 Dublikāts pazaudētas vai bojātas iekārtas detaļas nomaiņai. [↑](#footnote-ref-1)
2. Dublikāts pazaudētas vai bojātas iekārtas detaļas nomaiņai. [↑](#footnote-ref-2)
3. Pretendents norāda visus apakšuzņēmējus saskaņā ar Publisko iepirkumu likuma 20.panta otro un sesto daļu, kuriem, slēdzot vienošanos, sniedzamo pakalpojumu vērtība ir 20 procenti no kopējās vienošanās vērtības vai lielāka.

   Apakšuzņēmēja veicamo sniedzamo pakalpojumu kopējo vērtību noteic saskaņā ar Publisko iepirkumu likuma 20.panta piekto daļu - ņemot vērā apakšuzņēmēja un visu attiecīgā iepirkuma ietvaros tā saistīto uzņēmumu sniedzamo pakalpojumu vērtību. Par saistīto uzņēmumu uzskata kapitālsabiedrību, kurā saskaņā ar Koncernu likumu apakšuzņēmējam ir izšķirošā ietekme vai kurai ir izšķirošā ietekme apakšuzņēmējā, vai kapitālsabiedrību, kurā izšķirošā ietekme ir citai kapitālsabiedrībai, kam vienlaikus ir izšķirošā ietekme attiecīgajā apakšuzņēmējā. [↑](#footnote-ref-3)