

**Līgums par ārējā drošības dokumentācijas audita
un ielaušanās testu veikšanu
(SPRK 2017/260)**

Pasūtītāja līguma Nr.43/2017
Izpildītāja līguma Nr. A2017/10/07

Rīgā,

2017.gada 10.novembrī

Sabiedrisko pakalpojumu regulēšanas komisija (reģ. Nr. 90001162258), turpmāk tekstā – Pasūtītājs, kuras vārdā saskaņā ar pilnvarojumu rīkojas izpilddirektors Jānis Miķelsons no vienas puses, un

sabiedrība ar ierobežotu atbildību “Analytica” (reģ. Nr. 40003823267), turpmāk tekstā – Izpildītājs, tās valdes locekļa Jura Pūces personā, kurš rīkojas uz statūtu pamata, no otras puses, Pasūtītājs un Izpildītājs kopā saukti – Puses, saskaņā ar Pasūtītāja iepirkuma procedūras "Ārējs drošības dokumentācijas audits un ielaušanās testu veikšana" (ID Nr. SPRK2017/260), turpmāk tekstā – Iepirkums, rezultātiem, noslēdz šādu līgumu, turpmāk tekstā – Līgums:

1. Līgumā lietotie termini, definīcijas un līguma iztulkošana

1.1. Termini un definīcijas:

- 1.1.1. Līgums – šis Līgums, tā pielikumi un papildinājumi;
- 1.1.2. Pielikumi – šī Līguma pielikumi;
- 1.1.3. Trešās personas – visas personas, kas nav uzskatāmas par Pusēm;
- 1.1.4. Tehniskā specifikācija – Līguma 1.pielikumā pievienotā Iepirkuma tehniskā specifikācija;
- 1.1.5. Tehniskais piedāvājums – Izpildītāja Iepirkumā iesniegtais Tehniskais piedāvājums, kas pievienots šī Līguma 2.pielikumā;
- 1.1.6. Finanšu piedāvājums – Izpildītāja Iepirkumā iesniegtais Finanšu piedāvājums, kas pievienots šī Līguma 3.pielikumā;
- 1.1.7. Kalendārais grafiks - Izpildītāja Līguma izpildes kalendārais grafiks, kas pievienots šī Līguma 4.pielikumā;
- 1.1.8. Audita starpziņojums – Līguma 2.1.1.-2.1.9.apakšpunktā minētie Izpildītāja audita starpziņojumi, kas sagatvoti un iesniegti saskaņā ar Kalendāro grafiku;
- 1.1.9. Audita gala ziņojums – Līguma 2.1.10.punktā minētais Izpildītāja audita gala ziņojums, kas sagatvots un ieniegts saskaņā ar Kalendāro grafiku.

1.2. Līguma iztulkošana:

- 1.2.1. Minēto terminu skaidrojumi šī Līguma tekstā var tikt lietoti gan daudzskaitlī, gan vienskaitlī (atkarībā no konteksta), neizslēdzot iespēju, ka termins, kas Līgumā ir lietots vienskaitlī, var nozīmēt daudzskaitli un otrādi. Līguma teksta interpretāciju nevar balstīt uz tekstā lietoto terminu skaitli.

- 1.2.2. Līguma punktu numerācija un nodaļu nosaukumi tiek lietoti ērtības labad un nevar tikt izmantoti Līguma interpretācijas nolūkos.
- 1.2.3. Līgumā var tikt lietoti vispārāztīti informācijas tehnoloģiju nozares termini (vārdi) angļu valodā. Termini angļu valodā tiek rakstīti iekavās aiz skaidrojuma latviešu valodas vārda vai vārdu kopas un to lietojuma mērķis ir precizēt pirms tiem lietotā latviešu valodas vārda vai vārdu kopas nozīmi.

2. Līguma priekšmets

- 2.1. Pasūtītājs uzdod, bet Izpildītājs apņemas saskaņā ar šo Līgumu, ne vēlāk, kā līdz 2018.gada 15.janvārim (ieskaitot), veikt Pasūtītāja ārējo drošības dokumentācijas auditu un ielaušanās testus (turpmāk – Darbi), kas sevī ietver:
 - 2.1.1. Informācijas drošības novērtēšanu atbilstoši ISO/IEC 27001:2013 standarta kontrolēm un atbilstoša audita starpziņojuma sagatavošanu;
 - 2.1.2. Sociālās inženierijas testu veikšanu un drošības novērtēšanu un atbilstoša audita starpziņojuma sagatavošanu;
 - 2.1.3. Lietotāju darbstaciju satura pārbaūžu veikšanu un atbilstoša audita starpziņojuma sagatavošanu;
 - 2.1.4. Fiziskās drošības novērtēšanu un atbilstoša audita starpziņojuma sagatavošanu;
 - 2.1.5. Drošības, veiktspējas un pieejamības novērtēšanu Komersantu informācijas ievades un apstrādes sistēmai (IIAS) un atbilstoša audita starpziņojuma sagatavošanu;
 - 2.1.6. Drošības, veiktspējas un pieejamības novērtēšanu Starpsavienojumu datu bāzei (STARS) un atbilstoša audita starpziņojuma sagatavošanu;
 - 2.1.7. Drošības, veiktspējas un pieejamības novērtēšanu Elektroniskai dokumentu uzskaites sistēmai (EDUS) un atbilstoša audita starpziņojuma sagatavošanu;
 - 2.1.8. Drošības, veiktspējas un pieejamības novērtēšana grāmatvedības un peronālvadības sistēmai (Ozols) un atbilstoša audita starpziņojuma sagatavošanu;
 - 2.1.9. Drošības, veiktspējas un pieejamības novērtēšanu Sabiedrisko pakalpojumu regulēšanas komisijas failu glabātuves sistēmai un atbilstoša audita starpziņojuma sagatavošanu;
 - 2.1.10. Kopējo IT infrastruktūras komponentu drošības novērtēšanu un atbilstoša audita gala ziņojuma sagatavošanu.
- 2.2. Pasūtītājs pieņem un apņemas samaksāt Izpildītājam par savlaicīgi un kvalitatīvi saņemtajiem Darbiem, saskaņā ar šī Līguma nosacījumiem.

3. Darbu pasūtīšanas un sniegšanas kārtība

- 3.1. Līgums stājas spēkā 2017.gada 15.novembrī un ir spēkā līdz Pušu saistību pilnīgai izpildei, ja Līgums nav izbeigts Pusēm vienojoties vai, Līgumā noteiktajos gadījumos, vienpusējā kārtā.
- 3.2. Izpildītājs apņemas Darbus veikt kvalitatīvi, ievērojot šādus Darbu izpildes termiņus:
 - 3.2.1. Darbu uzsākšana – Izpildītājs uzsāk Darbus nākamajā kalendārajā dienā pēc Līguma spēkā stāšanās dienas, tos veicot saskaņā ar Kalendāro grafiku;
 - 3.2.2. Darbu pabeigšana – Izpildītājs pabeidz Darbus Kalendārajā grafikā noteiktajā termiņā, bet ne vēlāk kā līdz 2018.gada 15.janvārim.

- 3.3. Izpildītājs Līguma 2.1.1. - 2.1.9.punktā minētos Darbus veic pa etapiem saskaņā ar Kalendāro grafiku, un pēc katra Darbu izpildes etapa pabeigšanas iesniedz Pasūtītājam audita starpziņojumu.
- 3.4. Pasūtītājs 5 (piecu) darba dienu laikā pēc Kalendārā grafikā noteiktā attiecīgā Darbu izpildes etapa pabeigšanas un Līguma 3.3.punktā minētā audita starpziņojuma saņemšanas veic pārbaudi, pārliecinoties par veikto Darbu atbilstību Līgumā izvirzītajām prasībām. Pārbaudes rezultātā Pasūtītājs vai nu rakstveidā akceptē attiecīgā Darba etapu, vai iesniedz Izpildītājam motivētu rakstveida atteikumu akceptēt attiecīgo Darba etapu.
- 3.5. Izpildītājs pēc visu Līguma 2.1.punktā minēto Darbu veikšanas sagatavo Līguma 2.1.10.punktā minēto audita gala ziņojumu un iesniedz to Pasūtītājam akceptēšanai.
- 3.6. Pasūtītājs 10 (desmit) darba dienu laikā pēc visu Līgumā noteikto Darbu pabeigšanas un Darbu pieņemšanas – nodošanas akta saņemšanas no Izpildītāja pārbauda veikto Darbu atbilstību Līgumā un Līguma pielikumos noteiktajiem nosacījumiem.
- 3.7. Pasūtītājs bez saskaņošanas ar Izpildītāju var iesaistīt Darbu pieņemšanas-nodošanas procesā, tai skaitā Darbu apstiprināšanas procesā, trešās personas.
- 3.8. Ja Izpildītāja veiktie Darbi atbilst Līgumā noteiktajiem nosacījumiem, Puses paraksta Darbu pieņemšanas – nodošanas aktu, ar kuru tiek apstiprināta visu Līguma 2.1.punktā minēto Darbu izpilde.
- 3.9. Ja Darbu pieņemšanas - nodošanas procedūras izpildes gaitā ir konstatēta veikto Darbu neatbilstība Līgumā noteiktajam, Darbi netiek uzskatīti par izpildītiem atbilstoši Līguma noteikumiem un Pasūtītājs rakstveidā informē Izpildītāju par atteikumu pieņemt Darbus, norādot konstatētos trūkumus un norādot trūkumu novēršanas termiņu. Pēc minēto trūkumu novēršanas Darbu pieņemšana – nodošana notiek Līguma 3.6.punktā noteiktajā kārtībā. Šajā punktā noteiktais trūkumu novēršanas termiņš neietekmē Pasūtītāja tiesības aprēķināt līgumsodu (nokavējuma procentus) par Izpildītāja saistību izpildes nokavējumu.
- 3.10. Izpildītājam ir pienākums patstāvīgi segt visas izmaksas, kas tam radušās saistībā ar trūkumu novēršanu, kas veicami saskaņā ar Pasūtītāja norādījumiem atbilstoši Līguma 3.9.punktā norādīto trūkumu novēršanai.

4. Pušu tiesības un pienākumi

- 4.1. Izpildītājs apņemas:
 - 4.1.1. ievērot Līguma noteikumus;
 - 4.1.2. sniegt Līguma 2.1.punktā minētos Darbus saskaņā ar Līguma nosacījumiem;
 - 4.1.3. izpildot Darbus, ievērot un nodrošināt atbilstību Līgumam un Latvijas Republikas un Eiropas Savienības normatīvo aktu prasībām, kas noteic ārējā drošības dokumentācijas audita un ielaušanās testu veikšanu;
 - 4.1.4. uzskatīt par konfidenciālu jebkuru Līguma ietvaros saņemto informāciju. Izpildītājs apņemas minēto dokumentāciju bez iepriekšējas rakstiskas Pasūtītāja piekrišanas nublicēt un nenodot trešajām personām, izņemot nodošanu tiesībsargājošajām vai valsts pārvaldes iestādēm normatīvajos aktos noteiktajos gadījumos un kārtībā;
 - 4.1.5. nenodot Līguma izpildi trešajām personām, bez Pasūtītāja rakstiskas piekrišanas;
 - 4.1.6. Darbu izpildē iesaistīt tikai kompetentas, atbilstošu izglītību un kvalifikāciju ieguvušas personas un Izpildītājs ir pilnībā atbildīgs pret Pasūtītāju par to personu darba kvalitāti, kas iesaistītas Darbu izpildē.
- 4.2. Izpildītāja tiesības:

- 4.2.1. saņemt no Pasūtītāja samaksu par atbilstoši Līguma nosacījumiem izpildītajiem Darbiem saskaņā ar Līguma nosacījumiem;
- 4.2.2. savlaicīgi saņemt no Pasūtītāja visu informāciju, kas nepieciešama Līgumā paredzēto Darbu izpildei.
- 4.3. Pasūtītājs apņemas:
 - 4.3.1. ievērot Līguma noteikumus;
 - 4.3.2. iespēju robežās nodrošināt Izpildītāju ar visu nepieciešamo un Izpildītāja pieprasīto informāciju, dokumentiem un organizatorisko atbalstu, kas nepieciešams Līguma kvalitatīvai izpildei;
 - 4.3.3. pieņemt kavalitāvi veiktus Darbus un veikt samaksu par savlaicīgi un kvalitatīvi izpildītajiem Darbiem šajā Līgumā noteiktajos termiņos un kārtībā;
 - 4.3.4. Līgumā noteiktajā kārtībā parakstīt attiecīgo Darbu pieņemšanas - nodošanas aktu.
- 4.4. Pasūtītāja tiesības:
 - 4.4.1. saņemt Līguma 2.1.punktā minētos Darbus saskaņā ar Līguma noteikumiem;
 - 4.4.2. pieprasīt no Izpildītāja informāciju par Līguma izpildes gaitu;
 - 4.4.3. pieaicināt trešās personas Līguma izpildes kontrolei;
 - 4.4.4. Līgumā noteiktajos gadījumos rakstiski sniegt Izpildītājam motivētu atteikumu Darbu pieņemšanai Līgumā noteiktajā kārtībā;
 - 4.4.5. saskaņā ar Līguma noteikumiem piemērot Izpildītājam līgumsodu par Darbu neizpildi vai nekvalitatīvu izpildi.
- 4.5. Puses apņemas nekavējoties rakstiski informēt viena otru par jebkādam grūtībām Līguma izpildes procesā, kas varētu aizkavēt savlaicīgu Darbu un Līguma izpildi.
- 4.6. Izpildītāja personālu, kuru tas iesaistījis Līguma izpildē, par kuru sniedzis informāciju Pasūtītājam un kura kvalifikācijas atbilstību izvirzītajām prasībām Pasūtītājs ir vērtējis un atzinis par atbilstošiem, pēc Līguma noslēgšanas drīkst nomainīt tikai ar Pasūtītāja rakstveida piekrišanu, ievērojot Publisko iepirkumu likuma 68.pantā paredzētos nosacījumus.

5. Līguma cena un norēķinu kārtība

- 5.1. Puses vienojas, ka kopējā Līguma cena par visiem Līguma 2.1.punktā minētajiem un saskaņā ar Līguma noteikumiem veiktajiem Darbiem ir EUR 17545,00 (septiņpadsmit tūkstoši pieci simti četrdesmit pieci *euro*, 0 centi), tajā skaitā pievienotās vērtības nodoklis 21% apmērā EUR 3045,00 (trīs tūkstoši četrdesmit pieci *euro*, 0 centi), turpmāk tekstā – Līgumcena.
- 5.2. Līgumcenā ietverti visi nodokļi un nodevas, kā arī visi iespējamie Izpildītāja izdevumi, kas nepieciešami Līgumā noteikto saistību izpildei. Līgumcena neietver maksājumus, kas radušies par Līgumā noteikto saistību neizpildi vai nepienācīgu izpildi.
- 5.3. Pasūtītājs samaksu par Izpildītāja izpildītajiem un apstiprinātajiem Darbiem veic dienas, 10 (desmit) darba dienu laikā no Izpildītāja rēķina saņemšanas un Darbu pieņemšanas-nodošanas akta abpusējas parakstīšanas dienas, pārskaitot rēķinā norādīto summu uz Izpildītāja norādīto bankas norēķina kontu. Rēķins ir uzskatāms par saņemtu nākamajā darba dienā pēc tā nosūtīšanas uz Pasūtītāja e-pastu: sprk@sprk.gov.lv.

- 5.4. Visi norēķini, kas saistīti ar Līguma izpildi, tiek veikti bezskaidras naudas norēķinu veidā, pārskaitot naudu uz attiecīgās Puses rēķinā norādīto bankas kontu. Par samaksas brīdi tiek uzskatīta diena, kad Puse ir pārskaitījusi naudu uz otras Puses norādīto bankas kontu.
- 5.5. Pasūtītājs veic apmaksu tikai par tiem Darbiem, kurus Izpildītājs ir izpildījis Līgumā noteiktajā kārtībā, apjomā un kvalitātē.

6. Līguma grozīšana un izbeigšana

- 6.1. Visas izmaiņas Līgumā izdarāmas rakstveidā un apliecināmas tādā pašā kārtībā kā Līgums. Līguma grozījumi ir veicami, ievērojot Publisko iepirkumu likuma 61.pantā paredzēto kārtību un nosacījumus. Līguma grozījumi stājas spēkā tikai tad, kad tie ir noformēti rakstiski un tos ir parakstījuši katra Puse.
- 6.2. Pasūtītājs ir tiesīgs vienpusēji izbeigt Līgumu, nosūtot Izpildītājam rakstisku paziņojumu vismaz 10 (desmit) darba dienas iepriekš, ja iestājas kaut viens no turpmāk minētajiem apstākļiem:
 - 6.2.1. ir stājies spēkā tiesas spriedums par Izpildītāja atzīšanu par maksātnespējīgu;
 - 6.2.2. pret Izpildītāju tikušas vērstas tiesiskas darbības, kas saistītas ar aresta uzlikšanu vairāk kā 50% (piecdesmit procenti) no Izpildītāja bilances aktīviem;
 - 6.2.3. ja Izpildītājs ir nokavējis jebkuru no Līgumā vai tā pielikumos noteikto Darbu sniegšanas termiņu un ja Izpildītāja nokavējums ir sasniedzis vismaz 10 (desmit) kalendārās dienas;
 - 6.2.4. ja Pasūtītājs atkārtoti konstatē Izpildīto Darbu neatbilstību Līguma prasībām vai Izpildītājs saskaņotajos termiņos nenovērš konstatētos Darbu trūkumus;
 - 6.2.5. ja Izpildītājs nepilda citas no šī Līguma izrietošas saistības, un, ja Izpildītājs minēto saistību neizpildi nav novērsis 10 (desmit) kalendāro dienu laikā pēc Pasūtītāja rakstiska paziņojuma par šādu saistību neizpildi saņemšanas;
 - 6.2.6. ja Pasūtītājs un Izpildītājs 10 (desmit) kalendāro dienu laikā nespēj vienoties par veicamo Darbu apjomu un uzsākšanas termiņu.
- 6.3. Gadījumā, ja Puses izbeidz šo Līgumu pirms tā izpildes, Puses sastāda aktu, ar kuru tiek fiksētas uz šī Līguma izbeigšanas brīdi Izpildītāja izpildītie un Līgumā noteiktā kārtībā pieņemtie Darbi. Pasūtītājs veic norēķinu ar Izpildītāju par saskaņā ar šo aktu pieņemtajiem Darbiem. Pasūtītājs ir tiesīgs ieturēt nokavējuma procentus no Izpildītājam iazmaksājamās summas.
- 6.4. Ja Pasūtītājs izbeidz Līgumu 6.3.punkta apakšpunktos minētajos gadījumos, Pasūtītājam nav jāatlīdzina Izpildītājam nekādi zaudējumi, kas Izpildītājam radušies ar Līguma izbeigšanu.

7. Pušu atbildība

- 7.1. Par Līgumā noteiktajā termiņā neizpildītiem vai nekvalitatīvi veiktiem Darbiem, Izpildītājs maksā līgumsodu Pasūtītājam 0,5% (piecas desmitās daļas procenta) apmērā par katru nokavēto kalendāro dienu, bet ne vairāk kā 10% (desmit procenti) apmērā no Līgumcenas, kas noteikta Līguma 5.1.punktā.
- 7.2. Ja Pasūtītājs neveic samaksu par Izpildītāja savlaicīgi un kvalitatīvi sniegtajiem Darbiem Līgumā noteiktajos termiņos, tad Pasūtītājs maksā Izpildītājam līgumsodu 0,5% (piecas desmitās daļas procenta) apmērā no termiņā nesamaksātās summas par katru nokavējuma kalendāro dienu, taču ne vairāk par 10% (desmit procenti) no kopējās termiņā nesamaksātās summas apmēra.

- 7.3. Puses atbild par sakarā ar šī Līguma neizpildi vai nepienācīgu izpildi otrai Pusei vai trešajām personām nodarītajiem zaudējumiem saskaņā ar Latvijas normatīvajiem aktiem.
- 7.4. Puses vienojas, ka Pasūtītājs saskaņā ar Līgumu pienākošos līgumsodu ir tiesīgs atskaitīt no Izpildītājam saskaņā ar Līgumu izmaksājamās Līgumcenas.
- 7.5. Līgumsoda samaksa neatbrīvo Puses no saistību pilnīgas un kvalitatīvas izpildes, kā arī zaudējumu atlīdzības pienākuma.

8. Strīdu risināšanas kārtība

- 8.1. Puses ir savstarpēji atbildīgas par otrai Pusei nodarītajiem zaudējumiem, ja tie radušies vienas Puses vai tā darbinieku, kā arī Līguma izpildē iesaistīto trešo personu rīcības (darbības vai bezdarbības), tostarp arī rupjas neuzmanības, ļaunā nolūkā izdarīto darbību vai nolaidības rezultātā.
- 8.2. Jebkurš strīds, domstarpība vai prasība, kas izriet no šī Līguma, kas skar to vai tā pārkāpšanu, izbeigšanu vai spēkā esamību, un kuru Puses nevar atrisināt sarunu ceļā, tiek izšķirta saskaņā ar Latvijas Republikas spēkā esošajiem normatīvajiem aktiem vispārējās jurisdikcijas tiesā.
- 8.3. Ja šis Līgums nenosaka ar Līguma izpildi saistītus noteikumus, Puses saistību izpildē vadās no Latvijas Republikas spēkā esošajiem normatīvajiem aktiem.

9. Nepārvarama vara

- 9.1. Puses tiek atbrīvotas no atbildības par Līguma pilnīgu vai daļēju neizpildi, ja šāda neizpilde radusies nepārvaramas varas vai ārkārtēja rakstura apstākļu rezultātā, kuru darbība sākusies pēc Līguma noslēgšanas un kurus nevarēja iepriekš paredzēt, ne novērst. Pie nepārvaramas varas vai ārkārtēja rakstura apstākļiem pieskaitāmi: stihiskas nelaimes, avārijas, katastrofas, epidēmijas, kara darbība, blokādes, varas un pārvaldes institūciju rīcība, normatīvu aktu, kas būtiski ierobežo un aizskar Pušu tiesības un ietekmē uzņemtās saistības, pieņemšana un stāšanās spēkā.
- 9.2. Pusei, kas atsaucas uz nepārvaramas varas vai ārkārtēja rakstura apstākļu darbību, nekavējoties, bet ne vēlāk kā 3 (trīs) darba dienu laikā, par šādiem apstākļiem rakstveidā jāziņo otrai Pusei, veic visus iespējamus pasākumus, lai nepieļautu zaudējumu rašanos un vienojas par Līguma saistību izpildi. Ziņojumā norāda, kādā termiņā pēc viņa ieskata ir iespējama un paredzama viņa Līgumā paredzēto saistību izpilde, un, pēc pieprasījuma, šādam ziņojumam ir jāpievieno izziņa, kuru izsniegusi kompetenta institūcija un kura satur ārkārtējo apstākļu darbības apstiprinājumu un to raksturojumu.
- 9.3. Neapanākot vienošanos par Līguma saistību izpildi nepārvaramās varas gadījumā, ikviena no Pusēm ir tiesīga vienus pusēji pārtraukt Līguma izpildi, nosūtot otrai Pusei rakstisku paziņojumu vismaz 10 (desmit) darba dienas iepriekš.

10. Ierobežotas pieejamības informācija

- 10.1. Jebkura informācija (materiālā un nemateriālā formā), ko Darbu izpildes laikā Izpildītājs ir saņēmis no Pasūtītāja, tiek uzskatīta par ierobežotas pieejamības, un tās izpaušana trešajām personām bez Pasūtītāja rakstiskas piekrišanas ir aizliegta.
- 10.2. Pirms Līguma parakstīšanas Izpildītājs ir iepazinies ar normatīvo aktu prasībām par ierobežotas pieejamības informāciju, komercnoslēpumu, par informāciju, kurai normatīvajos aktos paredzēta īpaša izmantošanas kārtība un izplatīšanas liegums, kā arī personu vai institūciju loku, kurām tiesību aktos ir noteiktas tiesības šādu informāciju pieprasīt vai saņemt.

- 10.3. Ja Izpildītāja vainas dēļ, ierobežotas pieejamības informācijas, kuru Pasūtītājs sniedz Izpildītājam Darba izpildei pretlikumīgās izpaušanas rezultātā Pasūtītājam vai trešajām personām tiks nodarīti tieši zaudējumi, vai Izpildītājs izmantojis informāciju iedzīvošanās nolūkā vai to izpaudis par maksu, viņš mantiski atbild tiesību aktos noteiktā kārtībā un apmērā.
- 10.4. Pasūtītāja informācijas izpaušana netiks uzskatīta par Līguma noteikumu pārkāpumu tikai un vienīgi sekojošos gadījumos:
- 10.4.1. attiecīgā informācija tiek izpausta pēc tam, kad tā kļuvusi publiski zināma vai pieejama neatkarīgi no Pusēm;
- 10.4.2. informācija tiek izpausta tiesību aktos noteiktajos gadījumos, apjomā un kārtībā.
- 10.5. Šī Līguma 10.punkta noteikumi ir spēkā arī pēc Līguma termiņa beigām, kā arī pēc pirmstermiņa līgumattiecību pārtraukšanas līdz brīdim, kad tie tiek atcelti.

11. Citi noteikumi

- 11.1. Pasūtītāja kontaktpersona ar Līguma izpildi saistītos jautājumos (izņemot dokumentu parakstīšanu) ir _____.
- 11.2. Izpildītāja kontaktpersona ir _____.
- 11.3. Mainoties Līgumā norādītajai informācijai par kādu no Pusēm (adrese, tālrunis, bankas rekvizīti utt.), attiecīgā Puse ne vēlāk kā 5 (piecu) darba dienu laikā pēc izmaiņu veikšanas rakstiski par to paziņo otrai Pusei. Par zaudējumiem, kas Pusēm var rasties saistībā ar šo izmaiņu nesavlaicīgu un nepienācīgu paziņošanu pilnā apmērā, atbild vainīgā Puse.
- 11.4. Šis Līgums ir saistošs Pušu darbiniekiem un juridiskajiem tiesību pārņēmējiem.
- 11.5. Līgums ir sagatavots 2 (divos) eksemplāros uz 21 (divdesmit vienas) lapas 1 (vienam) eksemplāram katrai no Pusēm.

12. Pušu rekvizīti un paraksti:

Pasūtītājs:

Sabiedrisko pakalpojumu regulēšanas komisija

Reģ.Nr.90001162258

Ūnijas iela 45, Rīga, LV-1045

Valsts kase

Konts: LV09TREL2120640005000

Kods: TREL22

izpilddirektors

Izpildītājs:

SIA „Analytica”

Reģ.Nr. 40003823267

Elijas iela 17-8, Rīga, LV-1050

Luminor bank AS

Konts: LV37RIKO0002013294482

Kods: RIKOLV2X

valdes loceklis

/Jānis Miķelsons/

/Juris Pūce /

TEHNISKĀ SPECIFIKĀCIJA **iepirkumam Nr. SPRK 2017/260**

“Ārējs drošības dokumentācijas audits un ielaušanās testu veikšana”

I. Vispārējais apraksts

1. Sabiedrisko pakalpojumu regulēšanas komisijas (turpmāk - Regulators) informācijas sistēmas nodrošina Regulatora ikdienas darbu. IT drošības audita ietvaros ir jāveic Regulatora informācijas un informācijas sistēmu drošības pārbaudes atbilstoši šajā tehniskajā specifikācijā noteiktajām prasībām, kas ietver:
 - 1.1. informācijas drošības politikas un ar to saistošās dokumentācijas, un ārēju un iekšējo normatīvo dokumentu izvērtēšanu, atbilstoši LR normatīvajiem aktiem un IT jomu reglamentējošiem dokumentiem, tai skaitā ISO/IEC 27001:2013 standartam;
 - 1.2. tehnisko resursu fiziskās drošības pārbaudes un sociālās inženierijas testus un drošības novērtēšanu, kā arī Regulatora darbinieku darbstaciju satura pārbaudes (darbi tiek veikti attiecinot tos uz Regulatoru kopumā, nevis konkrētu informācijas sistēmu);
 - 1.3. informācijas sistēmu drošības, pieejamības un veiktspējas testēšanu un novērtēšanu;
 - 1.4. kopējo IT infrastruktūras komponentu drošības novērtēšanu (darbi tiek veikti attiecinot tos uz Regulatoru kopumā, nevis konkrētu informācijas sistēmu).

II. Auditējamo sistēmu un IT infrastruktūras komponentu apraksts

2. Pamatdarbības informācijas sistēmas:

- 2.1. **IIAS jeb Komersanta informācijas ievades un apstrādes sistēma** ir Regulatora izstrādāta un pārziņā esoša sistēma, ar kuras starpniecību regulējamie sabiedrisko pakalpojumu sniedzēji (turpmāk – komersanti) Regulatoram elektroniski iesniedz normatīvajos aktos noteikto informāciju - atskaites un dokumentus. Sistēmas mērķis ir komersantu datu ievade, uzkrāšana, apstrāde un analīze, nodrošinot iespēju drošā veidā komersantiem iesniegt visas nepieciešamās veidlapas elektroniski un komunicēt ar Regulatoru, izmantojot sistēmā ievietotus ziņojumus;
- 2.2. **STARS jeb Starpsavienojumu datu bāze** ir izstrādāta, lai uzkrātu informāciju par komersantu savstarpēji noslēgtajiem starpsavienojumu līgumiem un nodrošinātu to analīzi pēc dažādiem parametriem. Reģistrējamie dati ir: noslēgšanas datums, spēkā stāšanās datums, starpsavienojuma izveides parametri, starpsavienojuma savstarpējie tarifi u.c.;
- 2.3. **EDUS jeb elektroniskās dokumentu uzskaites sistēmas** mērķis ir nodrošināt informācijas uzglabāšanu un apriti Regulatorā (dokumentu uzglabāšanu, sistematizēšanu, datu apkopošanu, dokumentu vizēšanu un parakstīšanu, informāciju par Regulatora darbinieku prombūtni u.c.);
- 2.4. **OZOLS jeb grāmatvedības un personālvadības sistēma** nodrošina Regulatora finanšu un grāmatvedības informācijas uzskaiti, apstrādi un uzturēšanu, kā arī ar personāla vadību saistītas informācijas uzskaiti, uzturēšanu un apstrādi;
- 2.5. **Regulatora failu glabātuves sistēma** ir failu glabāšanas un pārvaldības serveris iekšējām Regulatora darbības nodrošināšanas vajadzībām;

2.6. Kopējās IT infrastruktūras komponentes:

- 2.6.1. Virtualizācijas vide;
- 2.6.2. Ugunsmūris;
- 2.6.3. Lokālais datortīkls (tai skaitā bezvadu tīkls);
- 2.6.4. Aktīvā direktorija.

III. IT drošības audita darbi drošības pārvaldības ietvaros

3. **Regulatora informācijas drošības novērtējums atbilstoši ISO/IEC 27001:2013 standartam:** IT drošības audita ietvaros jāveic kopējs Regulatora informācijas drošības novērtējums atbilstoši ISO/IEC 27001:2013 standarta kontrolēm.
4. **Sociālās inženierijas testi un drošības novērtējums:**
 - 4.1. IT drošības audita ietvaros jāveic sociālās inženierijas testi, kā arī kopējais drošības novērtējums attiecībā uz sociālās inženierijas uzbrukumiem;
 - 4.2. drošības novērtējums jābalsta uz attiecīgajām ISO/IEC 27001:2013 standarta kontrolēm un OSSTMM v3 drošības testēšanas rokasgrāmatas "Cilvēku drošības testēšanas" (*Human Security Testing*) kontrolēm.
5. **Lietotāju darbstaciju satura pārbaudes:**
 - 5.1. IT drošības audita ietvaros jāveic Regulatora darbinieku darba vietu datoru (tai skaitā "laptop" datoru) satura pārbaudes attiecībā uz datoros instalēto programmatūru un datoros esošo informāciju – jānosaka, vai datoros ir uzstādīta lietojumprogrammatūra, kas nav nepieciešama Regulatora darbinieka pienākumu pildīšanai, un datoros neatrodas datnes un faili, kas ievietoti Regulatora darbinieku personiskām vajadzībām (piemēram, video formāta faili, kas satur izklaides materiālu);
 - 5.2. par konkrētu pārbaudāmo programmatūru un informācijas uzglabāšanas failu jāvienojas ar Pasūtītāju pirms skenēšanas pārbaūžu veikšanas.
6. **Fiziskās drošības novērtēšana:**
 - 6.1. jāveic Regulatora informācijas tehnoloģiju tehnisko resursu fiziskās drošības novērtējums. Fiziskās drošības novērtējums ietver vismaz pārbaudes datu pārraides līniju piekļuvēm, datu centra vai serveru telpai un tās piekļuvei, klimata uzturēšanas iekārtām, elektrības nepārtrauktās barošanas elementiem;
 - 6.2. fiziskās drošības novērtējums jābalsta uz attiecīgajām ISO/IEC 27001:2013 standarta kontrolēm.

IV. IT drošības audita darbi Regulatora informācijas sistēmu drošības un veiktspējas pārbaudei

7. **Sistēmas drošības novērtēšana:**
 - 7.1. **Drošības novērtēšana atbilstoši LR un Regulatora iekšējiem normatīvajiem aktiem:**
 - 7.1.1. **veicot sistēmas drošības novērtējumu, jāņem vērā šāds normatīvais regulējums:**
 - 7.1.1.1. Informācijas tehnoloģiju drošības likums;
 - 7.1.1.2. Fizisko personu datu aizsardzības likums;

- 7.1.1.3. Ministru kabineta 2015.gada 28.jūlija noteikumi Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām";
- 7.1.1.4. Regulatora iekšējie normatīvie akti;
- 7.1.1.5. citi IT jomu reglamentējoši normatīvie akti.
- 7.1.2. **Drošības novērtēšana atbilstoši ISO/IEC 27001:2013 standarta kontrolēm:**
 - 7.1.2.1. drošības novērtēšanas ietvaros jāveic sistēmas drošības pārbaude pret LVS ISO/IEC 27001:2013 standarta kontrolēm;
 - 7.1.2.2. nav atkārtoti jāvērtē tās ISO/IEC 27001:2013 standarta kontroles, kuras jau pārbaudītas šī IT drošības audita ietvaros un ir attiecināmas uz visu Regulatoru kopumā (piemēram, Regulatora kopējās informācijas drošības politikas dokumenta izvērtēšana) un nav viennozīmīgi attiecināmas tikai uz konkrēto sistēmu.
- 7.1.3. **Drošības novērtēšana atbilstoši OSSTMM v3 drošības testēšanas rokasgrāmatai:**
 - 7.1.3.1. drošības novērtēšanas ietvaros jāveic sistēmas drošības pārbaudes testi pret katru no OSSTMM v3 (Open Source Security Testing Methodology Manual) rokasgrāmatas drošības testiem jeb prasībām. Pārbaudes jāveic atbilstoši OSSTMM v3 rokasgrāmatas "Bezvadu drošības testu" kontrolēm un "Datu tīkla drošības testu" kontrolēm;
 - 7.1.3.2. nav atkārtoti jāvērtē tās OSSTMM v3 rokasgrāmatas kontroles, kuras jau pārbaudītas šī IT drošības audita ietvaros un ir attiecināmas uz visu Regulatoru kopumā (piemēram, Regulatora kopējās informācijas drošības politikas dokumenta izvērtēšana) un nav viennozīmīgi attiecināmas tikai uz konkrēto sistēmu.
- 7.1.4. **Drošības novērtēšana atbilstoši OWASP v4 "Testing guide" drošības testēšanas kontrolēm:**
 - 7.1.4.1. drošības novērtēšanas ietvaros jāveic sistēmas drošības pārbaudes testi pret katru no OWASP v4 (Open Web Application Security Project) *Testing guide* drošības testēšanas kontrolēm;
 - 7.1.4.2. novērtējumam jāiekļauj pārbaudes par OWASP v4 Testing guide kontroļu grupām:
 - 7.1.4.2.1. informācijas vākšana;
 - 7.1.4.2.2. konfigurācijas pārvaldības testēšana;
 - 7.1.4.2.3. identitātes pārvaldības testēšana;
 - 7.1.4.2.4. autentifikācijas testēšana;
 - 7.1.4.2.5. autorizācijas testēšana;
 - 7.1.4.2.6. sesiju pārvaldības testēšana;
 - 7.1.4.2.7. ievaddatu validācijas testēšana;
 - 7.1.4.2.8. kļūdu apstrāde;
 - 7.1.4.2.9. kriptogrāfija;
 - 7.1.4.2.10. biznesa loģikas testēšana;
 - 7.1.4.2.11. klienta puses testēšana.
- 7.1.5. **Sistēmas rezerves kopiju izveides un atjaunošanas procesa novērtēšana:**

7.1.5.1. IT drošības audita ietvaros jāveic sistēmas rezerves kopēšanas procesa un atjaunošanas plāna realizācija un pietiekamības novērtējums;

7.1.5.2. saskaņojot darbus ar Pasūtītāju, jāveic sistēmas rezerves kopijas sagatavošana un sistēmas darbības atjaunošana no iepriekš sagatavotās rezerves kopijas.

7.2. Sistēmas veiktspējas un pieejamības novērtēšana:

7.2.1. Sistēmas stresa testi:

7.2.1.1. sistēmas veiktspējas novērtēšanā jāveic informācijas sistēmas tehnisko resursu stresa testi un novērtējumi. Stresa testiem jāatspoguļo sistēmas tehnisko resursu noslodze atkarībā no vienlaicīgo sesiju (lietotāju) skaita. Stresa testu laikā atsevišķi ir jātestē informācijas sistēmas publiskā daļa (ja tāda ir), kā arī tā daļa, kas nav publiski pieejama, kopumā sniedzot vienotu skatu uz procesa norisi;

7.2.1.2. informācijas sistēmas stresa testu laikā plānotie iegūstamie tehnisko resursu noslodzes rādītāji ir iepriekš jāaskaņo ar Pasūtītāju.

7.2.2. **Atteices DoS uzbrukuma testi:** sistēmas veiktspējas un pieejamības novērtēšanā jāveic DoS uzbrukumi, mēģinot iztukšot sistēmas, datu pārraides resursus vai izmantot informācijas apstrādes nepilnības.

7.2.3. **Testu veikšanas laiks:** informācijas sistēmas veiktspējas un pieejamības testi ir jāveic diennakts laikā no plkst.22:00 līdz plkst.7:00. Ja testējamo sistēmu darbības neietekmē sistēmu ekspluatāciju, tad, vienojoties ar Pasūtītāju, šos testus var veikt no plkst.7:00 līdz plkst.22:00.

7.2.4. **Sistēmas uzbūves analīze attiecībā uz veiktspēju un pieejamību:** sistēmas veiktspējas novērtēšanas laikā veicama informācijas sistēmas pašreizējās arhitektūras analīze un priekšlikumu sniegšana informācijas sistēmu pieejamības paaugstināšanai plānoto tehnisko apkopju un/vai tās jauninājumu uzstādīšanas laikā, ņemot vērā, informācijas sistēmas pieejamības prasības, kas noteiktas konkrētajai sistēmai.

7.3. **IT drošības audita darbu aktivitāšu sadalījums pa informācijas sistēmām un infrastruktūras komponentēm:** Tabula Nr.1 satur matricu, kurā ar "X" norādītas veicamās aktivitātes drošības un veiktspējas novērtēšanā, kā arī sistēmas rezerves kopēšanas procesa un atjaunošanas procesa novērtēšanā:

Tabula Nr.1

IS un IT infrastruktūras komponentes	IT drošības audita ietvaros veicamās novērtēšanas aktivitātes					
	Normatīvā dokumentācija	ISO/IEC 27001: 2013	OSSTMM v3	OWASP v4	Rezerves kopijas un atjaunošanas process	Veiktspējas un pieejamība
IAS	X	X		X	X	X
Regulatora mājas lapa	X	X		X	X	X
STARS	X	X		X	X	X

IS un IT infrastruktūras komponentes	IT drošības audita ietvaros veicamās novērtēšanas aktivitātes					
	Normatīvā dokumentācija	ISO/IEC 27001: 2013	OSSTMM v3	OWASP v4	Rezerves kopijas un atjaunošanas process	Veiktspējas un pieejamība
EDUS	X	X		X	X	X
OZOLS	X	X		X	X	X
Regulatora failu glabātuves sistēma	X	X	X		X	X
Kopējās IT infrastruktūras komponentes	X	X	X		X	X

V. IT drošības audita rezultātu nodevumi

8. Izpildītājs pēc katras informācijas sistēmas vai kopējo IT infrastruktūras komponentu audita Pasūtītājam iesniedz audita ziņojumu saskaņā ar izpildītāja iesniegto kalendāro izpildes grafiku.
9. Izpildītājs iesniedz Pasūtītājam audita gala ziņojumu, kas ietver audita darbu ietvaros sagatavotos ziņojumus, un kurā pilnvērtīgi ir iekļauts un aprakstīts:
 - 9.1. IT drošības audita apjoms un ierobežojumi;
 - 9.2. testēšanas vides detalizēts apraksts, norādot sistēmas versijas un infrastruktūras parametrus;
 - 9.3. atklāto kļūdu un nepilnību vai ievainojamību novērojumu apraksts, izmantošanas veids un risku vērtējums, rekomendācijas drošības un veiktspējas līmeņa paaugstināšanai;
 - 9.4. veikto pārbažu rezultāti (protokoli), kuros uzrādītas veiktās pārbaudes, to novērojumi un būtiskāko novērojumu pierādījumi. Pierādījumu protokoli tiek gatavoti tā, lai kompetenta persona varētu atkārtot novērojumu.

Pasūtītājs:

Izpildītājs:

Sabiedrisko pakalpojumu regulēšanas komisija SIA “Analytica”

Sabiedrisko pakalpojumu regulēšanas komisijas izpilddirektors **Jānis Miķelsons**

SIA “Analytica” valdes loceklis **Juris Pūce**

