Kiberdrošības prasības

1. **Pielikumā tiek lietotie šādi termini un saīsinājumi.**
   1.1. **Informācijas sistēma** (turpmāk tekstā – IS), organizēta sistēma, kas paredzēta informācijas resursu pārvaldībai un elektroniskajai apstrādei, izmantojot tehniskos resursus.
   1.2. **Ievainojamība** — informācijas un komunikācijas tehnoloģiju vai to pakalpojumu vājums, uzņēmība pret tehniskām problēmām vai nepilnība, kas var tikt izmantota kiberapdraudējumam.
   1.3. **Kiberdrošības incidents** (turpmāk tekstā — kiberincidents) notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību.
   1.4. **Kiberdrošība** ir darbības, kas jāveic, lai aizsargātu tīklu un informācijas sistēmas, to lietotājus un citas personas, kuras skar kiberdraudi.
   1.5. **Kiberdraudi** ir jebkādi iespējami apstākļi, notikums vai darbība, kas varētu radīt bojājumus vai traucējumus vai citādi negatīvi ietekmēt tīklu un informācijas sistēmas, to lietotājus un citas personas.
2. **Droša saziņa un atbildību sadalījums.**
   2.1. Pasūtītājs, līguma darbības laikā, nodrošina Izpildītājam drošu un šifrētu datu pārraidi pie Pasūtītāja datu pārraides tīkla, Līdzējiem vienojoties par tehnoloģisko risinājumu.
   2.2. Jebkāda informācijas apmaiņa, kas var ietekmēt Pakalpojuma drošību, tiek veikta tikai ar šajā Līgumā norādītajām pilnvarotajām kontaktpersonām un izmantojot turpmāk minētos drošās saziņas kanālus, kas nodrošina informācijas konfidencialitāti, integritāti un pieejamību:
      2.2.1. Šifrēts e-pasts;
      2.2.2. Pasūtītāja noteikta ziņu apmaiņas (čats, tērzēšana) risinājums;
      2.2.3. Pasūtītāja noteikta pieteikumu apstrādes IS.
   2.3. Programmatūras koda vai tā daļas, un IS konfigurācijas informācija tiek piegādāta Līdzējiem vienojoties, izmantojot kādu no Pasūtītāja noteiktajiem informācijas apmaiņas veidiem – Pasūtītāja SFTP (*SSH File Transfer Protocol*), versiju kontroles sistēma (*Version Control System*) vai pieteikumu pārvaldības IS.
   2.4. Izpildītājs pirms programmatūras koda vai tā daļas piegādes veic koda drošības pārbaudi, balstoties uz *OWASP Secure Coding Practices* vai citiem pielīdzināmiem nozares labās prakses principiem.
   2.5. Izpildītājs ir atbildīgs par to, ka darbības Pasūtītāja IS tiek veiktas tikai tādā apjomā, lai nodrošinātu Līguma priekšmeta izpildi.
3. **Piekļuves tiesību kontrole un kontu pārvaldība.**
   3.1. Pasūtītājs, Līguma darbības laikā, savstarpēji saskaņotiem Izpildītāja pārstāvjiem Pasūtītāja IS izveido Lietotāja kontus uz noteiktu laika periodu, bet ne ilgāku par Līgumā noteikto Pakalpojuma sniegšanas termiņu, nodrošinot Izpildītājam pieeju Pasūtītāja valdījumā vai īpašumā esošai IS produkcijas, testa un/vai izstrādes videi.
   3.2. Izpildītājs nodrošina šādus kiberdrošības kontroles pasākumus lietotāju kontu pārvaldībai:
      3.2.1. Sākotnējās Lietotāja paroles nomaiņu vietnē https://parole.latvenergo.lv ne vēlāk kā 72 stundu laikā pēc saņemšanas;
      3.2.2. Turpmākās paroles maiņu saskaņā ar IS paroles maiņas iestatījumiem un drošības paziņojumiem;
      3.2.3. IS autentifikācijas datu drošu glabāšanu, neizpaušanu un konfidencialitāti.
   3.3. Ja Izpildītāja darbinieks, kuram ir izveidots Lietotāja konts, pārtrauc darba attiecības un/vai saistības ar Izpildītāju, Izpildītājs nekavējoties par to paziņo Pasūtītājam.
4. **Kiberdrošības atbilstība.**
   4.1. Izpildītājs pastāvīgi nodrošina Izpildītāja īpašumā, valdījumā, lietošanā esošus tehniskos un organizatoriskos pasākumus atbilstoši Latvijas Republikas Nacionālās kiberdrošības likumam un saistītajiem Ministru kabineta noteikumiem, pielietojot drošu IS konfigurāciju ieviešanu, aizsardzību pret ļaunatūrām, tīkla drošības pārvaldību, savlaicīgu atjauninājumu un ievainojamību pārvaldību, kā arī atbilstošu fiziskās un vides drošības pasākumu nodrošināšanu. Minētās kontroles tiek uzturētas visu Pakalpojuma sniegšanas laiku.
   4.2. Izpildītājs apņemas pielietot Pasūtītāja norādītu papildus kiberdrošības aizsardzības programmatūru un tās uzturēšanu Līguma saistību izpildes termiņā, ja tādu pieprasa uzstādīt Pasūtītājs. Programmatūras izmaksas sedz Pasūtītājs.
   4.3. Izpildītājs apņemas nodrošināt Pasūtītājam iespēju pastāvīgi uzraudzīt Izpildītājam nodotās informācijas, kiberdrošības pasākumu ievērošanu, pārbaudīt atbilstību spēkā esošajām kiberdrošības prasībām attiecībā uz informācijas apstrādi, pārvaldību, aizsardzību, kas uzticēta Izpildītājam. Šim nolūkam Pasūtītājam ir tiesības veikt auditus — gan patstāvīgi, gan ar trešās personas starpniecību — Izpildītāja telpās un jebkurā vietā, kur tiek sniegti Pakalpojumi, par to rakstiski paziņojot Izpildītājam vismaz 2 (divas) darba dienas iepriekš.

4.4. Audita process ietver, bet neaprobežojas ar attiecīgās dokumentācijas, fizisko un tehnisko drošības pasākumu, programmatūras un IS konfigurāciju pārbaudi, kā arī jebkādas informācijas iegūšanu, kas nepieciešama, lai novērtētu atbilstību Līgumam un spēkā esošajām kiberdrošības prasībām.

4.5. Izpildītājam ir pienākums sadarboties ar Pasūtītāju audita procesa veikšanas laikā.

5. Ievainojamību pārvaldība.

5.1. Izpildītājs nodrošina, ka sniegtajā Pakalpojumā nav drošības risku, kas iekļauti atbilstošajos un aktuālajos "OWASP Top 10", "OWASP Mobile Top 10", "OWASP API Security Top 10" sarakstos (www.owasp.org).

5.2. Ja ievainojamības reģistrētas CVE (Common Vulnerabilities and Exposures) datu bāzē[1] un novērtētas pēc CVSS v3.0 vai jaunākas versijas kritērijiem[2], tad Izpildītājs par saviem līdzekļiem tās novērš:

5.2.1. Kritiskas ietekmes ievainojamības - vēlākais 7 (septiņu) kalendāro dienu laikā;

5.2.2. Augstas ietekmes ievainojamības - vēlākais 14 (četrpadsmit) kalendāro dienu laikā;

5.2.3. Vidējas un zemas ietekmes ievainojamības - vēlākais 30 (trīsdesmit) kalendāro dienu laikā.

5.3. Izpildītājs par saviem līdzekļiem novērš Pasūtītāja konstatētās ievainojamības vai drošības riskus ne vēlāk kā 30 (trīsdesmit) kalendāro dienu laikā.

6. Drošības apmācības un izpratne.

6.1. Izpildītājs nodrošina, ka visas personas, kas iesaistītas Pakalpojuma nodrošināšanā, ir iepazinušās un ievēro kiberdrošības prasības, kas noteikts Līgumā.

6.2. Izpildītājs nodrošina regulāras apmācības par kiberdrošības labās prakses principiem, kiberhigiēnu, konfidenciālas informācijas aizsardzību un atbilstību piemērojamajām tiesiskajām un līgumiskajām prasībām kiberdrošības jomā.

7. Kiberincidentu vadība.

7.1. Izpildītājs nekavējoties informē Pasūtītāju pa e-pastu palidzibas.dienests@latvenergo.lv vai tālruni +371 67728888 par jebkādu kiberincidentu, tostarp, bet ne tikai, drošības pārkāpumu, konstatētām ievainojamībām, apdraudējumiem vai citām aizdomīgām aktivitātēm, kas var ietekmēt Pakalpojuma drošību, konfidencialitāti, integritāti vai pieejamību.

7.2. Kiberincidenta gadījumā Izpildītājs sniedz detalizētu informācija par kiberincidenta raksturu, apmēru un iespējamo ietekmi, kā arī par veiktajiem tūlītējiem aizsardzības pasākumiem tā seku mazināšanai.

7.3. Izpildītājs sadarbojas ar Pasūtītāju kiberincidentu izmeklēšanā, sniedzot visu nepieciešamo atbalstu, tostarp piekļuvi attiecīgajiem auditācijas pierakstiem, personālam, lai veicinātu kiberincidenta atrisināšanu normatīvos aktos noteiktajā kārtībā.

7.4. Izpildītājs nodrošina, ka visi ar kiberincidentu saistītie auditācijas pieraksti, drošības notikumi tiek droši glabāti vismaz 18 (astoņpadsmit) mēnešus no kiberincidenta vai notikuma dienas.

[1] https://cve.mitre.org
[2] https://nvd.nist.gov/vuln-metrics/cvss