IT DROŠĪBAS NOTEIKUMI

1. Pasūtītājs, līguma darbības laikā, nodrošina Izpildītājam drošu un šifrētu datu pārraidi pie Pasūtītāja datu pārraides tīkla, Līdzējiem vienojoties par tehnoloģisko risinājumu.
2. Informācijas apmaiņa, kas var ietekmēt Pakalpojuma drošību, tiek nodrošināta tikai ar Līgumā noteikto kontaktpersonu starpniecību, ievērojot informācijas apmaiņas veidu, kas nodrošina tās konfidencialitāti, integritāti un pieejamību:
   2.1. šifrēts e-pasts;
   2.2. Pasūtītāja ziņu apmaiņas (tērzēšanas) risinājums;
   2.3. Pasūtītāja pieteikumu apstrādes sistēma.
3. Programmatūras koda vai tā daļas, un informācijas sistēmas (turpmāk tekstā – "IS") konfigurācijas informāciju piegādā Līdzējiem vienojoties izmantot kādu no Pasūtītāja noteiktajiem informācijas apmaiņas veidiem – Pasūtītāja SFTP (SSH File Transfer Protocol), versiju kontroles sistēma (Version Control System) vai pieteikumu apstrādes sistēma.
4. Izpildītājs ir atbildīgs par savu darbinieku veiktajām darbībām, kas vērstas uz Pasūtītāja IT sistēmu drošības apiešanu vai bojāšanu.
5. Izpildītājs ir atbildīgs par to, ka darbības Pasūtītāja IS tiek veiktas tikai tādā apjomā, lai nodrošinātu Līguma priekšmeta izpildi.
6. 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.
7. Izpildītājam ir pienākums nodrošināt sekojošus Lietotāja konta aizsardzības pasākumus:
   7.1. sākotnējās Lietotāja paroles nomaiņu vietnē https://parole.latvenergo.lv ne vēlāk kā 72 stundu laikā pēc saņemšanas;
   7.2. drošu IS autentifikācijas datu glabāšanu un neizpaušanu.
8. Ja Izpildītāja darbinieks, kuram ir izveidots Lietotāja konts, pārtrauc darba attiecības un/vai saistības ar Izpildītāju, Izpildītājs nekavējoties par to paziņo Pasūtītājam.
9. Pielietojot Izpildītāja valdījumā esošus tehniskos vai programmatūras līdzekļus, Izpildītājs uzņemas atbildību par šo līdzekļu sastāvā ietilpstošo operētājsistēmu drošības atbilstību, pielieto atjauninātus pretvīrusu aizsardzības un ugunsmūra risinājumus, kā arī nodrošina adekvātas fiziskās drošības kontroles Pakalpojuma sniegšanas laikā.
10. Izpildītājs apņemas pielietot Pasūtītāja norādītu papildus IT drošības aizsardzības programmatūru un tās uzturēšanu Līguma saistību izpildes termiņā, ja tādu pieprasa uzstādīt Pasūtītājs. Programmatūras izmaksas sedz Pasūtītājs.
11. Izpildītājs apņemas nodrošināt Pasūtītājam iespēju pastāvīgi uzraudzīt Izpildītājam nodotās informācijas IT drošības pasākumu ievērošanu. Šai sakarā, Izpildītājs apņemas nodrošināt Pasūtītājam iespēju jebkurā laikā, ja tas par to informējis Izpildītāju vismaz 2 (divas) darba dienas iepriekš, Izpildītāja pārstāvja klātbūtnē pārbaudīt Izpildītāja darbību tā atrašanās vai Pakalpojumu sniegšanas vietā saistībā ar Pakalpojumu sniegšanu, tai skaitā, iepazīties ar dokumentiem, pielietotiem tehniskās un programmatūras līdzekļiem, kā arī pieprasīt no UZŅĒMĒJA informāciju, kas saistīta ar Pakalpojumu sniegšanu.
12. Izpildītājs pirms programmatūras koda vai tā daļas piegādes veic koda pārbaudi (code review).
13. Sniegtajā Pakalpojumā jābūt novērstām visām IT drošības ievainojamībām, kas ir starp "OWASP Top 10" (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project). Pasūtītājam konstatējot neatbilstības, Izpildītājs par saviem līdzekļiem tās novērš vēlākais 30 (trīsdesmit) kalendāro dienu laikā. Ja konstatētās ievainojamības ir reģistrētas CVE (Common Vulnerabilities and Exposures) datu bāzē (https://cve.mitre.org) un novērtētas pēc CVSS v3.0 vai jaunākas versijas kritērijiem (https://nvd.nist.gov/vuln-metrics/cvss), tad Izpildītājs tās novērš:
   13.1. Kritiskas ietekmes ievainojamības - vēlākais 7 (septiņu) kalendāro dienu laikā;
   13.2. Augstas ietekmes ievainojamības - vēlākais 14 (četrpadsmit) kalendāro dienu laikā;
   13.3. Vidējas un zemas ietekmes ievainojamības - vēlākais 30 (trīsdesmit) kalendāro dienu laikā.
14. Izpildītājam ir pienākums iepazīstināt darbiniekus un/vai Izpildītāja pārstāvjus, kas nodrošina Pakalpojuma izpildi, ar līguma pielikumu - IT drošības noteikumi.
15. Ja Izpildītājam ir aizdomas par drošības incidentu vai Līgumā minēto IS drošības noteikumu pārkāpumu, Izpildītājs nekavējoties informē par to Pasūtītāja kontaktpersonu vai Pasūtītāja Palīdzības dienestu, tālrunis: +371 67728888.