Paslaugų viešojo pirkimo–pardavimo sutarties specialiosios dalies

Priedas Nr. 7

**SUSITARIMAS DĖL TAIKOMŲ ORGANIZACINIŲ IR TECHNINIŲ**

**KIBERNETINIO SAUGUMO REIKALAVIMŲ**

Vykdydamas Prekių viešojo pirkimo–pardavimo sutartį (toliau – Sutartis), tiekėjas privalo užtikrinti tinkamą duomenų saugumo lygį, t. y. nuolatinį tvarkomų asmens duomenų konfidencialumą, vientisumą, prieinamumą ir duomenų tvarkymo IT sistemų atsparumą, ir, siekdamas šio tikslo, priimti tinkamus sprendimus dėl techninių ir organizacinių saugumo priemonių naudojimo. Jei tiekėjas aptarnauja kritinę informacinių ir ryšių technologijų (toliau – IRT) infrastruktūrą arba teikia kitas esmines Lietuvos Respublikos kibernetinio saugumo įstatymo 1 priede numatytas paslaugas Lietuvoje, jis laikosi Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, reikalavimų, taikomų kibernetinio saugumo esminiam subjektui. Jeigu tai užsienio tiekėjas, kuris jam perduotus duomenis tvarko ne Vilniaus universiteto ligoninės Santaros klinikų, Lietuvos sveikatos mokslų universiteto ligoninės Kauno klinikų, Klaipėdos universiteto ligoninės (toliau – Partnerių) IRT infrastruktūroje, turi būti laikomasi tarptautinių, pavyzdžiui, ISO/IEC 27001, standartų reikalavimų arba kitų lygiaverčių standartų (NIST CSF, SOC 2 ir pan.).

Tiekėjas įsipareigoja užtikrinti toliau išvardintų organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimą:

|  |  |
| --- | --- |
| 1. Organizacinės duomenų tvarkymo saugumo priemonės | * 1. Sudarius Sutartį, tiekėjo paskirti darbuotojai, kurie teiks paslaugas pagal šią Sutartį ir jungsis prie Partnerių IRT infrastruktūros, privalo susipažinti su informacinio ištekliaus valdytojo patvirtinta Kibernetinio saugumo politika ir ją įgyvendinančiais teisės aktais bei laikytis nustatytų reikalavimų. Tais atvejais, kai tiekėjui yra perduodama tvarkyti Partnerių duomenis savo (tiekėjo) infrastruktūroje, tiekėjui būtina vadovautis tiekėjo organizacijoje patvirtinta informacijos ir (ar) kibernetinio saugumo politika.   2. Visą Sutarties galiojimo laikotarpį ir po jo privaloma užtikrinti perduodamos, saugomos ar kitais būdais tvarkomos informacijos konfidencialumą, o iki pradedant tokią informaciją tvarkyti, būtina raštiškai įsipareigoti saugoti tokio pobūdžio informaciją.   3. Privaloma užtikrinti gautų prisijungimo duomenų saugumą ir neatskleisti jų trečiosioms šalims.   4. Naudotojų teises galima suteikti, keisti ir (ar) panaikinti laikantis principo „Būtina žinoti“ arba būtina užtikrinti, kad teisė prieiti prie informacijos būtų suteikta tik konkrečioms funkcijoms įvykdyti (darbui atlikti) ir (ar) konkrečiai apibrėžtam laikotarpiui.   5. Tiekėjas turi taikyti atitinkamas ir adekvačias teisių suteikimo ar pareigų atšaukimo, vaidmenų ir atsakomybių perdavimo ar perleidimo darbuotojo atleidimo bei jų funkcijų pasikeitimo atveju procedūras savo organizacijoje.   6. Tiekėjo darbuotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri apdorojama Partnerių IRT infrastruktūroje ar IS, negalėtų susipažinti pašaliniai asmenys. Visada būtina atsijungti nuo Partnerių IRT infrastruktūros ar IS ir papildomai įjungti ekrano užsklandą su slaptažodžio apsauga.   7. Tiekėjas turi užtikrinti, kad jo pasitelkti tiekėjai (subtiekėjai) atitiktų tuos pačius informacijos ir kibernetinio saugumo reikalavimus.   8. Tiekėjas turi nedelsiant informuoti Partnerius apie nutrūkusius darbo santykius su organizacijos darbuotoju, kuriam buvo suteikta prieiga prie Partnerių IRT infrastruktūroje tvarkomos informacijos.   9. Tiekėjo pareiga nedelsiant informuoti apie Sutarties vykdymo metu Partnerių IRT infrastruktūroje pastebėtus didelius ir (ar) kitus elektroninės informacijos saugos incidentus, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, informacijos saugumo reikalavimų nesilaikymą, nusikalstamos veikos požymius, aptiktas saugumo spragas (pažeidžiamumus), kurie kelia riziką kibernetinio saugumo subjekto tinklams ir informacinėms sistemoms, bei kitus svarbius saugai įvykius. Taip pat būtina informuoti Partnerius, bet ne vėliau kaip per 24 val., kai tiekėjo valdomoje informacinių sistemų infrastruktūroje buvo nustatyti minėti atvejai, kurie turi įtakos Partnerių tvarkomiems duomenims. Tiekėjas privalo Partneriams pateikti kibernetinio incidento tyrimo ataskaitą, kurioje būtų išdėstyta visa turima informacija bei duomenys, susiję su incidentu, kai tyrimas bus užbaigtas.   10. Tiekėjo pareiga sudaryti sąlygas kibernetinio saugumo subjektui arba jo įgaliotiems paslaugų teikėjams atlikti tiekėjo atitikties auditą (įskaitant neplaninį) Sutarties vykdymo laikotarpiu ar įvykus dideliam incidentui.   11. Būtina vykdyti sutartinius paslaugų teikimo įsipareigojimus (angl. *Service Level Agreement*, SLA).   Draudžiama:   * 1. skenuoti Partnerių IRT infrastruktūrą ar IS, ieškant pažeidžiamumų ar kitais būdais stebėti Partnerių IRT infrastruktūros ar IS duomenų srautą. Jeigu šiame punkte išvardintos priemonės yra reikalingos tiesioginėms funkcijoms atlikti, tai šias priemones galima naudoti tik suderinus su Partnerių saugos įgaliotiniu;   2. be atskiro Partnerių leidimo ir žinios jungtis prie Partnerių IRT infrastruktūros ar IS naudojant ar Partnerių išduotą įrangą (Partnerių svečiams skirtame belaidžiame tinkle);   3. gerti, valgyti ir rūkyti šalia informacijos apdorojimo įrangos Partnerių patalpose;   4. savavališkai keisti suteiktus tinklo parametrus (IP adresą ir pan.);   5. naudoti programas, kurios gali trikdyti Partnerių IRT infrastruktūros ar IS elektroninės informacijos prieinamumą;   6. savarankiškai keisti, remontuoti, taisyti Partnerių išduotą programinę ir techninę įrangą;   7. naudoti Partnerių išduotą programinę ir techninę įrangą Lietuvos Respublikos įstatymais draudžiamai veiklai, šmeižikiško, įžeidžiančio, grasinamojo pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujančiai veiklai, kompiuterių virusams kurti ir platinti, masinei piktybiškai informacijai siųsti ar kitiems tikslams, kurie gali pažeisti Partnerių ar kitų asmenų teisėtus interesus;   8. diegti, saugoti, naudoti, kopijuoti ar platinti nelegalią, autorines teises pažeidžiančią programinę įrangą. |
| 2. Techninės duomenų tvarkymo saugumo priemonės | 1. Turi būti įdiegta, įgyvendinta prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras. 2. Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas. 3. Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos. Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį. Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių, slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir pan.). Naudotojo slaptažodis turi būti ne trupesnis kaip 10 simbolių ir keičiamas ne rečiau kaip kas šešis mėnesius. Administratoriaus slaptažodis turi būti ne trumpesnis kaip 15 simbolių ir keičiamas ne rečiau kaip kas šešis mėnesius. Turi būti užtikrintas prisijungimo duomenų saugumas. Turi būti imtasi visų priemonių, kad prisijungimo vardai ir slaptažodžiai netaptų žinomi tretiesiems asmenims. 4. Kompiuterinėje darbo vietoje ar taikomojoje programinėje įrangoje slaptažodžių išsaugojimas turi būti draudžiamas. 5. Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio. 6. Vadovaujantis susitarimu, techninių žurnalų įrašai turi būti kuriami kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). Saugojimo terminas – ne trumpesnis kaip 3 mėnesiai. Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį. 7. Kompiuterinių darbo vietų, naudojamų duomenų tvarkymui pagal susitarimą, apsauga:    * 1. darbo vietų naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų;      2. naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotos programinės įrangos;      3. baigus darbą arba pasitraukiant iš darbo vietos, turi būti atsijungiama nuo tinklų ir informacinių sistemų, įjungiama ekrano užsklanda su slaptažodžiu;      4. kritiniai kompiuterinių darbo vietų operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant;      5. antivirusinės taikomosios programos ir jų informacijos apie virusus bei kenkimo programinę įrangą duomenų bazės turi būti atnaujinamos ne rečiau kaip kartą per parą;      6. kai prieiga prie naudojamų IT sistemų, susijusių su duomenų tvarkymu pagal susitarimą, yra vykdoma internetu, duomenys turi būti šifruojami taikant virtualaus privataus tinklo (VPN) technologiją su TLS / SSL sertifikatu arba naudojama privataus prieigos taško (angl. *Access Point Name*, APN) per mobiliojo ryšio operatorių technologija, taikant perduodamų duomenų šifravimą sraute su TLS / SSL sertifikatu, kai VPN technologija nėra palaikoma mobiliųjų įrenginių;      7. belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojams ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidis ryšys turi būti šifruojamas pagal gerąją saugumo praktiką rekomenduojamu šifravimo ilgio raktu. Būtina naudoti visuotinai saugiais pripažįstamus raktus ir protokolų versijas. Belaidės prieigos stotelėje turi būti pakeisti standartiniai gamintojo raktai;      8. mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti;      9. mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti. 8. Viešaisiais elektroninių ryšių tinklais perduodamos kibernetinio saugumo subjektui jautrios informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą bei turi būti apsaugota slaptažodžiais. 9. Mobiliųjų įrenginių laikmenose ir išorinėse kompiuterinėse laikmenose laikomi tinklų ir informacinių sistemų duomenys turi būti šifruojami. Duomenis būtina šifruoti kietojo disko lygiu. 10. Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jei to padaryti neįmanoma (pvz., USB, DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti, pvz., naudojant tam skirtus smulkintuvus arba kitas mechanines priemones. 11. Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos. |