..... (įmonės pavadinimas, kodas, toliau – Tiekėjas), įsipareigoja laikytis žemiau nurodytos Informacijos saugos politikos ir minimalių informacijos ir kibernetinio saugumo reikalavimų:

1. Taikymo sritis

Šie Vičiūnų grupė, UAB (toliau – Bendrovė) minimalūs informacijos ir kibernetinio saugumo reikalavimai (toliau – Reikalavimai) taikomi Tiekėjui vykdant Sutartį. Šie reikalavimai apima Bendrovės informacinių technologijų ir telekomunikacijų įrenginius ir mikroprocesorinius įrenginius, įskaitant, bet neapsiribojant, teleinformacijos surinkimo ir perdavimo įrenginius, automatikos terminalus, valdymo sistemas (HMI), momentinių duomenų valdiklius, bendros paskirties valdiklius, teleinformacijos surinkimo ir perdavimo sistemas, komercinių duomenų valdiklius, informacinių technologijų sistemas ir t.t. (toliau – Įranga), bei su įranga susijusias paslaugas.

2. Vartojamos sąvokos

2.1. „Būtina darbui“ – prieiga suteikiama tik prie minimalios ir atitinkamai veiklai, paslaugoms būtinos informacinės sistemos (infrastruktūros) ar jos dalies.

3. Atitikties reikalavimai

3.1.Priklausomai nuo prieigos prie informacinės sistemos (infrastruktūros) tipo gali būti taikomi papildomi techniniai ir organizaciniai reikalavimai nurodyti Lietuvos Respublikos kibernetinio saugumo įstatyme ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018-08-13 d. nutarimu Nr. 818 (aktuali redakcija).

4. Nuotolinio darbo saugumo reikalavimai

4.1. Įvertinus potencialias rizikas ir suteikus Tiekėjui galimybę dirbti nuotolinėje kompiuterizuotoje darbo vietoje priklausančioje Tiekėjui bei suteikus nuotolinę prieigą prie informacinių resursų Bendrovės informacinėse sistemose (infrastruktūroje) Tiekėjui būtina:

4.1.1. naudoti saugų VPN (angl. *Virtual Private Network*) ryšį;

4.1.2. įsitikinti, kad informacinės sistemos, kompiuterinė įranga ir duomenų tinklai iš kurių jungiamasi per nuotolį yra saugūs ir patikimi (atnaujinta operacinė sistema ir kita programinė įranga, įdiegta antivirusinė programinė įranga, įjungta ir sukonfigūruota ugniasienė ir t. t.);

4.1.3. užtikrinti savalaikę ir reguliarią prieigos teisių kontrolę;

4.1.4. vykdyti nuolatinį veiksmų stebėjimą ir kontrolę;

4.1.5. užtikrinti Bendrovės neskelbtinos informacijos apsaugą techninėmis priemonėmis;

4.1.6. užtikrinti, kad nuotolinio prisijungimo ryšys būtų kontroliuojamas ir sutaptų su iš anksto tarpusavyje suderintais tikslais;

4.1.7. užtikrinti, kad nuotolinio ryšio prisijungimas ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „Būtina darbui“ bei turėtų sutartą galiojimo terminą.

5. Bendrieji kibernetinio saugumo reikalavimai

5.1. Tiekėjas turi užtikrinti, kad bet kokiai technologijai, diegiamai ar įdiegtai Bendrovėje, yra gautas Bendrovės sutikimas ją naudoti, taip pat užtikrinti, kad šios technologijos saugumas yra pakankamas.

5.2. Tiekėjų informacinių sistemų (infrastruktūros) naudotojai ar administratoriai turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone.

5.3. Suteikiant laikinus slaptažodžius informacinių sistemų (infrastruktūros) naudotojams ar administratoriams, šie slaptažodžiai turi būti unikalūs kiekvienam naudotojui ar administratoriui ir perduodami saugiu būdu.

5.4. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo naudotojo ar administratoriaus vardo ir tik tuo atveju, jeigu naudotojas ar administratorius neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių naudotojui ar administratoriui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

5.5. Visose informacinėse sistemose (infrastruktūroje), prieš pradedant jas eksploatuoti, Tiekėjų informacinių sistemų administratoriai privalo pakeisti standartinius (gamintojų) slaptažodžius į šiuos Reikalavimus atitinkančius slaptažodžius.

5.6. Informacinių sistemų (infrastruktūros) administratoriaus funkcijos turi būti atliekamos naudojant tam skirtą naudotojo vardą, kuris negali būti naudojamas kasdienėms informacinių sistemų (infrastruktūros) naudotojo funkcijoms atlikti.

5.7. Informacinių sistemų (infrastruktūros) naudotojams draudžiama suteikti privilegijuotas (angl. a*dministrator, root*) teises.

5.8. Kiekvienas informacinių sistemų (infrastruktūros) naudotojas ar administratorius turi būti unikaliai atpažįstamas.

5.9. Informacinėse sistemose (infrastruktūroje) turi būti išjungiamos visos nereikalingos gamyklinės naudotojų paskyros (įskaitant svečio paskyras).

5.10. Viešai prieinamose kompiuterizuotose darbo vietose paskutinio naudotojo vardas neturi būti matomas prisijungimo metu.

5.11. Tiekėjų personalui prieiga turi būti suteikiama vadovaujantis principu „Būtina darbui“.

5.12. Nuotolinė prieiga prie informacinių sistemų (infrastruktūros) su administratoriaus paskyra turi būti draudžiama.

5.13. Prisijungdamas nuotoline prieiga prie informacinių sistemų (infrastruktūros) naudotojas privalo patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone.

5.14. Bet kokia nepatvirtinta nuotolinė prieiga prie Bendrovės informacinių sistemų (infrastruktūros), duomenų ar įrangos yra draudžiama.

6. Trečiojo asmens (išorės šalies) įsipareigojimai

6.1. Tiekėjas įsipareigoja:

6.1.1. dirbant su Bendrovės išduotais informaciniais resursais (kompiuteriais, mobiliaisiais įrenginiais, informacijos laikmenomis, dokumentais, duomenimis ir informacija) vadovautis Bendrovės konfidencialumo reikalavimais, šiais Reikalavimais ir įdiegtais procesais;

6.1.2. saugoti ir be Bendrovės išankstinio raštiško sutikimo neatskleisti tvarkomų Asmens duomenų ir (ar) neskelbtinos informacijos jokiems kitiems asmenims ir gavėjams;

6.1.3. atsakyti už visus Bendrovės informacinėms sistemoms (infrastruktūrai) žalingus veiksmus, kuriuos padarė Tiekėjo atstovai ir atlyginti žalingais veiksmais padarytus nuostolius;

6.1.4. užtikrinti Bendrovės elektroninės informacijos konfidencialumą bei vientisumą, savo veiksmais netrikdyti elektroninės informacijos prieinamumo;

6.1.5. naudoti tik tas prieigos prie informacinės sistemos (infrastruktūros) teises (sukurti, redaguoti, papildyti ar panaikinti), kurios buvo suteiktos;

6.1.6. baigus darbą ar naudotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri apdorojama informacinėje sistemoje (infrastruktūroje), negalėtų susipažinti pašaliniai asmenys- atsijungiama nuo informacinės sistemos (infrastruktūros), įjungiama ekrano užsklanda su slaptažodžio reikalavimu ir panašiai;

6.1.7. naudotis tik tomis informacinės sistemos (infrastruktūros) funkcijomis ir tokia informacijos apimtimi prie kurios buvo suteikta prieiga;

6.1.8. sužinojus apie informacijos ir kibernetinio saugumo incidentą, kuris gali būti susijęs su Bendrovės duomenimis ar informaciniais resursais, nedelsiant, tačiau, bet kokiu atveju ne vėliau nei per 24 val. nuo sužinojimo laiko, informuoti Bendrovę žodžiu, tel.: +370 670 59912 ir raštu, el. p.: soc@vici.eu, pateikiant visą turimą informaciją bei duomenis, susijusius su incidentu;

6.1.9. imtis pakankamų priemonių rizikoms, susijusioms su savo pasitelktais trečiaisiais asmenimis, jų atliekamais darbais ir tiekimo grandine, suvaldyti.

6.2. Tiekėjams draudžiama:

6.2.1. skenuoti Bendrovės informacines sistemas (infrastruktūrą), ieškant pažeidžiamumų ar kitais būdais stebėti Bendrovės informacinių sistemų (infrastruktūros) duomenų srautą. Jeigu šiame punkte išvardintos priemonės yra reikalingos tiesioginėms paslaugoms atlikti, tai šias priemones galima naudoti tik suderinus su Bendrovės informacijos saugumo įgaliotiniu;

6.2.2. be atskiro Bendrovės leidimo ir žinios jungtis prie Bendrovės informacinių sistemų (infrastruktūros) naudojant ne Bendrovės išduotą įrangą (išskyrus Bendrovės svečiams skirtame belaidžiame tinkle);

6.2.3. gerti, valgyti ir rūkyti šalia informacijos apdorojimo įrangos;

6.2.4. savavališkai keisti suteiktus tinklo parametrus (IP adresą ir pan.);

6.2.5. naudoti programas, kurios gali trikdyti Bendrovės informacinių sistemų (infrastruktūros) veikimą (skenavimo, blokavimo programas ir pan.);

6.2.6. savarankiškai keisti, remontuoti, taisyti Bendrovės išduotą programinę ir techninę įrangą;

6.2.7. naudoti Bendrovės 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 Bendrovės ar kitų asmenų teisėtus interesus;

6.2.8. diegti, saugoti, naudoti, kopijuoti ar platinti nelegalią, autorines teises pažeidžiančią programinę įrangą.

7. Atsakomybė

7.1. Jeigu Lietuvos Respublikos kibernetinio saugumo įstatyme nurodytos kontroliuojančios institucijos nustato informacijos ir kibernetinio saugumo incidentą, kuris kilo dėl Tiekėjo veiksmų ar neveikimo vykdant Sutartį, ir Bendrovei skiriama piniginė sankcija, tai Tiekėjas įsipareigoja Bendrovei pareikalavus atlyginti tokios sankcijos sumą, vadovaujantis Sutartyje numatyta baudų sumokėjimo tvarka.

7.2. Už Tiekėjo pasitelktų trečiųjų asmenų tinkamą Reikalavimų įgyvendinimą atsako Tiekėjas.

8. Papildomi reikalavimai taikomi kuriant programinę įrangą

8.1. Tiekėjas nustato, dokumentuoja ir įgyvendina iniciatyvas, atitinkančias bendrai priimtus informacijos ir kibernetinio saugumo standartus bei praktiką, siekiant sukurti saugius programinės ar techninės įrangos kūrimo procesus. Tokios iniciatyvos turi užtikrinti informacijos ir kibernetinį saugumą visuose plėtros etapuose: mokymuose, reikalavimų apibrėžimuose, dizaino kūrime, diegime, patvirtinime, išleidime ir priežiūroje.

8.2. Programinė įranga neturi turėti naudotojo paskyrų, slaptažodžių ar privačių / slaptų

raktų, kurių negali pakeisti arba pašalinti įgaliotasis produkto galutinis vartotojas.

8.3. Programinė įranga neturi turėti jokių naudotojo paskyrų (individualių, bendrų, testavimo aplinkos), kurios nėra dokumentuotos.

8.4. Tiekėjas turi aktyviai imtis priemonių, kad būtų pagerinta produkto saugumo kokybė. Šios priemonės turi atitikti bendrai priimtus pramoninių procesų valdymo kibernetinio saugumo standartus ir praktiką bei, jei tai techniškai įmanoma, apimti patikimumo bandymus, pažeidžiamumų valdymą ir programinio kodo saugumo testavimus (įskaitant statinio ar binarinio kodo analizę).

8.5. Tiekėjas, perkeliant kuriamą ir/ar vystomą programinę įrangą į darbinę aplinką, privalo užtikrinti kuriamo programinio kodo higieną (pvz., negali būti pavyzdinės imties duomenų Ir scenarijaus kodo, nuorodų į nenaudojamas bibliotekas, derinimo kodo ir kitų naudotų įrankių).

8.6. Kuriamos ir/ar vystomos programinės įrangos kūrimo, testavimo ir darbinės aplinkos turi būti atskirtos.

8.7. Programinės įrangos naudotojams neturi būti rodomi, kuriamos ir/ar vystomos programinės įrangos klaidų apie programinį kodą ar tarnybinės stoties, pranešimai.

Tiekėjo vardu .....

(vardas, pavardė, pareigos, parašas, data)