TIEKĖJO SAUGUMO KLAUSIMYNAS

Klausimyną Perkančiosios organizacijos prašymu pildo Tiekėjas, kurio pasiūlymas atitinkamoje pirkimo dalyje preliminariai gali būti pripažintas laimėjusiu.

Klausimyno informacija naudojama Tiekėjo ir su jo siūlomu prietaisu susijusiai kibernetinio saugumo bei tiekimo grandinės rizikai įvertinti.

Tiekėjas	
Siūlomo Prietaiso gamintojas ir modelis	
Pirkimo dalis (-ys) Nr. ir pavadinimas (-ai)	
Klausimyno pildymo data	

Pildymo būdas. Tiekėjas pažymi vieną iš prie kiekvieno klausimo nurodytų atsakymo variantų. Kai prie klausimo prašoma pateikti paaiškinimą ar papildomą informaciją, ji pateikiama kartu su atsakymu. Perkančiajai organizacijai paprašius, Tiekėjas taip pat pateikia papildomus paaiškinimus, dokumentus ar kitus atsakymą pagrindžiančius įrodymus.

Tiekėjas pirmiausia užpildo A dalį „Prieigos ir duomenų tvarkymo modelis“. Atsižvelgdama į pateiktą informaciją, Perkančioji organizacija nustato taikomą klausimyno apimtį:

- jeigu Tiekėjui, gamintojui ar kitai trečiajai šaliai nereikalinga nei nuotolinė, nei vietinė prieiga prie Prietaiso kompiuterio, programinės įrangos, joje saugomų Perkančiosios organizacijos duomenų ar administravimo funkcijų ir Tiekėjo, gamintojo ar kitos trečiosios šalies infrastruktūroje nėra tvarkomi Perkančiosios organizacijos duomenys - taikoma B dalis „Mažos svarbos tiekėjo vertinimas“;
- jeigu Tiekėjui, gamintojui ar kitai trečiajai šaliai reikalinga nuotolinė prieiga arba vietinė prieiga prie Prietaiso kompiuterio, programinės įrangos, joje saugomų Perkančiosios organizacijos duomenų ar administravimo funkcijų, arba Tiekėjo, gamintojo ar kitos trečiosios šalies infrastruktūroje tvarkomi Perkančiosios organizacijos duomenys - taikoma C dalis „Vidutinės svarbos tiekėjo vertinimas“.

Galutinę Tiekėjo kategoriją ir vertinimo apimtį nustato Perkančioji organizacija, atsižvelgdama į suteikiamos prieigos pobūdį ir lygį, tvarkomų duomenų jautrumą bei galimą poveikį Perkančiosios organizacijos tinklų ir informacinių sistemų saugumui ir veiklos tęstinumui.

Jeigu Perkančioji organizacija nustato, kad Tiekėjas priskirtinas kritinių tiekėjų kategorijai, atliekamas papildomas kritiniams tiekėjams taikomas vertinimas pagal Perkančiosios organizacijos Tiekimo grandinės saugumo valdymo tvarką.

A. PRIEIGOS IR DUOMENŲ TVARKYMO MODELIS

A.1. Ar Prietaiso diegimui, techninei priežiūrai, diagnostikai, gedimų šalinimui ar programinės įrangos atnaujinimams Tiekėjui ir (ar) jo pasitelktiems gamintojo ar subtiekėjo specialistams reikalinga nuotolinė prieiga prie Prietaiso arba Perkančiosios organizacijos tinklų ir informacinių sistemų?

Tiekėjo atsakymas	☐ Taip ☐ Ne
Jeigu „Taip“	*Trumpai aprašykite nuotolinės prieigos paskirtį, komponentus, prie kurių jungiama, ir kas vykdys prisijungimą.*

A.2. Ar Prietaisas arba jo programinė įranga automatiškai jungiasi prie Tiekėjo, gamintojo ar kitų išorinių informacinių sistemų ar debesijos paslaugų?

Tiekėjo atsakymas	☐ Taip ☐ Ne
Jeigu „Taip“	*Nurodykite ryšio paskirtį ir perduodamos informacijos pobūdį.*

A.3. Ar pacientų, medicininiai arba kiti Perkančiosios organizacijos duomenys bus perduodami, saugomi ar kitaip tvarkomi Tiekėjo, gamintojo ar kitos trečiosios šalies infrastruktūroje?

Tiekėjo atsakymas	☐ Taip ☐ Ne
Jeigu „Taip“	*Nurodykite tvarkomų duomenų pobūdį, tvarkymo paskirtį ir kas juos tvarkys.*

A.4. Ar pagrindinėms Prietaiso funkcijoms vykdyti reikalingas nuolatinis interneto ryšys arba ryšys su Tiekėjo / gamintojo išorinėmis sistemomis?

Tiekėjo atsakymas	☐ Taip ☐ Iš dalies ☐ Ne
Paaiškinimas	*Jeigu atsakymas „Taip“ arba „Iš dalies“, nurodyti, kurioms funkcijoms reikalingas ryšys, ryšio paskirtį, su kokiomis išorinėmis sistemomis jungiamasi ir kokio pobūdžio informacija perduodama:*

A.5. Jeigu reikalinga nuotolinė prieiga, ar Tiekėjo techninės priežiūros modelis leidžia ją vykdyti tik per Perkančiosios organizacijos nustatytas ir valdomas nuotolinės prieigos priemones, nenaudojant nuolatinio ar nekontroliuojamo alternatyvaus prisijungimo kanalo?

Tiekėjo atsakymas	☐ Taip ☐ Iš dalies ☐ Ne ☐ Netaikoma

Paaiškinimas	*Jeigu atsakymas „Iš dalies“ arba „Ne“, trumpai paaiškinkite. Kitais atvejais - Perkančiajai organizacijai paprašius. „Netaikoma“ žymima tik tuo atveju, jeigu A.1 klausimo atsakymas yra „Ne“.*

A.6. Ar Prietaiso diegimo, techninės priežiūros, diagnostikos, gedimų šalinimo ar programinės įrangos atnaujinimo metu Tiekėjo, gamintojo ar subtiekėjo specialistams gali būti suteikiama vietinė (ne nuotolinė) prieiga prie Prietaiso kompiuterio, programinės įrangos, joje saugomų Perkančiosios organizacijos duomenų arba administravimo funkcijų?

Tiekėjo atsakymas	☐ Taip ☐ Ne
Jeigu „Taip“	*Jeigu atsakymas „Taip“, nurodyti, kokiais atvejais ir kokiu tikslu prieiga reikalinga, prie kokių komponentų, duomenų ar administravimo funkcijų ji gali būti suteikiama ir koks numatomas prieigos lygis:*

B. MAŽOS SVARBOS TIEKĖJO VERTINIMAS

Pildoma, kai pagal A dalyje pateiktą informaciją Tiekėjui, gamintojui ar kitai trečiajai šaliai nereikalinga nei nuotolinė, nei vietinė prieiga prie Prietaiso kompiuterio, programinės įrangos, joje saugomų Perkančiosios organizacijos duomenų ar administravimo funkcijų ir Perkančiosios organizacijos duomenys nėra tvarkomi Tiekėjo, gamintojo ar kitos trečiosios šalies infrastruktūroje.

Atsakymo forma: Taip / Ne. Jeigu atsakymas „Ne“, Tiekėjas privalo pateikti trumpą paaiškinimą. Nepriklausomai nuo pasirinkto atsakymo, Perkančioji organizacija prireikus gali paprašyti papildomų paaiškinimų, dokumentų ar kitų atsakymą pagrindžiančių įrodymų.

B.1. Konfidencialumas. Ar Tiekėjas užtikrina, kad jo darbuotojai ir kiti Sutarties vykdymui pasitelkti asmenys laikytųsi konfidencialumo reikalavimų, kiek vykdydami Sutartį jie gali susipažinti su Perkančiosios organizacijos duomenimis ar kita nevieša informacija?

Tiekėjo atsakymas	☐ Taip ☐ Ne
Paaiškinimas	*Paaiškinimas privalomas, jei atsakymas „Ne“. Atsakius „Taip“, papildomas paaiškinimas ar atsakymą pagrindžiantys įrodymai pateikiami Perkančiajai organizacijai paprašius.*

B.2. Bazinė IT higiena. Ar Tiekėjas laikosi bazinės IT saugos praktikos, susijusios su Sutarties vykdymui naudojamomis informacinėmis technologijomis, įskaitant gamintojo palaikomos programinės įrangos naudojimą, saugumo atnaujinimų diegimą ir apsaugos nuo kenkėjiškos programinės įrangos priemonių naudojimą, kai jos taikomos?

Tiekėjo atsakymas	☐ Taip ☐ Ne

Paaiškinimas	*Paaiškinimas privalomas, jei atsakymas „Ne“. Atsakius „Taip“, papildomas paaiškinimas ar atsakymą pagrindžiantys įrodymai pateikiami Perkančiajai organizacijai paprašius.*

C. VIDUTINĖS SVARBOS TIEKĖJO VERTINIMAS

Pildoma, kai Tiekėjui, gamintojui ar kitai trečiajai šaliai reikalinga nuotolinė prieiga arba vietinė prieiga prie Prietaiso kompiuterio, programinės įrangos, joje saugomų Perkančiosios organizacijos duomenų ar administravimo funkcijų, arba Tiekėjo, gamintojo ar kitos trečiosios šalies infrastruktūroje tvarkomi Perkančiosios organizacijos duomenys.

Atsakymo forma: Taip / Iš dalies / Ne / Netaikoma. „Netaikoma“ žymima tik tuo atveju, kai konkretus klausimas objektyviai netaikomas Tiekėjo veiklai, naudojamai infrastruktūrai, suteikiamai prieigai ar tvarkomiems Perkančiosios organizacijos duomenims. Jeigu atsakymas „Iš dalies“, „Ne“ arba „Netaikoma“, Tiekėjas pateikia trumpą paaiškinimą. Perkančioji organizacija prireikus gali paprašyti papildomų paaiškinimų, dokumentų ar kitų atsakymą pagrindžiančių įrodymų.

C.1. Tiekėjo naudojamų sistemų apsauga. Ar Tiekėjo ir (ar) jo pasitelkto gamintojo ar kitos trečiosios šalies valdomuose įrenginiuose ir sistemose, kurie naudojami nuotolinei ir (ar) vietinei Prietaiso priežiūrai ir (ar) Perkančiosios organizacijos duomenims tvarkyti, naudojamos antivirusinės, EDR arba kitos lygiavertės techninės apsaugos priemonės?

Tiekėjo atsakymas	☐ Taip ☐ Iš dalies ☐ Ne ☐ Netaikoma
Paaiškinimas / įrodymas	*Jeigu atsakymas „Iš dalies“, „Ne“ arba „Netaikoma“, trumpai paaiškinkite. Perkančiajai organizacijai paprašius, nurodykite atsakymą pagrindžiantį dokumentą, nuorodą ar kitą įrodymą.*

C.2. Programinės įrangos ir operacinių sistemų atnaujinimas. Ar Tiekėjo ir (ar) jo pasitelkto gamintojo ar kitos trečiosios šalies valdomuose įrenginiuose ir sistemose, kurie naudojami nuotolinei ir (ar) vietinei Prietaiso priežiūrai ir (ar) Perkančiosios organizacijos duomenims tvarkyti, naudojamos gamintojo palaikomos operacinių sistemų ir programinės įrangos versijos ir diegiami joms skirti saugumo atnaujinimai?

Tiekėjo atsakymas	☐ Taip ☐ Iš dalies ☐ Ne ☐ Netaikoma
Paaiškinimas / įrodymas	*Jeigu atsakymas „Iš dalies“, „Ne“ arba „Netaikoma“, trumpai paaiškinkite. Perkančiajai organizacijai paprašius, nurodykite atsakymą pagrindžiantį dokumentą, nuorodą ar kitą įrodymą.*

C.3. Individualios naudotojų paskyros. Ar Tiekėjo, gamintojo ar subtiekėjo specialistai, kuriems suteikiama nuotolinė arba vietinė prieiga prie Prietaiso kompiuterio, programinės įrangos ar administravimo funkcijų, naudoja individualias naudotojų paskyras, o bendros keliems specialistams skirtos paskyros nėra naudojamos? Taikoma, jeigu A.1 arba A.6 klausimo atsakymas yra „Taip“.

Taikoma tik tuo atveju, jeigu A.1 atsakymas „Taip“.

Tiekėjo atsakymas	☐ Taip ☐ Iš dalies ☐ Ne ☐ Netaikoma
Paaiškinimas / įrodymas	*Jeigu atsakymas „Iš dalies“, „Ne“ arba „Netaikoma“, trumpai paaiškinkite. Perkančiajai organizacijai paprašius, nurodykite atsakymą pagrindžiantį dokumentą, nuorodą ar kitą įrodymą.*

C.4. Saugumo incidentų valdymas ir pranešimas. Ar Tiekėjas turi nustatytą procesą, pagal kurį identifikuojami ir valdomi kibernetiniai incidentai ar saugumo pažeidimai ir Perkančioji organizacija informuojama apie incidentus, galinčius paveikti jos Prietaisą, tinklus, informacines sistemas ar duomenis?

Tiekėjo atsakymas	☐ Taip ☐ Iš dalies ☐ Ne ☐ Netaikoma
Paaiškinimas / įrodymas	*Jeigu atsakymas „Iš dalies“, „Ne“ arba „Netaikoma“, trumpai paaiškinkite. Perkančiajai organizacijai paprašius, nurodykite atsakymą pagrindžiantį dokumentą, nuorodą ar kitą įrodymą.*

C.5. Konfidencialumas. Ar Tiekėjo darbuotojai ir kiti Sutarties vykdymui pasitelkti asmenys, kuriems gali būti suteikta prieiga prie Perkančiosios organizacijos duomenų ar kitos neviešos informacijos, yra įsipareigoję laikytis konfidencialumo reikalavimų?

Tiekėjo atsakymas	☐ Taip ☐ Iš dalies ☐ Ne ☐ Netaikoma
Paaiškinimas / įrodymas	*Jeigu atsakymas „Iš dalies“, „Ne“ arba „Netaikoma“, trumpai paaiškinkite. Perkančiajai organizacijai paprašius, nurodykite atsakymą pagrindžiantį dokumentą, nuorodą ar kitą įrodymą.*