Paslaugų pirkimo-pardavimo
sutarties specialiųjų sąlygų
5 priedas

KIBERNETINIO SAUGUMO REIKALAVIMAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Šis Priedas, atsižvelgiant į tai, kad Pirkėjas yra kibernetinio saugumo subjektas pagal Lietuvos Respublikos kibernetinio saugumo įstatymą (toliau – **KSĮ**), nustato Kibernetinio saugumo reikalavimus, taip pat šių reikalavimų įgyvendinimo, taikymo ir kontrolės tvarką.

2. Šiame Priede vartojamos sąvokos:

2.1. **Aprašas** – Kibernetinio saugumo reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

2.2. **Rekomendacijos** – Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos Rekomendacijos kibernetinio saugumo subjektams[1].

2.3. **Kibernetinio saugumo reikalavimai** – šiame Priede nustatyti organizaciniai, techniniai, procesiniai ir kiti reikalavimai, taikomi Tiekėjui, taip pat reikalavimai, perkelti iš Aprašo ar kitų teisės aktų ir taikomi tiek, kiek jie susiję su Sutarties dalyku.

2.4. **Papildomi kibernetinio saugumo reikalavimai** – šiame Priede atskirose lentelėse nustatyti reikalavimai, kuriuos Tiekėjas gali įsipareigoti įgyvendinti teikdamas Pasiūlymą ir kurių įgyvendinimas, Tiekėjui prisiėmus tokį įsipareigojimą, tampa privaloma Sutarties vykdymo sąlyga.

2.5. **Atitikties patvirtinimų tikrinimo aktas** – Pirkėjo sudaromas dokumentas, kuriame fiksuojami Kibernetinio saugumo reikalavimų ir Papildomų kibernetinio saugumo reikalavimų (jeigu taikoma) laikymosi patikrinimo rezultatai, nustatyti neatitikimai, jų pašalinimo terminai ir kitos su patikrinimu susijusios aplinkybės.

3. Kitos šiame Priede vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos KSĮ, Lietuvos Respublikos viešųjų pirkimų įstatyme, Apraše, Rekomendacijose ir kituose teisės aktuose, reglamentuojančiuose kibernetinio saugumo reikalavimus.

---

[1] https://www.nksc.lt/doc/NKSC_rekomendacijos_kibernetinio_saugumo_subjektams.pdf Jeigu Sutarties vykdymo metu pasikeistų išnašoje nurodyta internetinė nuoroda, taptų neaktyvi, būtų pakeistas pavadinimas, struktūra ar publikavimo vieta, turi būti taikoma naujausia viešai prieinama to paties šaltinio versija ar jos lygiavertis dokumentas.

4. Priedas yra neatskiriama Sutarties dalis ir taikomas visą Sutarties galiojimo laikotarpį.

5. Visi šiame Priede nustatyti Kibernetinio saugumo reikalavimai ir Papildomi kibernetinio saugumo reikalavimai (jeigu taikomi) yra keliami Tiekėjui. Tiekėjas privalo užtikrinti tinkamą ir savalaikį Kibernetinio saugumo reikalavimų ir Papildomų kibernetinio saugumo reikalavimų (jeigu taikoma) įgyvendinimą teikdamas Paslaugas.

6. Kibernetinio saugumo reikalavimai ir Papildomi kibernetinio saugumo reikalavimai (jeigu taikoma) Tiekėjui taikomi nepriklausomai nuo jų formuluotės pobūdžio ar teisės akto, iš kurio jie yra perkelti. Tais atvejais, kai reikalavimo formuluotė pagal savo turinį galėtų būti suprantama kaip adresuota Pirkėjui ar kitam subjektui, laikoma, kad pagal Sutartį tokio reikalavimo įgyvendinimas, kiek tai susiję su Pirkimo objektu, yra Tiekėjo pareiga. Tiekėjas negali remtis reikalavimo formuluotės aiškinimu ar interpretacija kaip pagrindu atsisakyti vykdyti šiame Priede nustatytas pareigas ar siaurinti jų apimtį.

7. Jeigu Tiekėjas Pasiūlyme įsipareigojo įgyvendinti Papildomus kibernetinio saugumo reikalavimus (nurodytus šio priedo 2, 4, 6, 8, ir10 lentelėse), tokie įsipareigojimai tampa privaloma Sutarties vykdymo sąlyga ir yra laikomi Kibernetinio saugumo reikalavimų dalimi.

8. Tiekėjas atsako už visų pasitelktų subtiekėjų, partnerių ar kitų asmenų veiksmus ir neveikimą kaip už savo paties veiksmus ir privalo užtikrinti, kad jie laikytųsi šiame Priede nustatytų Kibernetinio saugumo reikalavimų ir Papildomų kibernetinio saugumo reikalavimų (jeigu taikoma).

II SKYRIUS
KIBERNETINIO SAUGUMO REIKALAVIMŲ ĮGYVENDINIMO KONTROLĖ IR TIKRINIMAS

9. Pirkėjas turi teisę bet kuriuo Sutarties vykdymo metu tikrinti, kaip Tiekėjas laikosi šiame Priede nustatytų Kibernetinio saugumo reikalavimų ir Papildomų kibernetinio saugumo reikalavimų (jeigu taikoma).

10. Kibernetinio saugumo reikalavimų ir Papildomų kibernetinio saugumo reikalavimų (jeigu taikoma) laikymasis gali būti bet kuriuo Sutarties vykdymo momentu.

11. Pirkėjas turi teisę savo nuožiūra pasirinkti patikrinimo laiką, apimtį ir būdą. Patikrinimo metu gali būti vertinama dokumentacija, techniniai sprendiniai, konfigūracijos, testavimo rezultatai, saugumo nustatymai, procesai, organizacinės priemonės ir kiti su Kibernetinio saugumo reikalavimų ir Papildomų kibernetinio saugumo reikalavimų (jeigu taikoma) įgyvendinimu susiję aspektai.

12. Tiekėjas privalo: (i) sudaryti tinkamas sąlygas patikrinimui atlikti; (ii) laiku ir išsamiai teikti prašomą informaciją, dokumentus bei paaiškinimus; (iii) užtikrinti atsakingų ir kompetentingų specialistų dalyvavimą; (iv) aktyviai bendradarbiauti su Pirkėju.

13. Jeigu patikrinimo metu nustatoma, kad Kibernetinio saugumo reikalavimas ir (ar) Papildomas kibernetinio saugumo reikalavimas (jeigu taikoma), kuris pagal Sutarties nuostatas turėjo būti įgyvendintas arba jau galėjo būti aktualus, nėra įgyvendintas arba

įgyvendintas netinkamai, Pirkėjas raštu pateikia Tiekėjui nustatytų neatitikimų sąrašą ir nustato terminą jiems pašalinti. Jeigu Pirkėjas nenustato kitokio termino, Tiekėjas privalo pašalinti nustatytus neatitikimus ne vėliau kaip per 10 darbo dienų nuo pranešimo gavimo dienos ir apie pašalinimo faktą informuoti Pirkėją.

III SKYRIUS
KIBERNETINIO SAUGUMO REIKALAVIMAI, SKIRTI KIBERNETINIŲ INCIDENTŲ VALDYMUI

1 lentelė. Kibernetinio saugumo reikalavimai, skirti kibernetinių incidentų valdymui

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
1.	Turi būti fiksuojami šie žurnaliniai įrašai:			
1.1.	Naudotojų ir administratorių autentifikavimo įvykiai	Aprašo 1 lentelės 1.2 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: pateiktų žurnalinių įrašų kopijų analizė (pasirinktiniai įvykiai), t. y., Tiekėjas nuotolinio susitikimo metu turi inicijuoti Pirkėjo pasirinktą įvykį ir pademonstruoti (Tiekėjui rodant ekraną), kad inicijuotas įvykis buvo užregistruotas žurnaluose.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
1.2.	Naudotojų, administratorių paskyrų sukūrimas, prieigų prie tinklų ir informacinių sistemų pakeitimai;	Aprašo 1 lentelės 1.3 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: pateiktų žurnalinių įrašų kopijų analizė (pasirinktiniai įvykiai), t. y., Tiekėjas	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
			nuotolinio susitikimo metu turi inicijuoti Pirkėjo pasirinktą įvykį ir pademonstruoti (Tiekėjui rodant ekraną), kad inicijuotas įvykis buvo užregistruotas žurnaluose.	Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
1.3.	Administratorių atliekami veiksmai;	Aprašo 1 lentelės 1.4 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: pateiktų žurnalinių įrašų kopijų analizė (pasirinktiniai įvykiai), t. y., Tiekėjas nuotolinio susitikimo metu turi inicijuoti Pirkėjo pasirinktą įvykį ir pademonstruoti (tiekėjui rodant ekraną), kad inicijuotas įvykis buvo užregistruotas žurnaluose.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
1.4.	Žurnalinių įrašų rinkimo funkcijos įjungimas, išjungimas;	Aprašo 1 lentelės 1.8 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: pateiktų žurnalinių įrašų kopijų analizė (pasirinktiniai įvykiai), t. y., Tiekėjas nuotolinio susitikimo metu turi inicijuoti Pirkėjo pasirinktą įvykį ir pademonstruoti (Tiekėjui rodant ekraną), kad inicijuotas įvykis buvo užregistruotas žurnaluose.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
1.5.	Žurnalinių įrašų peržiūrėjimas, trynimas, kūrimas ar keitimas.	Aprašo 1 lentelės 1.13 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: pateiktų žurnalinių įrašų kopijų analizė (pasirinktiniai įvykiai), t. y., Tiekėjas nuotolinio susitikimo metu turi inicijuoti Prikėjo pasirinktą įvykį ir pademonstruoti (Tiekėjui rodant ekraną), kad inicijuotas įvykis buvo užregistruotas žurnaluose.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
1.6.	Žurnaliniai įrašai turi būti saugomi ne trumpiau kaip 90 kalendorinių dienų.	Aprašo 1 lentelės 7 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu, kad jo naudojamoje programinėje įrangoje, skirtoje įrašams saugoti ir valdyti, galima rasti Pirkėjo pasirinkto laiko tarpo įrašus (ne senesnius, nei 90 dienų).	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
1.7.	Draudžiama žurnalinius įrašus trinti, keisti, kol nesibaigęs žurnalinių įrašų saugojimo terminas.	Aprašo 1 lentelės 8 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
			Techninės priemonės: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu, kad jo naudojamoje programinėje įrangoje, skirtoje įrašams saugoti ir valdyti, galima rasti Pirkėjo pasirinkto laiko tarpo įrašus (ne senesnius, nei 90 dienų).	Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
1.8.	Žurnalinių įrašų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.	Aprašo 1 lentelės 9 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: Tiekėjas turi nuotolinio susitikimo metu atlikti demonstraciją, kurios metu būtų bandoma pakeisti ar ištrinti žurnalinius įrašus.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
1.9.	Saugasienės saugumo taisyklės turi būti nuolat peržiūrimos ir prireikus atnaujinamos. Būtina atlikti detalią taisyklių analizę ne rečiau kaip kartą per 6 mėn.	Aprašo 1 lentelės 15 eilutė	Sutartinis įsipareigojimas: Tiekėjas viešojo pirkimo sutarties vykdymo laikotarpiu įsipareigoja ne rečiau kaip kas 1 mėn. peržiūrėti Saugasienės saugumo taisykles ir, esant poreikiui, jas atnaujinti. Atnaujinimas derinamas su Pirkėju.	Sutarčių administratorius vykdo viešojo pirkimo sutarties įgyvendinimo priežiūrą. Tiekėjas pateikia atnaujintas Saugasienės saugumo taisykles.

2 lentelė. Papildomi kibernetinio saugumo reikalavimai, skirti kibernetinių incidentų valdymui

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
1.	Turėti Kibernetinių bei asmens duomenų saugos incidentų valdymo procedūrą.	Aprašo 34.3, 34.4 punktai	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Tiekėjas patvirtina, kad pasirašius viešojo pirkimo sutartį, Pirkėjas turės teisę reikalauti įtraukti atitinkamus reikalavimus į po viešojo pirkimo sutarties pasirašymo atnaujinamą procedūrą.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
2.	Turėti Pokyčių valdymo procedūrą.	Aprašo 38, 42, 43 punktai	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Tiekėjas patvirtina, kad pasirašius viešojo pirkimo sutartį, Pirkėjas turės teisę reikalauti įtraukti atitinkamus reikalavimus į po viešojo pirkimo sutarties pasirašymo atnaujinamą procedūrą.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą; Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

IV SKYRIUS
KIBERNETINIO SAUGUMO REIKALAVIMAI, SKIRTI VEIKLOS TĘSTINUMO VALDYMUI

3 lentelė. Kibernetinio saugumo reikalavimai, skirti veiklos tęstinumo valdymui

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
1.	Turi būti užtikrintas kibernetinio saugumo subjekto įvertintų kaip kritinių veiklos tęstinumui būtinų tinklų ir informacinių sistemų prieinamumas ne mažiau kaip 99 proc. laiko.	Aprašo 2 lentelės 16.2 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: faktinis prieinamumo nustatymas visą viešojo pirkimo sutarties įgyvendinimo laikotarpį, t. y., fiksuojami galimo neprieinamumo atvejai.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: išrašus iš informacinės sistemos. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
2.	Tiekėjas turi pateikti veiklos atkūrimo planus.	Aprašo 27 punktas	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

4 lentelė. Papildomi kibernetinio saugumo reikalavimai, skirti veiklos tęstinumo valdymui

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
1.	Tiekėjas turi turėti detalius veiklos atkūrimo planus šiems scenarijams: 1) duomenų centro neveikimas (ugnis, apliejimas); 2) interneto ryšio su duomenų centru praradimas;	Aprašo 38 punktas	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją,

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
	3) duomenų bazės sugadinimas, pažeidimas; 4) asmens duomenų nutekėjimas; 5) nesankcionuoto priėjimas prie administravimo panelės; 6) duomenų vagystė. Tiekėjas turi būti išbandęs visus aukščiau nurodytus scenarijus ir turėti tai įrodančius dokumentus.			pateikia Atitikties patvirtinimų tikrinimo aktą.

V SKYRIUS
KIBERNETINIO SAUGUMO REIKALAVIMAI, SKIRTI TINKLŲ IR INFORMACINIŲ SISTEMŲ ĮSIGIJIMO, PLĖTOJIMO IR PRIEŽIŪROS SAUGUMO, ĮSKAITANT SPRAGŲ VALDYMĄ IR ATSKLEIDIMĄ, VALDYMUI

5 lentelė. Kibernetinio saugumo reikalavimai, skirti tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, valdymui

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
1.	Serveriuose (įskaitant ir virtualias mašinas) ir darbo stotyse turi būti įjungtos ir sukonfigūruotos saugasienės, kurios kontroliuoja visą įeinantį ir išeinantį srautą.	Aprašo 3 lentelės 23 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu šių komandinės eilutės komandų rezultatus iš serverių aplinkos:	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas, Portscan komandos ar Nmap ar lygiavertės komandos ar programinės įrangos skanavimo rezultatus į nurodytus vidinius IP adresus. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
			1) komandinės eilutės tracert (Windows) rezultatą į viešąjį IP adresą arba interneto svetainę, 2) traceroute (Linux, Unix) arba lygiavertės (kai yra kitos operacinės sistemos) komandos rezultatą į viešąjį IP adresą arba interneto svetainę 3) iš viešojo tinklo komandinės eilutės komandos telnet (visos operacinės sistemos) rezultatą, nurodant užsakovo pasirinktus prievadus. 4) iš viešojo ir vidinio tinklo komandinės eilutės komandos ping (visos operacinės sistemos) rezultatą, nurodant užsakovo pasirinktus IP adresus.	
2.	Tinklui valdyti turi būti naudojami saugūs tinklo protokolai.	Aprašo 3 lentelės 27 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu: 1) kad uždraustas ar išjungtas – telnet, SNNP v1/v2; 2) kad SSH naudoja 2048 bit ilgio raktą; 3) kad tam tikri prievadai yra užblokuoti (įskaitant, bet neapsiribojant 21, 23, 80, 161); 4) SSH, SNNP v3 įgalinimas.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas, Nmap arba lygiavertės programinės įrangos IP adresų ir prievadų bei protokolų skanavimo ataskaitą. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
3.	Turi būti uždrausti / išjungti visi nebūtini protokolai ir atviri prievadai (angl. p*ort)*.	Aprašo 3 lentelės 28 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Programos Nmap visų tinklo mazgų IP skanavimo galimybes.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: Programos Nmap visų tinklo mazgų IP skanavimo ataskaitą. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
4.	Turi būti diegiami naudojamos programinės įrangos gamintojų ir operacinių sistemų rekomenduojami atnaujinimai.	Aprašo 3 lentelės 30 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą – procedūrą. Techninės priemonės: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu, kaip veikia automatinių atnaujinimų diegimas, informacinei sistemai naudojamos programinės įrangos gamintojo išleistų atnaujinimų identifikavimas – automatinių atnaujinimų diegimo konfigūracija (Intune, WSUS, SCCM ar panašiomis priemonėmis).	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
5.	Draudžiama svetainės serveriuose saugoti sesijos duomenis (identifikatorių) prisijungimo tikslams, pasibaigus susijungimo sesijai.	Aprašo 3 lentelės 35 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu, kaip veikia: 1) prisijungimas; 2) atsijungimas; 3) back mygtuko spaudimas naršyklėse; 4) neaktyvumas, sesijos regeneravimas.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
			Pirkėjas gali paprašyti suteikti galimybę peržiūrėti kodą (static code review), kur suprogramuoti šie reikalavimai.	
6.	Internetu prieinamoms svetainėms, tinklų ir informacinėms sistemoms turi būti naudojama svetainės saugasienė (angl. *Web Application Firewall*).	Aprašo 3 lentelės 36 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: a) Tiekėjas turi pademonstruoti nuotolinio susitikimo metu. kaip atlieka: 1) SQL injection testą; 2) XSS testą; 3) Nslookup ar curl komandas (Pirkėjo pasirinktiems atvejams); 4) WAF žurnalus; b) Pirkėjas atliks http headers analizę. Pirkėjas pasilieka teise panaudoti pasirinktus interneto resursus WAF patikrai.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
7.	Internetu prieinamoms svetainėms, tinklų ir informacinėms sistemoms turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų remiantis OWASP (angl. *The Open Web Application Security Project)* Top 10 geriausiomis praktikomis (www.owasp.org).	Aprašo 3 lentelės 37 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu, kaip atlieka: 1) SQL injection testą; 2) XSS testą. Pirkėjas pasilieka teisę atlikti uncredentialed pažeidžiamumų testavimą.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Tiekėjas turi pateikti pažeidžiamumų testavimo protokolą. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
8.	Žiniatinklio (angl. *W*eb) formose turi būti naudojama svetainės	Aprašo 3 lentelės 38 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: a) Tiekėjas turi pademonstruoti nuotolinio susitikimo metu,	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
	naudotojo įvedamų duomenų kontrolė (angl. *Input validation*).		kaip atlieka bandymo įvesti netinkamus duomenis testus, įskaitant, bet neapsiribojant (Pirkėjas gali paprašyti įvesti ir kitus netikrus duomenis): 1) Tuščio lauko testą; 2) Maksimalaus ilgio testą; 3) Netinkamo formato testą; 4) Slapukų (coockies) testą; b) Pirkėjas patikrina tai nusakančius HTML 5 atributus pasirinktomis priemonėmis.	Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
9.	Internetu prieinamos tinklų ir informacinės sistemos neturi rodyti naudotojui klaidų pranešimų apie tinklų ir informacinės sistemos ir programinį kodą ar serverį.	Aprašo 3 lentelės 39 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: a) Tiekėjas turi pademonstruoti nuotolinio susitikimo metu, kaip atlieka šiuos testus (įskaitant, bet neapsiribojant): 1) neegzistuojančio adreso patikra; 2) draudžiamos prieigos patikra; b) Pirkėjas patikrina tai nusakančius HTML 5 atributus pasirinktomis priemonėmis.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
10.	Internetu naudojant HTTPS protokolą (angl. *HyperText Transfer Protocol Secure,* HTTPS) prieinamos tinklų ir informacinės sistemos saugumo priemonės turi leisti tik jų funkcionalumui užtikrinti reikalingus protokolo metodus.	Aprašo 3 lentelės 40 eilutė	Pirkėjas patikrina tai nusakančius HTML 5 atributus pasirinktomis priemonėmis. Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: a) Tiekėjas turi pademonstruoti nuotolinio susitikimo metu, kaip atlieka šiuos testus (įskaitant, bet neapsiribojant): 1) Pirkėjas pasirinktų metodų patikros testas; 2) įrašymo, trynimo testai; b) Pirkėjas patikrina tai nusakančius HTML 5 atributus pasirinktomis priemonėmis.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
			Pirkėjas gali paprašyti Web Serverio konfigūracijos audito ataskaitos.	
11.	Reikalavimas reguliariai vertinti spragas, o visą tinklų informacinės sistemos spragų skenavimą atlikti ne rečiau kaip kas 6 mėnesius.	Aprašo 45.8 punktas	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pateikti pažeidžiamumų (pentest) ataskaitą Pirkėjo peržiūrai. Rekomenduojama naudoti nemokamą https://site-check.nksc.lt/. Tiekėjas gali rinktis savo pentest partnerį.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: pažeidžiamumų (pentest) ataskaitą. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą, jei jame nėra pateikta Critical, High pažeidžiamumų.

6 lentelė. Papildomi kibernetinio saugumo reikalavimai, skirti tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, valdymui

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
1.	Tiekėjo patvirtintos techninės ir organizacinės priemonės, naudojamos saugai ir 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (BDAR) atitikčiai užtikrinti.	NKSC rekomendacijų Raudonos CIS kontrolės įmonėms 14, 15 punktai.	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas organizacines priemones: Tiekėjas turi pateikti vidaus dokumentą, įrodantį reikalavimo įgyvendinimą.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus dokumentą, įrodantį reikalavimo įgyvendinimą. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą patvirtinamas aktas.

VI SKYRIUS

KIBERNETINIO SAUGUMO REIKALAVIMAI, SKIRTI KRIPTOGRAFIJOS IR ŠIFRAVIMO NAUDOJIMO POLITIKOS IR PROCEDŪROS VALDYMUI

7 lentelė. Kibernetinio saugumo reikalavimai, skirti kriptografijos ir šifravimo naudojimo politikos ir procedūros valdymui

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	**2**	**3**	**4**	**5**
1.	Duomenys, perduodami tarp mobiliojo įrenginio ir tinklų ir informacinės sistemos, 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.	Aprašo 4 lentelės 46 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą, kad Pirkėjas galėtų įvertinti atitikimą reikalavimui: 1) naudojamų informacinei sistemai sertifikatų ir kodavimo algoritmų informaciją; 2) naudojamos VPN tarnybos informaciją ir konfigūracijos ekranvaizdžius, iš kurių galima įvertinti, kokie VPN kodavimo algoritmai naudojami. Techninės priemonės: Pirkėjo prašymu Tiekėjas turi pademonstruoti nuotolinio susitikimo metu: • AES-256 arba lygiavertis; • SHA-2 algoritmai arba lygiaverčiai; • ECDH/PFS rakto keitimo algoritmas arba lygiavertis.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
2.	**Turi būti įgyvendinti svetainės kriptografijos reikalavimai:**			

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
2.1.	turi būti naudojami oficialiai pripažinti saugus ilgio raktai;	Aprašo 4 lentelės 48.1 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą, kad Pirkėjas galėtų įvertinti atitikimą reikalavimui: 1) naudojamų informacinei sistemai sertifikatų ir kodavimo algoritmų informaciją; 2) naudojamos VPN tarnybos informaciją ir konfigūracijos ekranvaizdžius, iš kurių galima įvertinti, kokie VPN kodavimo algoritmai naudojami. Techninės priemonės: Pirkėjo prašymu Tiekėjas turi pademonstruoti nuotolinio susitikimo metu: 1) AES-256 arba lygiavertis 2) SHA-2 algoritmai arba lygiaverčiai, 3) ECDH/PFS rakto keitimo algoritmas arba lygiavertis.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
2.2.	atliekant svetainės administravimo darbus, ryšys turi būti šifruojamas;	Aprašo 4 lentelės 48.2 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines ir organizacines priemones. Organizacinės priemonės: Tiekėjas turės pateikti (įskaitant, tačiau neapsiribojant) vidaus dokumentus, įrodančius nurodyto reikalavimo įgyvendinimą, kad Pirkėjas galėtų įvertinti atitikimą reikalavimui: 1) naudojamų informacinei sistemai sertifikatų ir kodavimo algoritmų informaciją; 2) naudojamos VPN tarnybos informaciją ir konfigūracijos ekranvaizdžius, iš kurių galima įvertinti, kokie VPN kodavimo algoritmai naudojami. Techninės priemonės: Pirkėjo prašymu Tiekėjas turi pademonstruoti nuotolinio susitikimo metu: 1) AES-256 arba lygiavertis; 2) SHA-2 algoritmai arba lygiaverčiai; 3) ECDH/PFS rakto keitimo algoritmas arba lygiavertis.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
			Pirkėjas pasirinktomis priemonėmis patikrina: 1) TLS/SSL sertifikato informaciją; 2) ar naudojamas RSA algoritmas, kurio viešojo rakto ilgis bent jau 2048 bitų.	
2.3.	šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų;	Aprašo 4 lentelės 48.3 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones. Techninės priemonės: Pirkėjo prašymu Tiekėjas turi pademonstruoti nuotolinio susitikimo metu: 1) TLS/SSL sertifikato informacija viešai prieinamomis priemonėmis; 2) ar naudojamas RSA algoritmas, kurio viešojo rakto ilgis bent jau 2048 bitų; 3) ar nėra pernelyg ilgas sertifikato galiojimo laikas (paprastai yra <=12 mėn.); 4) ar sertifikatas nėra atšauktas (angl. revoked); 5) kad sertifikatas išduotas būtent tam domeno vardui arba jo subdomenams (angl. wildcard), įsitikinama, kad domeno vardas įtrauktas į SAN (angl. Subject Alternative Name); 6) ar sertifikatas išduotas pasaulyje pripažintų ir patikimų sertifikatų tarnybų (angl. Certificate Authority), įskaitant, tačiau neapsiribojant, DigiCert, Sectigo, Let's Encrypt, GlobalSign; 7) ar nenaudojamas self-signed certificate sertifikatas.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
2.4.	turi būti naudojamas TLS standartas (1.3 versija arba naujesnė);	Aprašo 4 lentelės 48.4 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones. Techninės priemonės: Pirkėjo prašymu Tiekėjas turi pademonstruoti nuotolinio susitikimo metu: 1) serverių konfigūracijos failų demonstracija; 2) komandinės eilutės komandos openssl rezultatas; TLS versiją naudojant viešai prieinamas priemones, įskaitant, bet neapsiribojant;	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
			3) https://www.ssllabs.com/ssltest/; 4) https://www.immuniweb.com/ .	
2.5.	svetainės kriptografinės funkcijos turi būti įdiegtos serverio, kuriame yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. *Hardware security module*);	Aprašo 4 lentelės 48.5 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones. Techninės priemonės: Pirkėjo prašymu Tiekėjas turi pademonstruoti nuotolinio susitikimo metu: 1) Web Serverių konfigūracijos failus; 2) atlikti slaptažodžio siuntimo analizę (pvz., naudojant naršyklės Kūrėjo įrankius (F12)-Network).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
2.6.	visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. *fail securely*).	Aprašo 4 lentelės 48.6 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones. Techninės priemonės: Pirkėjo prašymu Tiekėjas turi pademonstruoti nuotolinio susitikimo metu HTML atributų peržiūrą (pvz., naudojant naršyklių Kūrėjo įrankius (F12)-Elements, Application, Storage).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
3.	Duomenys atsarginėse kopijose turi būti užšifruoti (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų	Aprašo 4 lentelės 49 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas organizacines ir technines priemones. Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą; kontrolės priemones, naudojamas, užtikrinti šiam reikalavimui. Techninės priemonės: Pirkėjo prašymu Tiekėjas turi pademonstruoti nuotolinio susitikimo metu, kad atsarginės kopijos yra užšifruotos.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
	informacijai neteisėtai atkurti.			
4.	Turi būti saugomi ir stebimi audito įrašai, susiję su kriptografinių raktų valdymo veikla (generavimas, sunaikinimas, archyvavimas, naudotojų veiksmai).	Aprašo 4 lentelės 50 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas organizacines priemones. Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą; Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

8 lentelė. Papildomi kibernetinio saugumo reikalavimai, skirti kriptografijos ir šifravimo naudojimo politikos ir procedūros valdymui

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
1.	Duomenų ramybės būsenoje šifravimo funkcionalumas.	NKSC rekomendacijų Raudonos CIS kontrolės įmonėms 3 punktas.	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu konfigūraciją, kuria remiantis Pirkėjas galėtų įvertinti atitikimą reikalavimui.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

VII SKYRIUS
KIBERNETINIO SAUGUMO REIKALAVIMAI, SKIRTI PRIEIGOS IR KELIŲ VEIKSNIŲ TAPATUMO NUSTATYMO PRIEMONIŲ VALDYMUI

9 lentelė. Kibernetinio saugumo reikalavimai, skirti prieigos ir kelių veiksnių tapatumo nustatymo priemonių valdymui

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
1.	Administratoriaus funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms naudotojo funkcijoms atlikti.	Aprašo 7 lentelės 58 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu: 1) lokalių informacinės sistemos paskyrų sąrašą; 2) naudojamo centralizuoto vartotojų valdymo sprendimą.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
2.	Kiekvienas naudotojas turi būti unikaliai atpažįstamas.	Aprašo 7 lentelės 60 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Tiekėjo naudojamo centralizuoto vartotojų valdymo sprendimo konfigūraciją.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
3.	Naudotojas ir administratorius turi patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksnių tapatumo nustatymo priemonės).	Aprašo 7 lentelės 61 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Tiekėjo naudojamo centralizuoto vartotojų valdymo sprendimo konfigūraciją.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
4.	Naudotojo teisė dirbti su konkrečia tinklų ir informacine sistema turi būti sustabdoma, kai naudotojas nesinaudoja tinklų ir informacine sistema ilgiau kaip 3 mėnesius.	Aprašo 7 lentelės 62 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Tiekėjo naudojamo centralizuoto vartotojų valdymo sprendimo konfigūraciją.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
5.	Administratoriaus teisė dirbti su tinklų ir informacine sistema turi būti sustabdoma, kai administratorius nesinaudoja tinklų ir informacine sistema ilgiau kaip 2 mėnesius.	Aprašo 7 lentelės 63 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Tiekėjo naudojamo centralizuoto vartotojų valdymo sprendimo konfigūraciją.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
6.	Kai naudotojas ar administratorius nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų naudotojo ar administratoriaus kvalifikacinių reikalavimų, taip pat pasibaigia jo darbo (tarnybos) santykiai, jis praranda patikimumą, jo teisė naudotis tinklų ir informacine sistema turi būti panaikinta nedelsiant, bet ne vėliau kaip per kibernetinio saugumo subjekto nustatytą terminą.	Aprašo 7 lentelės 64 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas organizacines priemones. Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą.	Reikalavimo atitikimui Tiekėjas pateikia: Organizacinės priemonės: vidaus teisės aktus, įrodančius nurodyto reikalavimo įgyvendinimą. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
7.	Baigus darbą arba pasitraukiant iš darbo vietos, turi būti atsijungiama nuo tinklų ir informacinių sistemų, įjungiama ekrano užsklanda su slaptažodžiu.	Aprašo 7 lentelės 65 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją,

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
				pateikia Atitikties patvirtinimų tikrinimo aktą.
8.	Kai naudotojas ar administratorius nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų naudotojo ar administratoriaus kvalifikacinių reikalavimų, taip pat pasibaigia jo darbo (tarnybos) santykiai, jis praranda patikimumą, jo teisė naudotis tinklų ir informacine sistema turi būti panaikinta nedelsiant, bet ne vėliau kaip per kibernetinio saugumo subjekto nustatytą terminą.	Aprašo 7 lentelės 66 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
9.	Tinkluose ir informacinėse sistemose neatliekant jokių veiksmų, darbo stotis turi užsirakinti (ne ilgiau nei po 15 minučių), kad toliau naudotis tinklų ir informacine sistema būtų galima tik pakartotinai patvirtinus savo tapatybę.	Aprašo 7 lentelės 67 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
10.	Tinklų ir informacinės sistemos dalys, tarp jų ir svetainės ir naršyklės, patvirtinančios naudotojo tapatumą, turi drausti išsaugoti slaptažodžius,	Aprašo 7 lentelės 68 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją,

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
	išskyrus specializuotą slaptažodžių tvarkymo programinę įrangą.			pateikia Atitikties patvirtinimų tikrinimo aktą.
11.	Slaptažodis turi būti sudarytas iš didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų simbolių.	Aprašo 7 lentelės 69 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
12.	Turi būti nustatytas maksimalus leistinas naudotojų mėginimų prisijungti prie tinklų ir informacinių sistemų skaičius – ne daugiau negu 5 kartai iš eilės. Po numatyto bandymų skaičiaus prisijungti prie tinklų ir informacinių sistemų paskyra turi užsiblokuoti. Atblokuoti gali tik įgalioti asmenys.	Aprašo 7 lentelės 70 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
13.	**Papildomi naudotojo slaptažodžių reikalavimai:**			
13.1.	slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius;	Aprašo 7 lentelės 71.1 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
13.2.	slaptažodį turi sudaryti ne mažiau kaip 10 simbolių;	Aprašo 7 lentelės 71.2 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
13.3.	keičiamo slaptažodžio neturi būti leidžiama sudaryti iš buvusių 6 paskutinių slaptažodžių;	Aprašo 7 lentelės 71.3 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
13.4.	pirmąkart jungiantis prie tinklų ir informacinių sistemų, turi būti reikalaujama, kad naudotojas pakeistų slaptažodį;	Aprašo 7 lentelės 71.4 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
13.5.	naudotojas turi turėti galimybę bet kuriuo metu pasikeisti slaptažodį.	Aprašo 7 lentelės 71.5 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
14.	**Papildomi administratorių slaptažodžių reikalavimai:**			
14.1.	slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius;	Aprašo 7 lentelės 72.1 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
14.2.	slaptažodį turi sudaryti ne mažiau kaip 15 simbolių;	Aprašo 7 lentelės 72.2 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
14.3.	keičiant slaptažodį, neturi būti leidžiama naudoti slaptažodžio iš buvusių 8 paskutinių slaptažodžių.	Aprašo 7 lentelės 72.3 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
15.	**Turi būti vykdoma administratorių paskyrų kontrolė:**			
15.1.	naudojamos administratorių paskyrų kontrolės priemonės, kurios periodiškai tikrina administratoriaus paskyras. Apie administratoriaus paskyras, kurios neatitinka	Aprašo 7 lentelės 73.2 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu administratorių paskyrų valdymo priemones ir konfigūraciją.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją,

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
	šiame skirsnyje nustatytų reikalavimų, turi būti pranešama įgaliotam asmeniui.			pateikia Atitikties patvirtinimų tikrinimo aktą.
16.	**Vykdoma naudotojų paskyrų kontrolė:**			
16.1.	naudojamos naudotojų paskyrų kontrolės priemonės, kurios periodiškai tikrina naudotojų paskyras. Apie naudotojų paskyras, kurios neatitinka šiame skirsnyje nustatytų reikalavimų, turi būti pranešama įgaliotam asmeniui.	Aprašo 7 lentelės 74.2 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
17.	Lokalios naudotojų ir administratorių paskyros turi atitikti reikalavimus, nurodytus šiame skirsnyje.	Aprašo 7 lentelės 75 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO): 1) lokalių administratoriaus paskyrų Grupinės politikos objektus (GPO), jei Windows Server; 2) /etc/security/pwquality.conf konfigūraciją, jei Linux serveriai; 3) kitų sistemų slaptažodžių konfigūraciją; 4) Tiekėjo patvirtintą dokumentą, aprašantį slaptažodžių politiką.	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.
18.	**Papildomi atpažinties, tapatumo patvirtinimo ir naudojimosi kontrolės reikalavimai (kibernetinio saugumo subjekto svetainėms, pasiekiamoms iš viešųjų elektroninių ryšių tinklų):**			
18.1.	programiniame kode draudžiama išsaugoti duomenis (vardą, slaptažodį, aplikacijų programavimo	Aprašo 7 lentelės 76.1 eilutė	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas techninės priemones: Tiekėjas turi pademonstruoti nuotolinio susitikimo metu Grupinės politikos objektą (GPO). Jei naudojama git repositorija, patikrina su	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas.

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
	sąsajas (angl. *Application programming interface*) raktus / ženklus (angl. *Token*) ir kt.), kuriuos atskleidus gali būti pasinaudota prieiga prie įrenginių, resursų, paskyrų ar valdiklių.		komanda git grep (naudojant tam tikrus raktinius žodžius, parinktus Pirkėjo): 1) Parodo Gitignore failo konfigūraciją; 2) Envirounment Variables konfigūraciją; 3) Atlieka kodo demonstracija, ieškant bet neapsirobojant šių žodžių password=, api_key=, secret=, token=, ftp_user, conn_string. Pirkėjas pasilieka teisę pareikalauti statinės kodo analizės įrankių, tokių kaip SonarQube, Bandit, TruffleHog, Gitleaks raporto.	Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

10 lentelė. Papildomi kibernetinio saugumo reikalavimai, skirti prieigos ir kelių veiksnių tapatumo nustatymo priemonių valdymui

Nr.	Reikalavimas	Teisinis pagrindas	Patikros procedūra	Pagrindžiantis dokumentas
1	2	3	4	5
1.	Vartotojų autentifikavimo, taikant vieningojo prisijungimo sistemą (angl. SSO) sprendimus užtikrinimas.	NKSC rekomendacijų Raudonos CIS kontrolės įmonėms 5 ir 6 punktai.	Pirkėjas šio reikalavimo atitiktį tikrins pasitelkdamas technines priemones. Techninės priemonės: Tiekėjas turi pademonstruoti, kad vartotojų autentifikavimas vyksta taikant vieningojo prisijungimo sistemą (angl. SSO).	Reikalavimo atitikimui Tiekėjas pateikia: Techninės priemonės: demonstracijos įrašus ir (ar) ekrano nuotraukas. Pirkėjas, įvertinęs Tiekėjo pateiktų dokumentų visumą ir informaciją, pateikia Atitikties patvirtinimų tikrinimo aktą.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

14. Tiekėjas privalo nedelsdamas, bet ne vėliau kaip per 1 darbo dieną nuo sužinojimo momento, informuoti Pirkėją apie:

14.1. bet kokį su Pirkimo objektu susijusį Kibernetinį incidentą;

14.2. nustatytus pažeidžiamumus ar saugumo spragas;

14.3. aplinkybes, galinčias turėti įtakos Kibernetinio saugumo reikalavimų ir (ar) Papildomų kibernetinio saugumo reikalavimų (jeigu taikoma) laikymuisi.

15. Tiekėjas privalo nedelsdamas imtis priemonių Kibernetiniam incidentui suvaldyti, jo pasekmėms sumažinti ir užkirsti kelią pasikartojimui, nepriklausomai nuo atskiro Pirkėjo nurodymo.

16. Pasikeitus teisės aktams ar atsiradus naujiems privalomiems kibernetinio saugumo reikalavimams, Tiekėjas privalo užtikrinti, kad Pirkimo objektas būtų pritaikytas taip, kad atitiktų naujus reikalavimus, jeigu tokie reikalavimai yra susiję su Sutarties dalyku.

17. Bet kokios abejonės dėl šio Priedo nuostatų aiškinimo sprendžiamos taip, kad būtų užtikrintas aukštesnis Pirkimo objekto Kibernetinio saugumo lygis ir maksimaliai apsaugoti Pirkėjo interesai.

18. Šiame Priede nustatytų Kibernetinio saugumo reikalavimų vykdymas neatleidžia Tiekėjo nuo atsakomybės laikytis kitų Sutartyje ar teisės aktuose nustatytų pareigų.

KIBERNETINIO SAUGUMO ĮSIPAREIGOJIMAI

Šalys įsipareigoja laikytis kibernetinio saugumo užtikrinimo sąlygų (ta apimtimi, kiek tai susiję su Sutarties vykdymu):

1. Personalo kvalifikacija ir mokymai

1.1. Šalys užtikrina, kad Sutartį vykdantys darbuotojai, įskaitant Tiekėjo pasitelktus subtiekėjo darbuotojus, būtų kompetentingi, turėtų reikiamus įgūdžius bei atitiktų galiojančių teisės aktų ir profesinių standartų reikalavimus.

1.2. Šalys prisiima atsakomybę už darbuotojų kvalifikacijos palaikymą – organizuoja periodinius mokymus, žinių atnaujinimą ir užtikrina, kad kompetencija būtų pakankama saugiam ir kokybiškam Sutarties vykdymui.

2. Pranešimas apie incidentus

2.1. Viena Šalis, sužinojusi apie kibernetinį incidentą, kaip jis apibrėžtas Lietuvos Respublikos kibernetinio saugumo įstatyme (toliau – **KSĮ**), Šalis privalo informuoti kitą Šalį nedelsdama, bet ne vėliau kaip per 24 valandas nuo sužinojimo momento.

2.2. Šalys bendradarbiauja atliekant incidento tyrimą ir, esant poreikiui, įgyvendina papildomas saugumo priemones, proporcingas nustatytai rizikai ir techniškai pagrįstas.

3. Informacijos teikimas apie sutrikimus

3.1. Šalys įsipareigoja viena kitai pateikti išsamią informaciją apie visus incidentus, sutrikimus ar gedimus, įskaitant jų priežastis, poveikį, pašalinimo veiksmus ir prevencines priemones.

3.2. Šalis incidento tyrimo laikotarpiu ataskaitos teikiamos reguliariai, bet ne rečiau kaip kartą per 30 kalendorinių dienų, iki incidento uždarymo.

4. Audito teisė ir priežiūra

4.1. Pirkėjas turi teisę vertinti Tiekėjo taikomas saugumo priemones ir jų atitiktį teisės aktų reikalavimams.

4.2. Šalys privalo sudaryti sąlygas auditui, įskaitant:

4.2.1. prieigos suteikimą prie reikalingų sistemų ir infrastruktūros,

4.2.2. visos reikšmingos informacijos pateikimą,

4.2.3. nustatytų trūkumų pašalinimą per suderintą terminą.

4.3. Neeilinis auditas gali būti atliekamas, jei kyla pagrįstų abejonių dėl atitikties arba įvyksta reikšmingas saugumo incidentas.

5. Konfidencialumas

Visa informacija ir dokumentai, kuriais Šalys keičiasi remiantis šiuo Priedu, laikomi konfidencialiais ir negali būti atskleidžiami tretiesiems asmenims, išskyrus teisės aktų nustatytus atvejus.

6. Loginės prieigos valdymas

6.1. Standartinė (pirmo lygio) prieiga

6.1.2. Kiekvienam naudotojui suteikiami individualūs prisijungimo duomenys.

6.1.3. Taikoma daugiafaktorinė autentifikacija (MFA).

6.1.4. Prieiga ribojama pagal nustatytus IP adresus.

6.1.5. Teisės suteikiamos vadovaujantis mažiausių privilegijų principu.

6.2. Administracinė (antro lygio) prieiga

6.2.1. Naudojami unikalūs prisijungimo duomenys ir MFA.

6.2.2. Prisijungimas vykdomas tik per saugų VPN ryšį.

6.2.3. Taikoma privilegijuotos prieigos kontrolė.

6.2.4. Visi administraciniai veiksmai registruojami ir stebimi.

7. Techninės ir organizacinės saugumo priemonės (taikoma ta apimtimi, kiek tai susiję su Sutarties vykdymu)

Tiekėjas užtikrina, kad būtų įgyvendintos šios priemonės:

7.2.1. Reguliarūs programinės įrangos atnaujinimai ir palaikymas;

7.2.2. Centralizuotas prieigų ir paskyrų valdymas;

7.2.3. IT turto apskaita ir inventorizacija;

7.2.4. Reguliarus atsarginių kopijų darymas ir testavimas;

7.2.5. Duomenų šifravimas perdavimo ir saugojimo metu;

7.2.6. Tinklo segmentavimas, ugniasienės, IDS/IPS ir saugūs protokolai;
7.2.7. Apsauga nuo kenkėjiškos programinės įrangos;
7.2.8. Pažeidžiamumų identifikavimas ir šalinimas;
7.2.9. Incidentų valdymo planas ir praktinės pratybos;
7.2.10. Periodinis įsilaužimo testavimas;
7.2.11. Auditų žurnalų rinkimas ir saugojimas ne trumpiau kaip 90 dienų;
7.2.12. Leistinos programinės įrangos kontrolė;
7.2.13. Duomenų klasifikavimo ir apsaugos priemonės;
7.2.14. Saugios konfigūracijos valdymas;
7.2.15. Kibernetinės higienos mokymai visiems darbuotojams;
7.2.16. Trečiųjų šalių rizikos vertinimas;
7.2.17. Saugus programinės įrangos kūrimo procesas (jei taikoma);
7.2.18. Nuotolinės prieigos kontrolė per VPN su MFA;
7.2.19. Fizinės patalpų apsaugos priemonės ir 24/7 stebėsena (jei taikoma).

8. Sertifikavimas

Šalys numato, kad Tiekėjas turi dėti maksimalias pastangas, jog paslaugų teikimo laikotarpiu paslaugas teiktų pagal LST EN ISO/IEC 27001 standartą „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ arba EN ISO/IEC 27001 standartą „Information security, cybersecurity and privacy protection — Information security management systems — Requirements“ arba lygiavertį standartą, arba savo veikloje įsidiegtų priemones, atitinkančias nurodytą standartą.

9. Bendradarbiavimas su institucijomis

Tiekėjas teikia reikalingą informaciją kompetentingoms institucijoms, jei to reikalauja teisės aktai, ir bendradarbiauja su Pirkėju vykdant tokius įsipareigojimus.

10. Tiekėjo veiksmai pasibaigus Sutarčiai

Pasibaigus paslaugų teikimui ar nutraukus Sutartį Tiekėjas:

1. Išsaugo su Paslaugomis susijusius audito įrašus ne trumpiau kaip 90 dienų nuo Paslaugų teikimo pabaigos;
2. Pirkėjo prašymu pateikia juos struktūruotu ir kompiuteriu skaitomu formatu;
3. Saugiai sunaikina arba grąžina visus Pirkėjo duomenis.