PATVIRTINTA
Lietuvos kalėjimų tarnybos direktoriaus
2026 m. gegužės 18 d. įsakymu Nr. V-473

TIEKIMO GRANDINĖS SAUGUMO VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tiekimo grandinės saugumo valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos kalėjimų tarnybos (toliau – Tarnyba) trečiųjų šalių teikiamoms paslaugoms, produktams, techninei ir programinei įrangai, debesijos paslaugoms bei priežiūros darbams, susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir kibernetinio saugumo užtikrinimu, taikomus kibernetinio saugumo, kokybės, patikimumo, prieigos kontrolės ir tiekimo grandinės rizikų valdymo reikalavimus.

2. Aprašas taikomas, kai Tarnyba planuoja bendradarbiauti, vykdo viešuosius pirkimus, sudaro sutartis, perka paslaugas, programinę ar techninę įrangą, debesijos sprendimus, licencijas, ryšio paslaugas, priežiūros ar vystymo darbus. Aprašas taip pat taikomas vykdant bendrus projektus su trečiosiomis šalimis, kurių veikla tiesiogiai arba netiesiogiai susijusi su Tarnybos tinklų ir informacinių sistemų veikimu, duomenų saugumu ar kibernetinio saugumo užtikrinimu.

3. Apraše vartojamos sąvokos:

3.1. **„Būtina žinoti“** – minimalus informacijos kiekis, kuris būtinas trečiajai šaliai tinkamai suteikti paslaugą, atlikti darbus, pateikti prekes arba įgyvendinti techninius sprendimus;

3.2. **Darbuotojas** – Tarnybos valstybės tarnautojas, pareigūnas ir darbuotojas, dirbantis pagal darbo sutartį;

3.3. **Kibernetinio saugumo vadovas** – Tarnybos direktoriaus įsakymu paskirtas tiesiogiai jam atskaitingas darbuotojas arba paslaugos teikėjas, su kuriuo yra sudaryta kibernetinio saugumo vadovo paslaugų teikimo sutartis, atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą, rengia arba dalyvauja rengiant informacijos saugumo politiką ir ją papildančius dokumentus bei prižiūri ir koordinuoja informacijos saugumo valdymo sistemos įgyvendinimą Tarnyboje;

3.4. **Paslaugų teikimo lygio susitarimas** (angl. *Service Level Agreement, SLA*) – Tarnybos ir trečiosios šalies sutartyje arba jos prieduose nustatyti paslaugų kokybės, prieinamumo, reagavimo į incidentus, atkūrimo terminų, atsarginių kopijų, priežiūros, žurnalinių įrašų, saugos priemonių ir kitų paslaugų teikimo rodiklių reikalavimai;

3.5. **Saugos įgaliotinis** – Tarnybos direktoriaus įsakymu paskirtas Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atsakingas už Tarnybos informacinių išteklių atitiktį Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

3.6. **Saugumo operacijų centras** (toliau – SOC) – Tarnybos direktoriaus ar jo įgalioto asmens paskirtas asmuo ar grupė, taip pat – paslaugas teikianti trečioji šalis, atsakinga už žurnalinių įrašų ir kibernetinių incidentų stebėjimą ir valdymą;

3.7. **Sutartis** – tarp Tarnybos ir trečiosios šalies sudaryta paslaugų, darbų, licencijų, techninės ar programinės įrangos, debesijos sprendimų, ryšio paslaugų, priežiūros, vystymo, SOC, audito ar

kitų su tinklų ir informacinėmis sistemomis susijusių paslaugų teikimo sutartis;

3.8. **Tinklų ir informacinė sistema** (toliau – TIS) – Tarnybos valdomi elektroninių ryšių tinklai, serveriai, duomenų bazės, dokumentų valdymo sistemos, Microsoft 365 aplinka, virtualizacijos sprendimai, saugyklos, rezervinių kopijų sprendimai, perimetro apsaugos priemonės, darbo vietos ir kitos informacinės sistemos bei jų komponentai;

3.9. **Trečioji šalis** – išorinis juridinis ar fizinis asmuo, viešojo pirkimo laimėtojas, rangovas, paslaugų teikėjas, programinės įrangos gamintojas, debesijos tiekėjas, ryšio operatorius, priežiūros paslaugų tiekėjas arba kitas subjektas, kuris pagal sutartį teikia Tarnybai su TIS, duomenimis ar kibernetiniu saugumu susijusias paslaugas, produktus ar darbus, taip pat paslaugų teikėjas, klientas, kiti asmenys ir organizacijos, turintys ar galintys turėti prieigą prie Tarnybos informacijos ir (ar) Tarnybos informacinių išteklių.

4. Kitos Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos viešųjų pirkimų įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir kituose minėtus įstatymus įgyvendinančiuose ar Tarnybos veiklą reglamentuojančiuose teisės aktuose.

II SKYRIUS
TREČIŲJŲ ŠALIŲ ATITIKTIES VALDYMAS

5. Trečiosioms šalims taikomi kibernetinio saugumo, prieigos kontrolės, paslaugų patikimumo ir tiekimo grandinės rizikų valdymo reikalavimai nustatomi vadovaujantis šiuo Aprašu, Tarnybos vidaus teisės aktais ir aktualiais teisės aktais:

5.1. Lietuvos Respublikos kibernetinio saugumo įstatymu.

5.2. Kibernetinio saugumo reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau - Kibernetinio saugumo reikalavimų aprašas).

5.3. Tarnybos informacijos saugumo politikos, prieigų valdymo, žurnalinių įrašų valdymo, incidentų valdymo, veiklos tęstinumo, atsarginių kopijų ir kitais vidaus teisės aktais.

5.4. Tarptautiniais gerosios praktikos standartais, įskaitant ISO/IEC 27001, ISO/IEC 27002, ISO 22301, CIS Controls, OWASP ir kitus su paslaugos pobūdžiu susijusius standartus.

6. Kiekviena trečioji šalis, kurios paslaugos, darbai, licencijos, infrastruktūra ar techniniai sprendimai turi sąsają su Tarnybos tinklų ir informacinėmis sistemomis, privalo atitikti Apraše nustatytus reikalavimus:

6.1. Šie reikalavimai turi būti perkeliami į viešojo pirkimo dokumentus, technines specifikacijas, kvalifikacinius reikalavimus, sutartis, SLA priedus, konfidencialumo susitarimus ir prieigos suteikimo procedūras.

6.2. Sutartyse turi būti aiškiai nustatyti paslaugų prieinamumo, reagavimo į incidentus, prieigų valdymo, žurnalinių įrašų saugojimo, atsarginių kopijų, pažeidžiamumų šalinimo, duomenų apsaugos, konfigūracijų keitimo ir veiklos tęstinumo reikalavimai.

6.3. Jei trečioji šalis turi administracinę arba techninę prieigą prie Tarnybos TIS, sutartyse papildomai turi būti nustatyti prieigos ribojimo, autentifikavimo, veiksmų registravimo, pakeitimų derinimo ir prieigų panaikinimo reikalavimai.

7. Prieš sudarant sutartį arba suteikiant prieigą prie Tarnybos TIS, turi būti įvertinta trečiosios šalies atitiktis kibernetinio saugumo reikalavimams:

7.1. Vertinimo metu turi būti įvertinamas tiekėjo patikimumas, techninės kompetencijos, naudojamos saugos priemonės, incidentų valdymo brandumas, veiklos tęstinumo pajėgumai,

naudojami subrangovai ir priklausomybės nuo kitų tiekėjų.

7.2. Esant padidintai rizikai, Tarnyba gali reikalauti papildomų įrodymų, įskaitant saugumo sertifikatus, auditų ataskaitas, SOC ataskaitas, įsilaužimo testavimo (angl. *penetration test*) rezultatus, ISO sertifikatus, veiklos tęstinumo planus ir kitus dokumentus.

III SKYRIUS
KOKYBĖS REIKALAVIMAI TREČIŲJŲ ŠALIŲ TEIKIAMOMS PASLAUGOMS IR (AR) PRODUKTAMS

8. Tarnybos darbuotojai, atsakingi už trečiųjų šalių paslaugų ir (ar) produktų įsigijimo inicijavimą, rengdami technines specifikacijas, užduočių aprašymus, kvalifikacijos reikalavimus, vertinimo kriterijus, sutarties projektus ir kitus pirkimo dokumentus, privalo nustatyti detalius įsigyjamų tinklų ir informacinių sistemų valdymo, priežiūros, kūrimo, diegimo, modernizavimo ir kibernetinio saugumo užtikrinimo paslaugų bei produktų kokybės, saugumo, veiklos tęstinumo ir paslaugų lygio reikalavimus:

8.1. Kokybės vertinimo kriterijai turi apimti ne tik techninę atitiktį, bet ir kibernetinio saugumo, atsparumo, atnaujinimų valdymo, audituojamumo, veiklos tęstinumo bei tiekimo grandinės rizikos aspektus.

8.2. Techninėse specifikacijose turi būti nustatomi konkretūs kokybės rodikliai, įskaitant:

8.2.1. atitiktį techninei specifikacijai ir integracijų reikalavimams;

8.2.2. suderinamumą su Tarnybos naudojamomis sistemomis, įskaitant Microsoft 365, Active Directory, Azure AD, VPN, SIEM, EDR, ugniasienes ir kitą saugumo infrastruktūrą;

8.2.3. testavimo metu nenustatytų kritinių ar aukšto lygio pažeidžiamumų reikalavimą pagal CVSS v3.1;

8.2.4. dokumentacijos išsamumą, konfigūracijų aprašus, diegimo instrukcijas, administravimo ir atkūrimo procedūras;

8.2.5. privalomą gamintojo arba tiekėjo palaikymą visą sutarties laikotarpį.

9. Jei perkamos kibernetinio saugumo, SOC, SIEM, infrastruktūros administravimo, debesijos, duomenų centrų, programinės įrangos kūrimo ar kritinių TIS priežiūros paslaugos, tiekėjui turi būti keliami šie minimalūs vadybinių sistemų reikalavimai:

9.1. galiojantis ISO/IEC 27001 sertifikatas informacijos saugumo valdymo sistemai;

9.2. jei teikiamos IT paslaugų valdymo paslaugos – galiojantis ISO/IEC 20000-1 sertifikatas;

9.3. jei paslaugos susijusios su veiklos tęstinumu, rezerviniu duomenų centru, DR ar BC paslaugomis – galiojantis ISO 22301 sertifikatas;

9.4. jei teikiamos programinės įrangos kūrimo paslaugos – saugaus kūrimo gyvavimo ciklo (Secure SDLC) procesų taikymo įrodymai pagal OWASP ASVS, OWASP SAMM, NIST SSDF arba lygiaverčius standartus.

10. Paslaugų lygiui (SLA) turi būti nustatyti ne žemesni kaip šie rodikliai, jei pirkimo objektas susijęs su kritinėmis Tarnybos TIS:

10.1. paslaugos prieinamumas – ne mažiau kaip 99,9 proc. per kalendorinį mėnesį;

10.2. reagavimo laikas:

10.2.1. kritinis incidentas – ne ilgiau kaip 1 valanda;

10.2.2. didelis incidentas – ne ilgiau kaip 4 valandos;

10.2.3. vidutinis incidentas – ne ilgiau kaip 8 darbo valandos;

10.2.4. žemas incidentas – ne ilgiau kaip 1 darbo diena;

10.3. sprendimo laikas:

10.3.1. kritinis incidentas – ne ilgiau kaip 4 valandos;

10.3.2. didelis incidentas – ne ilgiau kaip 1 darbo diena;

10.3.3. vidutinis incidentas – ne ilgiau kaip 3 darbo dienos;

10.4. atsarginių kopijų darymas – ne rečiau kaip kartą per 24 valandas, o kritinėms sistemoms pagal nustatytą RPO;

10.5. mėnesinių SLA ir saugumo ataskaitų teikimas.

11. Sutartyse privalo būti įtvirtinta tiekėjo pareiga:

11.1. nedelsiant diegti gamintojo kritinius saugumo atnaujinimus;

11.2. ne rečiau kaip kartą per 6 mėnesius atlikti pažeidžiamumų skenavimą ir saugumo spragų testavimą;

11.3. ne rečiau kaip kartą per metus atlikti veiklos tęstinumo ir atkūrimo scenarijų išbandymą;

11.4. nedelsiant, bet ne vėliau kaip per 24 valandas informuoti apie didelį kibernetinį incidentą;

11.5. užtikrinti žurnalinių įrašų rinkimą, saugojimą ir perdavimą Tarnybai arba jos SOC.

12. Tiekėjo darbuotojams, turintiems prieigą prie Tarnybos TIS, turi būti keliami kvalifikacijos reikalavimai:

12.1. profesiniai sertifikatai pagal paslaugos pobūdį (pvz., CISSP, CISM, CEH, Microsoft, Cisco, Fortinet, VMware, ITIL, ISO 27001 Lead Implementer / Lead Auditor);

12.2. ne mažesnė kaip 3 metų analogiškų projektų patirtis;

12.3. patirtis dirbant su valstybės informacinėmis sistemomis arba kritine infrastruktūra.

13. Trečioji šalis privalo užtikrinti, kad jos darbuotojai ne rečiau kaip kartą per metus keltų kvalifikaciją kibernetinio saugumo, duomenų apsaugos, incidentų valdymo ir prieigos kontrolės klausimais.

14. Trečiosios šalies prieiga prie Tarnybos TIS suteikiama tik:

14.1. pagal sutartimi aiškiai apibrėžtą paslaugos apimtį;

14.2. minimalių teisių principu;

14.3. sutartyje nustatytam terminui;

14.4. naudojant MFA, privilegijuotų paskyrų valdymo priemones ir veiksmų žurnalizavimą.

15. Tiekėjas privalo iš anksto, ne vėliau kaip prieš 30 kalendorinių dienų, informuoti apie:

15.1. naudojamų subrangovų keitimą;

15.2. paslaugų perkėlimą į kitą duomenų centrą ar debesijos regioną;

15.3. paslaugų teikimo jurisdikcijos pasikeitimą;

15.4. esminius techninės architektūros pakeitimus;

15.5. administravimo personalo, turinčio prieigą prie Tarnybos TIS, pasikeitimus.

16. Tarnyba turi teisę atlikti tiekėjo atitikties patikrinimus, auditą, dokumentų peržiūrą, techninių kontrolės priemonių vertinimą ir reikalauti neatitikčių šalinimo plano.

IV SKYRIUS
TREČIŲJŲ ŠALIŲ TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO RIZIKOS VALDYMAS

17. Trečioji šalis, vadovaujantis Kibernetinio saugumo reikalavimų aprašo reikalavimais ne rečiau kaip kartą per metus arba įvykus esminiams organizaciniams ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliam kibernetiniam incidentui, nustatomam pagal Kibernetinių incidentų valdymo planą, turi atlikti TIS kibernetinio saugumo rizikos vertinimą (toliau – Rizikos vertinimas).

18. Tarnybos prašymu trečioji šalis turi neatlygintinai sudaryti sąlygas kibernetinio saugumo vadovui ar saugos įgaliotiniui atlikti TIS kibernetinio saugumo rizikos vertinimą ar kitus kibernetinio saugumo patikrinimo veiksmus potencialių pažeidžiamumų nustatymui.

19. Trečioji šalis neatlygintinai turi pateikti duomenis, kurie reikalingi įsitikinti, jog trečioji šalis atitinka ir laikosi sutartyje, kibernetinį saugumą ir asmens duomenų apsaugą reglamentuojančiuose teisės aktuose ir visuotinai pripažintuose gerosios praktikos standartuose nustatytų reikalavimų.

V SKYRIUS
PRIEIGŲ VALDYMAS

20. Trečiųjų šalių prieigos yra valdomos vadovaujantis Prieigų prie Lietuvos kalėjimų tarnybos tinklų ir informacinių sistemų valdymo tvarkos aprašu, papildomai įgyvendinant Apraše numatytus reikalavimus.

21. Trečioji šalis gali gauti prieigą prie TIS tik pasirašiusi sutartį bei konfidencialumo ir duomenų neatskleidimo įsipareigojimus su Tarnyba, įskaitant abiejų šalių atsakomybes dėl Tarnybos informacijos saugumo reikalavimų įgyvendinimo užtikrinimo bei baudų už įsipareigojimų nevykdymą.

22. Prieigos suteikimo faktas turi būti aprašytas sutartyje nurodant, kaip bus identifikuojami asmenys, kurie turės prieigą, prieigos naudotojų teisės, suteikiamos prieigos laikotarpis ir prieigos aktyvumo periodas (pvz., darbo valandas).

23. Suteikus trečiajai šaliai galimybę dirbti kompiuterinėje darbo vietoje priklausančioje trečiajai šaliai, bei suteikiant nuotolinę prieigą prie TIS, privaloma:

23.1. kompiuterinę darbo vietą sukonfigūruoti taip, jog prisijungti prie TIS būtų galima tik naudojant VPN (angl. *Virtual Private Network*) arba alternatyvią, didesnį ar tą patį saugumą užtikrinančią technologiją;

23.2. įsitikinti, kad trečiosios šalies kompiuterinė darbo vieta ir tinklų bei informacinė sistema, iš kurios jungiamasi nuotoliniu būdu, atitinka ne žemesnius kaip Tarnybos nustatytus kibernetinio saugumo reikalavimus: naudojama gamintojo palaikoma ir laiku atnaujinama operacinė sistema, įdiegta ir nuolat atnaujinama galinių įrenginių apsaugos priemonė (EDR arba antivirusinė programinė įranga), aktyvuota vietinė ugniasienė, taikomas pilnas disko šifravimas, kelių veiksnių autentifikavimas, ribojamos administratoriaus teisės, užtikrinamas automatinis saugumo naujinimų diegimas, įrenginys yra valdomas centralizuotomis saugos politikomis arba lygiavertėmis techninėmis kontrolės priemonėmis;

23.3. užtikrinti nuolatinę prieigos teisių kontrolę;

23.4. vykdyti nuolatinį veiksmų stebėjimą ir kontrolę arba rinkti ir ne trumpiau kaip 6 mėnesius saugoti žurnalinius įrašus apie atliktus veiksmus, užtikrinant jų vientisumą, konfidencialumą ir prieinamumą pagal pareikalavimą;

23.5. užtikrinti Tarnybos viešai neskelbtinos informacijos apsaugą organizacinėmis ir techninėmis priemonėmis;

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

23.7. užtikrinti, kad prisijungimas per nuotolinį ryšį ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „būtina žinoti“ bei turėtų sutartą galiojimo terminą, kuris būtų nurodytas sutartyje;

23.8. kiekvienam vartotojui turi būti sukurtas individualus prisijungimo identifikatorius;

23.9. prisijungdama nuotoline prieiga prie TIS trečioji šalis privalo patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksnių tapatumo nustatymo priemonės, angl. *Multi-factor authentication*);

23.10. prisijungimo slaptažodis trečiajai šaliai privalo būti perduotas atskirai nuo naudotojo prisijungimo identifikatoriaus, naudojant saugius ryšio kanalus.

24. Bet kokia nuotolinė prieiga prie TIS, neatitinkanti šiame Aprašo skyriuje aprašytų reikalavimų yra draudžiama.

25. Pasibaigus sutarties terminui ar pilnai suteikus paslaugas prieš sutarties pasibaigimo terminą, trečiųjų šalių prieigos prie TIS turi būti nedelsiant sustabdytos ir (ar) panaikintos.

VI SKYRIUS
SUTARČIŲ SUDARYMO REIKALAVIMAI

26. Tarnybos darbuotojai, įgyvendindami Tarnybos sutarčių sudarymo ir trečiųjų šalių valdymo procesus, privalo užtikrinti, kad perkant TIS ar kibernetinio saugumo valdymo paslaugas ir (ar) produktus būtų derinamos sutarties sąlygos su organizacijos kibernetinio saugumo vadovu ar saugos įgaliotiniu, siekiant įtraukti kibernetinio saugumo reikalavimus.

27. Tarnybos sutartyse su trečiosiomis šalimis (tiekėjais, įskaitant subtiekėjus), kiek tai susiję su teikiamomis paslaugomis ir (ar) produktais, būtina numatyti:

27.1. trečiosios šalies atitiktį Kibernetinio saugumo reikalavimų aprašo reikalavimams;

27.2. trečiosios šalies personalui reikalingus įgūdžius, mokymus, sertifikatus, kvalifikaciją;

27.3. trečiosios šalies pareigą ne rečiau kaip kartą per metus arba įvykus esminiams trečiosios šalies organizaciniams ar kitiems reikšmingiems pokyčiams, taip pat įvykus dideliam kibernetiniam incidentui atlikti Rizikos vertinimą, parengti ir Tarnybos atsakingiems darbuotojams pateikti rizikos vertinimo ataskaitą ir rizikų valdymo planą;

27.4. trečiosios šalies pareigą pranešti Tarnybai apie visus didelius ir kitus incidentus, susijusius su Tarnybos TIS, kai tik trečioji šalis sužino apie incidentą, ir neatlygintinai pateikti Tarnybai kibernetinio incidento tyrimo ataskaitą pagal Lietuvos kalėjimų tarnybos kibernetinių incidentų valdymo tvarkos aprašą;

27.5. vadovaujantis Kibernetinio saugumo reikalavimų aprašu, suteikti Tarnybai arba jos įgaliotiems paslaugų teikėjams teisę atlikti trečiosios šalies auditą (įskaitant neplaninį);

27.6. trečiosios šalies pareigą neatlygintinai sudaryti sąlygas 27.5. papunktyje numatytam auditui atlikti sutarties vykdymo laikotarpiu ar įvykus dideliam incidentui;

27.7. trečiosios šalies pareigą užtikrinti spragų, keliančių riziką TIS, valdymą;

27.8. trečiosios šalies konfidencialumo ir duomenų neatskleidimo įsipareigojimus pagal Tarnybos direktoriaus patvirtintą Tarnybos tinklų ir informacinių sistemų turto valdymo tvarkos aprašą;

27.9. trečiajai šaliai taikomą SLA;

27.10. apibrėžti trečiosios šalies prieigos (loginės ir fizinės) prie TIS lygius ir sąlygas pagal šio Aprašo V skyriaus nuostatas;

27.11. numatyti reikalavimus, keliamus trečiosios šalies patalpoms, įrangai, TIS priežiūrai, informacijos perdavimui tinklais;

27.12. numatyti trečiosios šalies ir Tarnybos teises ir pareigas.

28. Tarnyba su interneto, duomenų perdavimo, MPLS, VPN, rezervinio ryšio ar kitų elektroninių ryšių paslaugų teikėju, kai šios paslaugos yra būtinos Tarnybos tinklų ir informacinių sistemų, saugumo priemonių ar kritinių paslaugų veikimui užtikrinti, privalo būti sudariusi sutartį (-

is), kurioje (-iose) numatyta:

28.1. reagavimas į kritinius kibernetinius incidentus ir ryšio sutrikimus nepertraukiamai, 24 valandas per parą, 7 dienas per savaitę, įskaitant poilsio ir švenčių dienas;

28.2. nepertraukiamas paslaugos teikimas 24 valandas per parą, 7 dienas per savaitę, užtikrinant ne mažesnį kaip 99,9 proc. mėnesinį prieinamumą;

28.3. paslaugos sutrikimų, našumo problemų, ryšio degradacijos ir saugumo incidentų registravimas bei eskalavimas 24 valandas per parą, 7 dienas per savaitę;

28.4. apsaugos nuo Tarnybos tinklų ir informacinių sistemų trikdymo atakų (DoS / DDoS) priemonių taikymas, įskaitant automatinį srauto filtravimą, srauto nukreipimą, anomalijų stebėseną ir atakų švelninimą;

28.5. rezervinių ryšio kanalų, alternatyvių maršrutų arba automatinio persijungimo (angl. *failover*) mechanizmų užtikrinimas kritinėms Tarnybos paslaugoms;

28.6. paslaugos teikėjo pareiga nedelsiant, bet ne vėliau kaip per 1 valandą, informuoti Tarnybos atsakingus asmenis apie nustatytą ryšio saugumo incidentą, paslaugos trikdymą, neįprastą srauto aktyvumą ar kitą grėsmę;

28.7. ryšio paslaugos žurnalinių įrašų, srauto analizės duomenų ir incidentų įrodymų saugojimas ne trumpiau kaip 6 mėnesius ir jų pateikimas Tarnybai arba jos įgaliotam SOC pagal pareikalavimą;

28.8. paslaugos teikėjo pareiga bendradarbiauti su Tarnyba, Nacionaliniu kibernetinio saugumo centru ir kitomis kompetentingomis institucijomis, kai incidentas daro poveikį Tarnybos kritinėms funkcijoms.

VII SKYRIUS
TREČIŲJŲ ŠALIŲ SĄRAŠO VALDYMAS

29. Tarnybos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, rengia ir nuolat atnaujina Trečiųjų šalių sąrašą (Aprašo 1 priedas), kuriame pateikia informaciją apie trečiąją šalį, jos teikiamas paslaugas ar produktus, atsakingus asmenis, sutartį ir joje numatytus pagrindinius SLA bei įvykusius incidentus.

30. Trečiųjų šalių sąrašas turi būti peržiūrimas ir atnaujinamas inicijuojant numatytus informacinių technologijų ir kibernetinio saugumo reikalavimų pakeitimus naujoms sutartims ir pasikeitus sutartims arba kai įvyksta reikšmingi pokyčiai ar reikšmingi incidentai, susiję su trečiosiomis šalimis.

VIII SKYRIUS
TREČIŲJŲ ŠALIŲ INCIDENTŲ IR TEIKIAMŲ PASLAUGŲ IR (AR) PRODUKTŲ KOKYBĖS VALDYMAS

31. Atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą Tarnybos darbuotojai, gavę informaciją apie incidentą iš trečiosios šalies, Trečiųjų šalių incidentų valdymo registre (Aprašo 2 priedas) turi fiksuoti pas trečiąsias šalis įvykusius incidentus, susijusius su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais. Kibernetinio saugumo vadovas ar saugos įgaliotinis privalo pateikti Tarnybos darbuotojui, atsakingam už sutarties įgyvendinimą, reikiamą informaciją apie įvykusius trečiųjų šalių incidentus, kurie turėjo įtakos Tarnybos naudojamomis trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais.

32. Tarnybos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, turi įrašyti Trečiųjų šalių sąraše užfiksuotus trečiųjų šalių SLA neatitikimus, susijusius su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais, vertinti šiuos SLA neatitikimus bei nutarti, ar šie neatitikimai Tarnybai yra priimtini. Nustačius, kad trečiųjų šalių neatitikimai Tarnybai yra nepriimtini, Tarnybos darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, turi inicijuoti sutartyje numatytų sankcijų taikymą ir (ar) sutarties su trečiąja šalimi nutraukimą.

33. Kibernetinio saugumo vadovas ar saugos įgaliotinis periodiškai (ne rečiau kaip vieną kartą per ketvirtį) turi vertinti Trečiųjų šalių sąraše ir Trečiųjų šalių incidentų valdymo registre fiksuotus incidentus, susijusius su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais bei nutarti, ar rizika, kilusi dėl pas trečiąsias šalis įvykusių incidentų, susijusių su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais, Tarnybai vis dar yra priimtina. Nustačius, kad pas trečiąsias šalis įvykę incidentai Tarnybai yra nepriimtini, kibernetinio saugumo vadovas turi inicijuoti sutartyje numatytų sankcijų taikymą ir (ar) sutarties su trečiąja šalimi nutraukimą.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

34. Sutartyse dėl paslaugų ar produktų pirkimo turi būti aiškiai numatyta, kad šio Aprašo reikalavimai yra neatskiriama ir privaloma sutarties dalis. Kai tai būtina dėl paslaugų pobūdžio, papildomų saugumo kontrolės priemonių, subrangovų naudojimo, debesijos paslaugų, nuotolinės prieigos ar kitų specifinių sąlygų, Tarnyba ir trečioji šalis gali sudaryti papildomus susitarimus, detalizuojančius šio Aprašo reikalavimų įgyvendinimą.

35. Šio Aprašo reikalavimai trečiajai šaliai galioja visą sutarties galiojimo laikotarpį, įskaitant paslaugų pereinamąjį laikotarpį, duomenų grąžinimo, sunaikinimo, prieigų panaikinimo, atsarginių kopijų perdavimo ir kitus užbaigimo veiksmus, jei tokie veiksmai numatyti sutartyje.

36. Jei kuri nors šio Aprašo nuostata tampa negaliojanti arba negali būti taikoma dėl pasikeitusių imperatyvių teisės aktų, Nacionalinio kibernetinio saugumo centro reikalavimų, viešųjų pirkimų reguliavimo ar kitų privalomų norminių nuostatų, ji nedelsiant keičiama ar tikslinama vadovaujantis Tarnybos vidaus dokumentų valdymo ir sutarčių keitimo tvarka, išlaikant maksimaliai artimą pirminiam saugumo tikslui teisinį ir organizacinį rezultatą.

37. Šis Aprašas turi būti peržiūrimas ir, jei reikia, atnaujinamas ne rečiau kaip kartą per metus arba nedelsiant atsiradus esminiams pokyčiams Tarnybos veikloje, tinklų ir informacinių sistemų architektūroje, tiekimo grandinėje, naudojamose technologijose, trečiųjų šalių paslaugų modelyje, teisės aktuose arba po didelio kibernetinio incidento, turėjusio įtakos tiekėjų ar subrangovų paslaugoms. Už šio Aprašo peržiūrą, atnaujinimo inicijavimą ir pakeitimų derinimą yra atsakingas kibernetinio saugumo vadovas.

38. Aprašo peržiūros procesas fiksuojamas Aprašo 3 priede nustatyta tvarka pildant atvejus, kai Aprašas patvirtinamas ir (ar) atnaujinamas.

_____

Tiekimo grandinės saugumo valdymo tvarko
1 priedas

TREČIŲJŲ ŠALIŲ SĄRAŠAS

(Trečiųjų šalių sąrašo forma)

Eil. Nr.	Informacija paie sutartį							Prieiga	Incidentai		Privalomas paslaugų teikimo lygiai (angl. SLA)	
	Trečiosios šalies pavadinimas	**Teikiamos paslaugos ir (ar) produkto pobūdis**	**Trečiosios šalies kontaktinis asmuo**	**Už sutarties vykdymą atsakingas darbuotojas**	**Sutarties numeris**	**Sutarties terminas**	**Kokybės reikalavimai**	**Suteiktos prieigos prie tinklų ir informacinių sistemų**	**Ar įvyko incidentas (Taip/ Ne)**	**Incidentų skaičius**	**Paslaugų prieinamumas proc. (sutartyje)**	**Paslaugų prieinamumas proc. (pagal faktą)**
1	*[Nurodykite trečiosios šalies pavadinimą]*	*[Nurodykite trečiosios šalies teikiamą paslaugą ir (ar) produktą]*	*[Nurodykite trečiosios šalies teikiamą paslaugą ir (ar) produktą]*	*[Už sutarties vykdymą atsakingą darbuotoją]*	*[Nurodykite sutarties numerį]*	*[Nurodykite, kad baisis sutarties galiojimas]*	*[Nurodykite kokybės reikalavimus, pvz. ISO 27001 sertifikatas]*	*[Nurodykite suteiktas prieigas prie tinklų ir informacinių sistemų]*	*[Nurodykite, ar įvyko incidentas (-ai) - Taip arba Ne]*	*[Nurodykite įvykusių incidentų skaičių]*	*[Nurodykite paslaugų prieinąmumą, pvz., 99% per mėnesį ar metus]*	*[Nurodykite koks buvo paslaugų prieinamumas pagal faktą po incidentų]*
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
....												

Tiekimo grandinės saugumo valdymo tvarkos
2 priedas

TREČIŲJŲ ŠALIŲ INCIDENTŲ VALDYMO REGISTRAS

(Trečiųjų šalių incidentų valdymo registro forma)

Eil. Nr.		Informacija apie incidentus				Incidentų valdymas								Trečiosios šalies pagalbos tarnyba	
	Trečiosios šalies pavadinimas	**Eil. Nr.**	**Incidento data**	**Incidento aprašymas**	**Incidento lygis - didelis, nedidelis**	**Reakcijos į incidentą laikas (sutartyje)**	**Reakcijos į incidentą laikas (pagal faktą)**	**Problemų sprendimo laikas (sutartyje)**	**Problemų sprendimo laikas (pagal faktą)**	**Maksimalus leistinas nepasiekiamumo laikas (sutartyje)**	**Maksimali leistina nepasiekiamumo trukmė (pagal faktą)**	**Duomenų atsarginės kopijos atkūrimo laikas (sutartyje)**	**Duomenų atsarginės kopijos ir atkūrimo laikas (pagal faktą)**	**Pagalbos tarnybos darbo valandos (sutartyje)**	**Pagalbos tarnybos kontaktai**
1	*[Nurodykite organizacijos pavadinimą, kurioje įvyko incidentas, pvz., UAB „XXX"]*	1,1	*[Nurodykite incidento datą]*	*[Trumpai apibūdinkite incidentą, pvz., XXX IS nepasiekiama. 50 darbuotojų negali vykdyti darbo funkcijų]*	*[Nurodykite kos incidentas įvyko - didelis arba nedidelis]*	*[Nurodykite reakcijos į incidentą laiką remdamiesi sutarties sąlygomis, pvz., per 30 minučių]*	*[Nurodykite reakcijos į incidentą laiką pagal faktą, pvz., 50 minučių]*	*[Nurodykite problemos sprendimo laiką remdamiesi sutarties sąlygomis, pvz., per 4 valandas]*	*[Nurodykite problemos sprendimo laiką pagal faktą, pvz., per 6 valandas]*	*[Nurodykite maksimalų leistinas nepasiekiamumo laiką remdamiesi sutarties sąlygomis, pvz., 1 val. per mėnesį]*	*[Nurodykite maksimalus nepasiekiamumo laiką pagal faktą po incidento pvz., 2 val.]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką remdamiesi sutarties sąlygomis, pvz., per 12 val]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką pagal faktą po incidento, pvz., per 16 val]*	*[Nurodykite Pagalbos tarnybos darbo valandas, pvz., 24/7 arba 8/5]*	*[Nurodykite Pagalbos tarnybos kontaktus, pvz., tel. xxxxx; Interneto adresas: www.xxxx.xxx]*
		1,2	*[Nurodykite incidento datą]*	*[Eilučių skaičius kuriamas pagal įvykusių incidentų skaičių]*											
		1.3.	*[Nurodykite incidento datą]*	*[Eilučių skaičius kuriamas pagal įvykusių incidentų skaičių]*											
2	*[Nurodykite organizacijos pavadinimą, kurioje įvyko incidentas, pvz., Vīį „XXX"]*	2,1	*[Nurodykite incidento datą]*	*[Trumpai apibūdinkite incidentą, pvz., XXX interneto puslapis neveikia]*	*[Nurodykite kos incidentas įvyko - didelis arba nedidelis]*	*[Nurodykite reakcijos į incidentą laiką remdamiesi sutarties sąlygomis, pvz., per 30 minučių]*	*[Nurodykite reakcijos į incidentą laiką pagal faktą, pvz., 50 minučių]*	*[Nurodykite problemos sprendimo laiką remdamiesi sutarties sąlygomis, pvz., per 4 valandas]*	*[Nurodykite problemos sprendimo laiką pagal faktą, pvz., per 6 valandas]*	*[Nurodykite maksimalų leistinas nepasiekiamumo laiką remdamiesi sutarties sąlygomis, pvz., 1 val. per mėnesį]*	*[Nurodykite maksimalus nepasiekiamumo laiką pagal faktą po incidento pvz., 2 val.]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką remdamiesi sutarties sąlygomis, pvz., per 12 val]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką pagal faktą po incidento, pvz., per 12 val]*	*[Nurodykite Pagalbos tarnybos darbo valandas, pvz., 24/7 arba 8/5]*	*[Nurodykite Pagalbos tarnybos kontaktus, pvz., tel. xxxxx; Interneto adresas: www.xxxx.xxx]*
		2,2	*[Nurodykite incidento datą]*												
3	*[Nurodykite organizacijos pavadinimą, kurioje įvyko incidentas, pvz., AB „XXX"]*	3,1	*[Nurodykite incidento datą]*	*[Trumpai apibūdinkite incidentą, pvz., mtekinti slaptažodžiai]*	*[Nurodykite kos incidentas įvyko - didelis arba nedidelis]*	*[Nurodykite reakcijos į incidentą laiką remdamiesi sutarties sąlygomis, pvz., per 30 minučių]*	*[Nurodykite reakcijos į incidentą laiką pagal faktą, pvz., 50 minučių]*	*[Nurodykite problemos sprendimo laiką remdamiesi sutarties sąlygomis, pvz., per 4 valandas]*	*[Nurodykite problemos sprendimo laiką pagal faktą, pvz., per 6 valandas]*	*[Nurodykite maksimalų leistinas nepasiekiamumo laiką remdamiesi sutarties sąlygomis, pvz., 1 val. per mėnesį]*	*[Nurodykite maksimalus nepasiekiamumo laiką pagal faktą po incidento pvz., 2 val.]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką remdamiesi sutarties sąlygomis, pvz., per 12 val]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką pagal faktą po incidento, pvz., per 12 val]*	*[Nurodykite Pagalbos tarnybos darbo valandas, pvz., 24/7 arba 8/5]*	*[Nurodykite Pagalbos tarnybos kontaktus, pvz., tel. xxxxx; Interneto adresas: www.xxxx.xxx]*
4	*[Nurodykite organizacijos pavadinimą, kurioje įvyko incidentas, pvz., UAB „XXX"]*	4,1	*[Nurodykite incidento datą]*	*[Trumpai apibūdinkite incidentą, pvz., duomenų bazėje dingo klientų asmens duomenys]*	*[Nurodykite kos incidentas įvyko - didelis arba nedidelis]*	*[Nurodykite reakcijos į incidentą laiką remdamiesi sutarties sąlygomis, pvz., per 30 minučių]*	*[Nurodykite reakcijos į incidentą laiką pagal faktą, pvz., 50 minučių]*	*[Nurodykite problemos sprendimo laiką remdamiesi sutarties sąlygomis, pvz., per 4 valandas]*	*[Nurodykite problemos sprendimo laiką pagal faktą, pvz., per 6 valandas]*	*[Nurodykite maksimalų leistinas nepasiekiamumo laiką remdamiesi sutarties sąlygomis, pvz., 1 val. per mėnesį]*	*[Nurodykite maksimalus nepasiekiamumo laiką pagal faktą po incidento pvz., 2 val.]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką remdamiesi sutarties sąlygomis, pvz., per 12 val]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką pagal faktą po incidento, pvz., per 12 val]*	*[Nurodykite Pagalbos tarnybos darbo valandas, pvz., 24/7 arba 8/5]*	*[Nurodykite Pagalbos tarnybos kontaktus, pvz., tel. xxxxx; Interneto adresas: www.xxxx.xxx]*
5															
....															

Tiekimo grandinės saugumo valdymo
tvarkos aprašo
3 priedas

TIEKIMO GRANDINĖS SAUGUMO VALDYMO TVARKOS APRAŠO PERŽIŪRA

(Tiekimo grandinės saugumo valdymo tvarkos aprašo peržiūros forma)

Dokumento versija	Veiklos data	Statusas	Dokumento rengėjas	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____