

UAB „Baltnetos Komunikacijos“

Duomenų tvarkymo sutartis (DTS)

Ši Duomenų tvarkymo sutartis (toliau – „DTS“) reguliuoja asmens duomenų tvarkymą, kurią vykdo UAB „Baltnetos komunikacijos“, veikianti kaip „Duomenų tvarkytojas“ savo kliento, veikiančio kaip „Duomenų valdytojas“, vardu. Ši DTS tampa neatsiejama bendrosios sutarties dalimi bei tampa privaloma Duomenų tvarkytojui ir Duomenų valdytojui pagal 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 (toliau – „GDAR“).

1. Duomenų tvarkymo dalykas, tikslas, pobūdis, asmens duomenų rūšis ir duomenų subjektų kategorijos

- 1.1. Asmens duomenų tvarkymo – kurią atlieka Duomenų tvarkytojas Duomenų valdytojo vardu – pobūdis, dalykas ir tikslas, taip pat informacija, susijusi su tvarkomų asmens duomenų rūšimi bei duomenų subjektų kategorijomis, yra nurodyti šios DTS Prieduose.

2. Duomenų tvarkymo trukmė

- 2.1. Ši DTS taikoma tol, kol Duomenų tvarkytojas tvarko asmens duomenis Duomenų valdytojo vardu.
- 2.2. Duomenų valdytojo prašymu, Duomenų tvarkytojas privalo po šios DTS nutraukimo ar pasibaigimo nutraukti savo vykdomą duomenų tvarkymo veiklą ir – Duomenų valdytojo pasirinkimu ir, jei kitaip nenumato taikomi duomenų apsaugos teisės aktai – turi ištrinti visus asmens duomenis, tvarkomus Duomenų valdytoju vardu, arba gražinti visus asmens duomenis Duomenų valdytojui, kartu ištrinant visas turimas tokių duomenų kopijas.

3. Duomenų tvarkytojo ir Duomenų valdytojo įsipareigojimai

- 3.1. Duomenų tvarkytojas yra įgyvendinęs tinkamas technines bei organizacines priemones, užtikrinančias, kad jo vykdomas asmens duomenų tvarkymas pagal šios DTS nuostatas atitiktų taikomus duomenų apsaugos teisės aktų reikalavimus, konkrečiai – GDAR reikalavimus, ir garantuotų duomenų subjekto teisių apsaugą. Duomenų tvarkytojas yra įsidiegęs paslaugų valdymo sistemą ISO/IEC 20000 ir Informacijos saugos valdymo sistemą ISO/IEC27001:2022 ir kontrolės priemones pagal šio standarto reikalavimus. Duomenų tvarkytojo taikomos techninės ir organizacinės priemonės yra nustatytos DTS 6 priede.
- 3.2. Duomenų tvarkytojas įsipareigoja tvarkyti asmens duomenis tik pagal Duomenų valdytojo pateiktus dokumentais informintus nurodymus, išskyrus atvejus, kai taikomi teisės aktai nustato kitaip. Tokiu atveju, prieš pradėdamas tvarkyti asmens duomenis, Duomenų tvarkytojas, kiek tai leidžia teisės aktai, privalo informuoti Duomenų valdytoją apie tokį teisinį reikalavimą. Jei Duomenų tvarkytojas neturi nurodymų, kaip tvarkyti asmens duomenis konkrečioje situacijoje, arba, jei koks nors Duomenų valdytojo nurodymas pažeidžia taikomą duomenų apsaugos teisės aktą, Duomenų tvarkytojas privalo nedelsdamas apie tai informuoti Duomenų valdytoją. Duomenų valdytojo nurodymai pateikti bendrosios sutarties sąlygose ir šioje DTS.
- 3.3. Duomenų tvarkytojas, atsižvelgdamas į duomenų tvarkymo pobūdį ir galima apimtį panaudodamas tinkamas technines bei organizacines priemones, padeda Duomenų valdytojui įvykdyti Duomenų valdytojo prievolę atsakyti į prašymus pasinaudoti duomenų subjekto teisėmis, nustatytomis GDAR III skyriuje.

- 3.4. Duomenų tvarkytojas, atsižvelgdamas į duomenų tvarkymo pobūdį bei turimą informaciją, padeda Duomenų valdytojui įvykdyti konkrečias prievoles pagal taikomus duomenų apsaugos teisės aktus. Konkrečios prievolės apima duomenų tvarkymo saugumą (BDAR 32 straipsnis), pranešimą apie asmens duomenų saugumo pažeidimą (BDAR 33 – 34 straipsniai) ir poveikio duomenų apsaugai vertinimą bei išankstines konsultacijas (BDAR 35 – 36 straipsniai).
- 3.5. Duomenų tvarkytojas įsipareigoja pateikti Duomenų valdytojui visą informaciją ir suteikti jam visą pagalbą, siekiant įrodyti, kad yra vykdomi pagal šią DTS prisiimti įsipareigojimai, taip pat sudaro sąlygas bei padeda Duomenų valdytojui arba kitam jo įgaliotam auditoriui atlikti auditą, įskaitant patikrinimus vietoje.
- 3.6. Duomenų valdytojas įsipareigoja užtikrinti, kad asmens duomenys būtų tvarkomi laikantis BDAR, kitų asmens duomenų apsaugą ir (ar) tvarkymą reglamentuojančių teisės aktų ir šios DTS. Duomenų valdytojas yra atsakingas už tai, kad asmens duomenų tvarkymas, kurį Duomenų tvarkytojui pavesta atlikti, turėtų teisinį pagrindą.

4. Pagalbiniai duomenų tvarkytojai

- 4.1. Duomenų tvarkytojas turi bendrąjį rašytinį Duomenų valdytojo leidimą, kad jis galėtų pasitelkti pagalbinus duomenų tvarkytojus. Duomenų tvarkytojas raštu informuoja Duomenų valdytoją apie numatomus pakeitimus, susijusius su pagalbinių duomenų tvarkytojų pasitelkimu ar pakeitimu prieš 10 darbo dienų, tokiu būdu Duomenų valdytojui suteikiant galimybę prieštarauti tokiems pakeitimams iki atitinkamo (-ų) pagalbinių (-ų) duomenų tvarkytojo (-ų) pasitelkimo. Aktualus pagalbinių duomenų tvarkytojų sąrašas pateikiamas Duomenų valdytojui jo prašymu arba skelbiamas Duomenų tvarkytojo interneto svetainėje.
- 4.2. Duomenų tvarkytojas užtikrina ir, Duomenų valdytojo prašymu, dokumentais patvirtina, kad pagalbiniai duomenų tvarkytojai yra įsipareigoję pagal rašytines sutartis, pagal kurias jie privalo vykdyti tas pačias duomenų tvarkymo prievoles, kaip yra nustatyta šioje DTS. Duomenų tvarkytojas yra visiškai atsakingas Duomenų valdytojui už pagalbinių duomenų tvarkytojų vykdomus įsipareigojimus.
- 4.3. Duomenų valdytojas gali paprašyti, kad Duomenų tvarkytojas patikrintų pagalbinių duomenų tvarkytoją arba pateiktų patvirtinimą, kad toks patikrinimas buvo atliktas, arba, jei yra tokia galimybė, gautų ar padėtų Duomenų valdytojui gauti išorinio auditoriaus išvadą dėl pagalbinių duomenų tvarkytojo veiklos, siekiant užtikrinti taikomų duomenų apsaugos teisės aktų reikalavimų vykdymą.

5. Duomenų perdavimas į trečiąsias šalis

- 5.1. Įsipareigojimas tvarkyti asmens duomenis pagal DTS gali būti vykdomas tik Europos Sąjungos (ES) valstybėje narėje arba Europos ekonominės erdvės (EEE) valstybėje narėje. Bet koks asmens duomenų perdavimas į šalį, kuri nėra ES ar EEE valstybė narė, gali būti vykdomas tik gavus Duomenų valdytojo išankstinį rašytinį sutikimą ir tik tuo atveju, jei yra įvykdytos specialios sąlygos, nurodytos taikomuose duomenų apsaugos teisės aktuose, BDAR V skyriuje.
- 5.2. Duomenų valdytojas gali bet kada atšaukti savo sutikimą dėl duomenų perdavimo į trečiąsias šalis pagal šios DTS 5.1 punktą. Tokiu atveju, Duomenų tvarkytojas privalo iškart nutraukti duomenų perdavimą ir, Duomenų valdytojui prašant, pateikti rašytinį tokio nutraukimo patvirtinimą.

6. Informacijos saugumas ir konfidencialumas

- 6.1. Duomenų tvarkytojas užtikrina tinkamą asmens duomenų apsaugą pagal šią DTS su tikslu apsaugoti asmens duomenis nuo sunaikinimo, pakeitimo, neteisėto platinimo arba neteisėtos prieigos. Asmens duomenys taip pat saugomi nuo kitokio pobūdžio neteisėto tvarkymo.
- 6.2. Duomenų tvarkytojas parengia ir nuolat atnaujina savo techninių, organizacinių ir fizinių priemonių aprašymą, kad šis atitiktų taikomų duomenų apsaugos teisės aktų reikalavimus.
- 6.3. Be Duomenų valdytojo išankstinio rašytinio sutikimo Duomenų tvarkytojas įsipareigoja neatskleisti pagal šią DTS tvarkomų asmens duomenų ar kitaip neleisti su jais susipažinti jokiai trečiajai šaliai, išskyrus pagalbinius duomenų tvarkytojus, kurie pasitelkiami pagal šią DTS.
- 6.4. Duomenų tvarkytojas užtikrina, kad visi prieigą prie Duomenų valdytojo vardu tvarkomų asmens duomenų turintys asmenys būtų įsipareigoję užtikrinti konfidencialumą arba, kad jiems būtų taikoma atitinkama įstatymais nustatyta konfidencialumo prievolė.

7. Taikoma teisė ir ginčų sprendimas

- 7.1. Ši DTS yra sudaryta ir aiškinama vadovaujantis šios DTS Prieduose nurodytoje jurisdikcijoje galiojančiais įstatymais, išskyrus kolizinės teisės principus, kuomet priešingu atveju gali būti taikomos kitos teisės normos.
- 7.2. Šalys susitaria, kad vienintelė ir išimtinė jurisdikcija bei vieta, kurioje nagrinėjami visi iš šios DTS kylantys ginčai, yra sutartos jurisdikcijos teismas.

8. Atsakomybės ribojimas ir nuostolių atlyginimas

- 8.1. Jei nesusitariama kitaip, šalys atsako pagal DTS 7 skyriuje nurodytas bendrąsias taikomas teisės normas. Nepaisant to, kas nurodyta aukščiau, šalys neprisiima atsakomybės už eksploatacinius nuostolius, pelno netekimą, prestižo praradimą, bet kokius kitus netiesioginius nuostolius ir jų padarinių žalą. Duomenų praradimas laikomas netiesioginiu nuostoliu.
- 8.2. Bendra Duomenų tvarkytojo atsakomybė pagal šią DTS bet kuriuo atveju ribojama paskutinių 6 (šešių) mėnesių atlygio, sumokėto už paslaugas ir šia DTS prisiimtus įsipareigojimus ir atitinkamu metu apskaičiuoto nuo ginčo dalyko atsiradimo momento, dydžiu. Jei praėjo mažiau kaip 6 (šeši) mėnesiai, sumokėtas atlygis yra laikomas vidutinis sumokėtas atlygis, padaugintas iš 6 (šešių) mėnesių.

Duomenų tvarkymo sutarties Priedas Nr. 1 Serverių ir kompiuterių priežiūros paslaugoms

Duomenų tvarkymo dalykas ir tikslas	Toliau nurodytų Duomenų tvarkytojo paslaugų ar užduočių teikimas Duomenų valdytojui: Serverių ir kompiuterių priežiūros paslaugos
Tvarkomų asmens duomenų rūšys	Tvarkomi asmens duomenys apima asmeninę dalykinę kontaktinę informaciją, tokią kaip vardas, pavardė, telefono numeris arba mobiliojo telefono numeris, elektroninio pašto adresas ir slaptažodžiai; darbovietes, asmens kodus
Duomenų subjektų kategorijos	Duomenų valdytojo atstovai ir galutiniai vartotojai, tokie kaip darbuotojai, kandidatai į darbo vietą, rangovai, bendradarbiai, partneriai, taip pat Duomenų valdytojo klientai, ligoninės pacientai ir kiti asmenys, kurie turi būti suvesti į centrinę duomenų valdytojo sistemą
Duomenų tvarkymo veikla	Asmens duomenų suvedimas, koregavimas ir trynimasis, taip pat serverių, kuriuose gali būti asmens duomenys atsarginių kopijų darymas ir saugojimas ne ilgiau nei duomenų valdytojas nusipirkęs atsarginių kopijų paslaugą
Pagalbinių duomenų tvarkytojų sąrašas	Nėra
Jurisdikcija	Lietuva

Duomenų tvarkymo sutarties Priedas Nr. 2 Resursų nuomos paslaugoms

Duomenų tvarkymo dalykas ir tikslas	Toliau nurodytų Duomenų tvarkytojo paslaugų ar užduočių teikimas Duomenų valdytojui: Resursų nuomos paslaugos
Tvarkomų asmens duomenų rūšys	Tik duomenų valdytojo kontaktinė informacija, vardas, pavardė, pareigos, telefono numeris, mobilus telefono numeris, elektroninis adresas, šifruotas slaptažodis prisijungimui į valdymo panelę
Duomenų subjektų kategorijos	Duomenų valdytojo atstovai
Duomenų tvarkymo veikla	Virtualių mašinų atsarginių kopijų darymas pagal kliento nusipirktą atsarginių kopijų atlikimo paslaugą
Pagalbinių duomenų tvarkytojų sąrašas	Nėra
Jurisdikcija	Lietuva

Duomenų tvarkymo sutarties Priedas Nr. 3 Svetainių talpinimo ir virtualių dedikuotų serverių paslaugoms

Duomenų tvarkymo dalykas ir tikslas	Toliau nurodytų Duomenų tvarkytojo paslaugų ar užduočių teikimas Duomenų valdytojui: Svetainių talpinimo ir virtualių dedikuotų serverių paslaugos
Tvarkomų asmens duomenų rūšys	Tik duomenų valdytojo kontaktinė informacija, vardas, pavardė, pareigos, telefono numeris, mobilus telefono numeris, elektroninis adresas, šifruotas slaptažodis prisijungimui į valdymo panelę

Duomenų subjektų kategorijos	Duomenų valdytojo atstovai
Duomenų tvarkymo veikla	Virtualių mašinų ir svetainių atsarginių kopijų darymas bei saugojimas ne ilgiau nei 14 dienų
Pagalbinių duomenų tvarkytojų sąrašas	Nėra
Jurisdikcija	Lietuva

Duomenų tvarkymo sutarties Priedas Nr. 4 Telefonijos paslaugoms

Duomenų tvarkymo dalykas ir tikslas	Toliau nurodytų Duomenų tvarkytojo paslaugų ar užduočių teikimas Duomenų valdytojui: Telefonijos paslaugos
Tvarkomų asmens duomenų rūšys	Duomenų valdytojo kontaktinė informacija, vardas, pavardė, pareigos, telefono numeris, mobilus telefono numeris, elektroninis adresas, šifruotas slaptažodis prisijungimui į valdymo panelę. Duomenų valdytojo klientų/partnerių skambučių informacija, laikas, trukmė, į kokį numerį skambinta (CDR'ai), vardas, pavardė, elektroninio pašto adresas, pareigos
Duomenų subjektų kategorijos	Duomenų valdytojo atstovai, duomenų valdytojo klientai
Duomenų tvarkymo veikla	Skambučių CDR įrašų saugojimas ne ilgiau nei 6 mėn.
Pagalbinių duomenų tvarkytojų sąrašas	Nėra
Jurisdikcija	Lietuva

Duomenų tvarkymo sutarties Priedas Nr. 5 bendrai visoms paslaugoms

Duomenų tvarkymo dalykas ir tikslas	Toliau nurodytų Duomenų tvarkytojo paslaugų ar užduočių teikimas Duomenų valdytojui: paslaugų teikimas – Duomenų subjekto paslaugų pirkimo (užsakymo) apdorojimui, administravimui, užklausų apdorojimui; Duomenų subjekto identifikavimui Duomenų tvarkytojo informacinėse sistemose
Tvarkomų asmens duomenų rūšys	Tik duomenų valdytojo kontaktinė informacija, vardas, pavardė, pareigos, asmens kodas, telefono numeris, mobilus telefono numeris, elektroninis adresas, šifruotas slaptažodis prisijungimui į valdymo panelę
Duomenų subjektų kategorijos	Duomenų valdytojo atstovai
Duomenų tvarkymo veikla	Asmens duomenų suvedimas, koregavimas ir trynimasis, taip pat serverių, kuriuose gali būti asmens duomenys, atsarginių kopijų darymas ir saugojimas
Pagalbinių duomenų tvarkytojų sąrašas	Nėra
Jurisdikcija	Lietuva

Priedas Nr. 6 Duomenų tvarkytojo taikomos techninės ir organizacinės priemonės

Duomenų tvarkytojas organizacijoje yra įsodiegęs paslaugų valdymo sistemą ISO/IEC 20000 ir Informacijos saugos valdymo sistemą ISO/IEC 27001:2022, kur techninių ir organizacinių priemonių sąrašas yra platesnis. Čia išvardintos pagrindinės asmens duomenų apsaugai taikomos priemonės:

A. ORGANIZACINĖS PRIEMONĖS

1. Informacijos saugumo politika

Organizacijoje patvirtinta, dokumentuota ir darbuotojams komunikuota informacijos saugumo politika, apimanti asmens duomenų konfidencialumo, vientisumo ir prieinamumo užtikrinimą. Ji reguliariai peržiūrima (ne rečiau kaip kartą per metus) ir atitinka teisės aktų bei sutarčių reikalavimus.

2. Vaidmenys, atsakomybė ir pareigų atskyrimas

Aiškiai apibrėžti informacijos saugumo vaidmenys ir atsakomybės, užtikrintas nesuderinamų funkcijų atskyrimas. Nustatytos teisių suteikimo ir atšaukimo procedūros bei darbuotojų įsipareigojimai, galiojantys ir pasibaigus darbo santykiams.

3. Išteklių (turto) valdymas

Vykdomas informacijos ir IT turto inventorizavimas (įranga, sistemos, vieta, tiekėjai), paskirti atsakingi savininkai. Nustatytos turto naudojimo taisyklės, o pasibaigus santykiams užtikrinamas turto grąžinimas.

4. Informacijos klasifikavimas ir žymėjimas

Informacija klasifikuojama pagal konfidencialumą, vientisumą ir prieinamumą, o žymėjimas atliekamas pagal nustatytą schemą. Reikalavimai taikomi ir dokumentams bei komunikacijai už sistemų ribų.

5. Grėsmių žvalgyba

Organizacija renka ir analizuoja informaciją apie kibernetines grėsmes, vertina jų aktualumą ir atitinkamai atnaujina saugumo priemones.

6. Informacijos saugumas projektuose

Informacijos saugumas integruojamas į projektų valdymą ir IT sprendimų kūrimo gyvavimo ciklą. Saugumo reikalavimai nustatomi ankstyvuose projektų etapuose.

7. Tiekėjų ir subtvarkytojų santykiai

Valdomos rizikos, susijusios su tiekėjais ir subtvarkytojais, nustatomi saugumo reikalavimai ir jų laikymasis yra stebimas. Subtvarkytojai įpareigoti užtikrinti lygiavertį saugumo lygį ir laiku pranešti apie incidentus.

8. Debesijos paslaugų sauga

Debesijos paslaugų naudojimas reguliuojamas nustatytais procedūromis, o prieš pasirenkant tiekėją atliekamas rizikos vertinimas.

9. Incidentų valdymas

Apibrėžti incidentų identifikavimo, registravimo, tyrimo ir uždarymo procesai. Incidentai dokumentuojami, o įgyta patirtis naudojama saugumo stiprinimui; laikomasi BDAR pranešimo reikalavimų.

10. Verslo tęstinumas ir IRT pasirengimas

Parengti veiklos tęstinumo ir IT atsparumo planai, užtikrinantys sistemų veikimą ir duomenų prieinamumą sutrikimų atveju. Priemonės yra periodiškai testuojamos.

11. Teisės aktų reikalavimų laikymasis ir nepriklausoma peržiūra

Nuolat stebima atitiktis teisės aktams ir vidinėms politikoms, atliekamos reguliarios peržiūros. Atitiktis gali būti pagrindžiama sertifikatais (pvz., ISO/IEC 27001:2022).

B. ŽMONIŲ KONTROLĖS PRIEMONĖS

12. Darbuotojų patikrinimas ir įdarbinimas

Prieš įdarbinant darbuotojus atliekamas proporcingas patikrinimas, o darbo sutartyse nustatomi saugumo įsipareigojimai.

13. Mokymai ir informuotumo didinimas

Darbuotojai reguliariai mokomi informacijos saugumo ir asmens duomenų apsaugos klausimais, atsižvelgiant į jų funkcijas.

14. Drausminės procedūros

Nustatytos formalios drausminės procedūros už saugumo politikos pažeidimus.

15. Pareigos pasibaigus ar pasikeitus darbo santykiams

Užtikrinama, kad konfidencialumo ir kitos saugumo pareigos galiotų ir po darbo santykių pabaigos.

16. Konfidencialumo pasižadėjimai

Darbuotojai ir kitos susijusios šalys pasirašo konfidencialumo susitarimus, kurie reguliariai peržiūrimi.

17. Nuotolinis darbas

Taikomos saugumo priemonės nuotoliniam darbui, užtikrinant duomenų apsaugą ne organizacijos patalpose.

18. Informacijos saugumo įvykių pranešimas

Darbuotojai turi aiškius kanalus ir procedūras pranešti apie saugumo incidentus.

C. FIZINĖS KONTROLĖS PRIEMONĖS

19. Fizinio saugumo perimetras ir prieiga

Užtikrinama fizinė apsauga ir ribota prieiga prie patalpų bei serverių, naudojant kontrolės mechanizmus ir signalizaciją.

20. Fizinės saugos stebėseną

Patalpos stebimos siekiant užkirsti kelią neautorizuotai prieigai.

21. Apsauga nuo fizinių ir aplinkos grėsmių

Įgyvendintos priemonės apsaugai nuo gaisro, elektros sutrikimų ir kitų aplinkos rizikų.

22. Įrangos apsauga ir priežiūra

Įranga tinkamai įrengta, apsaugota ir prižiūrima viso naudojimo laikotarpiu.

23. Švaraus stalo ir ekrano politika

Taikomos taisyklės, užtikrinančios, kad fiziniai ir elektroniniai duomenys nebūtų palikti be priežiūros.

24. Duomenų laikmenų valdymas

Laikmenos valdomos per visą gyvavimo ciklą, taikant apsaugos ir šifravimo priemones.

25. Saugus įrangos šalinimas ir pakartotinis naudojimas

Prieš šalinant ar perduodant įrangą užtikrinamas duomenų sunaikinimas arba saugus ištrynimasis.

D. TECHNOLOGINĖS KONTROLĖS PRIEMONĖS**26. Prieigos valdymas ir autentifikavimas**

Taikomas „būtina žinoti“ principas, valdomas paskyrų gyvavimo ciklas, naudojami stiprūs slaptažodžiai ir daugiafaktorė autentifikacija.

27. Privilegijuotos prieigos teisių valdymas

Privilegijos ribojamos ir stebimos, o prieigos prie kritinių sistemų yra registruojamos ir kontroliuojamos.

28. Apsauga nuo kenkėjiškų programų

Naudojamos antivirusinės priemonės, ribojamas neautorizuotos programinės įrangos naudojimas, užtikrinami atnaujinimai.

29. Techninių pažeidžiamumų valdymas

Reguliariai atliekamas pažeidžiamumų vertinimas ir testavimas, įgyvendinamos taisomosios priemonės.

30. Konfigūracijos valdymas

Valdomos IT sistemų konfigūracijos ir pakeitimai pagal nustatytas procedūras.

31. Galutinių naudotojų įrenginiai ir mobilieji įrenginiai

Užtikrinama įrenginių apsauga, taikomos naudojimo taisyklės, kontroliuojamas BYOD naudojimas ir numatyta galimybė nuotoliniu būdu ištrinti duomenis.

32. Duomenų maskavimas ir pseudonimizavimas

Taikomi duomenų apsaugos metodai, o testavimui naudojami tik nuasmeninti duomenys.

33. Duomenų nutekėjimo prevencija

Stebimas ir kontroliuojamas duomenų perdavimas iš organizacijos tinklo.

34. Atsarginės kopijos

Reguliariai daromos, testuojamos ir saugomos atsarginės kopijos, užtikrinant jų apsaugą ir atkuriamumą.

35. Informacinių sistemų pertekliškumas ir prieinamumas

Užtikrinamas sistemų atsparumas ir pajėgumų planavimas.

36. Žurnalų įrašai, stebėseną ir sinchronizavimas

Registruojami ir analizuojami saugumo įvykiai, žurnalai apsaugoti, o sistemos stebimos.

37. Tinklo sauga

Tinklai segmentuojami, apsaugoti ir naudojami šifruoti ryšiai bei kontrolės priemonės.

38. Kriptografija

Taikomi duomenų šifravimo ir kriptografinių raktų valdymo principai.

39. Programinės įrangos sauga ir kūrimas

Taikomi saugaus kūrimo principai, vykdomas testavimas, atskiriamos aplinkos.

40. Informacijos ištrynimasis

Duomenys ištrinami ar gražinami, kai nebereikalingi.

41. Informacijos perdavimas

Nustatytos saugaus duomenų perdavimo taisyklės visiems kanalams.