TVARKOMŲ ASMENS DUOMENŲ SAUGUMO PRIEMONIŲ IR RIZIKOS ĮVERTINIMO GAIRĖS DUOMENŲ VALDYTOJAMS IR DUOMENŲ TVARKYTOJAMS

3 versija
2020-06-18

Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams (toliau – gairės) parengtos remiantis Europos Sąjungos kibernetinio saugumo agentūros (ENISA) rekomendacijomis („Handbook on Security of Personal Data Processing“, 2018 m.) ir ISO standartais LST ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ bei ISO/IEC 27701:2019 „Saugumo metodai – ISO/IEC 27001 ir ISO/IEC 27002 papildymas dėl privatumo valdymo – Reikalavimai ir gairės“[1].

Dėl gairių taikymo organizacijoje

Prie visų šiose gairėse išvardytų priemonių yra pateikiama nuoroda į susijusį informacijos saugumo valdymo **standarto** LST ISO/IEC 27001:2017 **reikalavimą** ir jį papildantį **privatumo užtikrinimo reikalavimą** pagal ISO/IEC 27701:2019[2]. Paaiškinimai pateikti atsižvelgiant į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos **reglamentą** (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – **BDAR**).

Atkreipiame dėmesį, kad kuriant (diegiant) ar vertinant turimas organizacines ir technines saugumo priemones, organizacijos turi visapusiškai atsižvelgti į „duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus ir riziką, susijusią su pavojais fizinių asmenų teisėms ir laisvėms. BDAR 24 ir 32 straipsniai organizacijas įpareigoja **visais atvejais atlikti rizikos vertinimą**.

[1] Oficialus standarto pavadinimas anglų kalba ISO/IEC 27701:2019 „Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines“.

[2] Atkreiptinas dėmesys, kad dalis terminų, vartojamų BDAR ir standarte ISO/IEC 27701:2019, skiriasi. Taip pat yra nežymių skirtumų tarp šių terminų apibrėžimų. BDAR apibrėžtas terminas „Asmens duomenys“ (angl. *Personal data*) atitinka ISO standarte vartojamą terminą „Asmenį identifikuojanti informacija“ (angl. *Personally Identifiable Information (PII)*), atitinkamai terminas „Duomenų valdytojas“ (angl. *Data controller*) – terminą „Asmens duomenų valdytojas“ (angl. *PII controller*), „Duomenų tvarkytojas“ (angl. *Data processor*)“ – „Asmens duomenų tvarkytojas“ (angl. *PII processor*), „Duomenų subjektas“ (angl. *Data subject*) – „Asmens duomenų subjektas“ (angl. *PII principal*), „Pritaikytoji duomenų apsauga“ (angl. *Data protection by design*) – „Pritaikytasis privatumas“ (angl. *Privacy by design*), „Standartizuotoji duomenų apsauga“ (angl. *Data protection by default*) – „Standartizuotasis privatumas“ (angl. *Privacy by default*).

Gairės parengtos siekiant padėti duomenų valdytojams ir duomenų tvarkytojams, kurie priskiriami prie smulkiojo ar vidutinio verslo subjektų. Gairėmis taip pat gali naudotis ir kitos organizacijos (pvz., viešojo sektoriaus ar didelės įmonės) atsižvelgiant į vykdomos veiklos specifiką.

Gairėse yra pateikiama informacija, kuria gali vadovautis organizacijos, valdančios ir (ar) tvarkančios asmens duomenis (duomenų valdytojai ir duomenų tvarkytojai)[3], atlikdamos duomenų tvarkymo operacijas savo veikloje. Gairės padės įvertinti aktualius pavojus asmens duomenų saugumui ir įgyvendinti tinkamas saugumo priemones.

[3] Nors tekste vietomis yra minimas duomenų valdytojas ar organizacija, tačiau atitinkamos nuostatos yra taikomos ir duomenų tvarkytojams.

Turinys

Rizikos vertinimas 4

1 žingsnis. Duomenų tvarkymo operacijos nustatymas ir jos kontekstas 4

2 žingsnis. Poveikio supratimas ir vertinimas 4

3 žingsnis. Galimų grėsmių nustatymas ir jų atsiradimo tikimybės vertinimas 5

4 žingsnis. Rizikos įvertinimas 7

Organizacinės duomenų saugumo priemonės 9

Techninės duomenų saugumo priemonės 19

Rizikos vertinimas

Šiose gairėse pateiktas rizikos vertinimo požiūris yra paremtas šiais keturiais žingsniais:

1. Duomenų tvarkymo operacijos nustatymas ir jos kontekstas;
2. Poveikio supratimas ir vertinimas;
3. Galimų grėsmių nustatymas ir jų atsiradimo tikimybės vertinimas;
4. Rizikos įvertinimas.

Po rizikos įvertinimo organizacija gali įgyvendinti (ar pasitikrinti jau įgyvendintas) technines ir organizacines saugumo priemones (iš toliau pateikiamo sąrašo), kurios tinka nusistatytam rizikos lygiui. Rizikos vertinimas gali būti atliekamas, procesą skaidant į daugiau žingsnių, kuriuos gali nusistatyti pati organizacija.

1 žingsnis. Duomenų tvarkymo operacijos nustatymas ir jos kontekstas

Rizikos vertinimas prasideda organizacijai nustačius vertinamų asmens duomenų apimtį ir kontekstą. Siekiant padėti organizacijai tiksliau nustatyti asmens duomenų tvarkymo operacijos pobūdį, rekomenduotina atsižvelgti į šiuos klausimus:

1. Kokios yra organizacijos asmens duomenų tvarkymo operacijos?
2. Kokios kategorijos asmens duomenys yra tvarkomi?
3. Koks tvarkymo tikslas?
4. Kokios priemonės naudojamos tvarkyti asmens duomenis?
5. Kur vykdomas asmens duomenų tvarkymas?
6. Kokios yra duomenų subjektų kategorijos?
7. Kas yra duomenų gavėjai?

Atsakydama į šiuos klausimus organizacija turi apsvarstyti įvairius duomenų tvarkymo etapus (rinkimą, saugojimą, naudojimą, perdavimą, sunaikinimą ir kt.).

2 žingsnis. Poveikio supratimas ir vertinimas

Remiantis 1 žingsnio analize organizacija turi įvertinti fizinių asmenų pagrindinėms teisėms ir laisvėms kylantį poveikį dėl galimo asmens duomenų saugumo pažeidimo. Nagrinėjami trys poveikio lygiai (žemas, vidutinis ir aukštas). Poveikio fiziniam asmeniui lygio reikšmių įvertinimas:

- **Žemas**: fizinis asmuo gali susidurti su tam tikrais nepatogumais (pvz., sugaištas laikas iš naujo suvedant informaciją, susierzinimas, nepasitenkinimas ir pan.);
- **Vidutinis**: fizinis asmuo gali patirti didelių nepatogumų, kuriuos jis galės įveikti nepaisant tam tikrų sunkumų (pvz., papildomos išlaidos, prieigos prie reikalingų išteklių praradimas, stresas, nedideli fiziniai negalavimai ir kt.);
- **Aukštas**: fizinis asmuo gali patirti reikšmingas pasekmes ir norint jas ištaisyti, pašalinti reikės susidurti su rimtais sunkumais (pvz., lėšų praradimas, asmens įtraukimas į finansinių institucijų juodąjį sąrašą, turto nuostoliai (žala), darbo vietos praradimas, teisminiai procesai, sveikatos būklės pablogėjimas ir pan.) arba dideles ar negrįžtamas pasekmes, kurių negalės ištaisyti, pašalinti (pvz., negalėjimas dirbti, ilgalaikiai psichiniai ar fiziniai negalavimai, mirtis ir pan.).

Poveikio vertinimas yra kokybinis procesas ir duomenų valdytojas privalo atsižvelgti į įvairius veiksnius, tokius kaip tvarkomų asmens duomenų kategorijos ir kiekis, duomenų tvarkymo operacijos svarba, organizacijos veiklos specifika, taip pat pažeidžiamų duomenų subjektų kategorijos (pvz., vaikai, pacientai) ar veiklos sritys.

Atkreiptinas dėmesys, kad jeigu organizacijoje specialių kategorijų ar pažeidžiamų asmenų asmens duomenys tvarkomi dideliu mastu arba vykdomas sistemingas ir išsamus asmens savybių vertinimas, grindžiamas automatizuotu tvarkymu, įskaitant profiliavimą, tai poveikis dėl galimo asmens duomenų saugumo pažeidimo turėtų būti vertinamas kaip „Aukštas“.

Specialių kategorijų asmens duomenys – tai duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose; genetiniai duomenys, biometriniai duomenys, pagal kuriuos galima *konkrečiai nustatyti fizinio asmens tapatybę*; sveikatos duomenys; duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.

Siekiant lengviau organizacijai įvertinti poveikį, rekomenduotina naudotis šių gairių 1 lentele ir įvertinti atskirai poveikį dėl duomenų konfidencialumo, vientisumo ir prieinamumo praradimo. Vertinant poveikį, būtina atsižvelgti į rizikos veiksnius, kylančius ne tik iš organizacijos vidaus, bet ir išorinius, kuriems organizacija neturi įtakos (pvz., IT paslaugų tiekėjo bankrotas ir kt.).

Atlikus šį vertinimą gaunami trys skirtingi poveikio lygiai (dėl konfidencialumo, vientisumo ir prieinamumo praradimo). Aukščiausias nustatytas poveikis laikomas galutiniu poveikio, susijusio su bendru asmens duomenų tvarkymu, įvertinimo rezultatu.

1 lentelė. Poveikio vertinimo klausimai

Nr.	Klausimas	Poveikis
1.	Ar organizacijoje tvarkomi specialių kategorijų asmens duomenys?	☐ Taip ☐ Ne
2.	Nurodykite, kokį poveikį, Jūsų manymu, gali sukelti neleistinas tvarkomų asmens duomenų ***atskleidimas***, ***konfidencialumo praradimas*** Jūsų organizacijos veiklos kontekste ir kokį tai galėtų turėti poveikį fiziniam asmeniui bei pateikite įvertinimą (pažymėkite poveikio lygį).	☐ Žemas ☐ Vidutinis ☐ Aukštas
3.	Nurodykite, kokį poveikį, Jūsų manymu, gali sukelti neleistinas tvarkomų asmens duomenų ***pakeitimas***, ***vientisumo praradimas*** Jūsų organizacijos veiklos kontekste ir kokį tai galėtų turėti poveikį fiziniam asmeniui bei pateikite įvertinimą (pažymėkite poveikio lygį).	☐ Žemas ☐ Vidutinis ☐ Aukštas
4.	Nurodykite, kokį poveikį, Jūsų manymu, gali sukelti neleistinas tvarkomų asmens duomenų ***sunaikinimas ar prieigos praradimas*** Jūsų organizacijos veiklos kontekste ir kokį tai galėtų turėti poveikį fiziniam asmeniui bei pateikite įvertinimą (pažymėkite poveikio lygį).	☐ Žemas ☐ Vidutinis ☐ Aukštas

3 žingsnis. Galimų grėsmių nustatymas ir jų atsiradimo tikimybės vertinimas

Šiame etape organizacijai reikia nustatyti grėsmes, susijusias su visa asmens duomenų tvarkymo aplinka (išorės arba vidaus), ir įvertinti jų atsiradimo tikimybę.

Siekiant šį procesą supaprastinti yra pateikiami klausimai, skirti įvertinti organizacijos asmens duomenų tvarkymo aplinką (ji yra tiesiogiai susijusi su grėsmėmis) ir galimas grėsmes.

Šie klausimai yra susiję su keturiais pagrindiniais šios aplinkos aspektais (vertinimo sritimis), tai yra:

- Tinklo ir techniniai ištekliai;
- Procesai ir procedūros, susiję su asmens duomenų tvarkymu;
- Duomenų tvarkymo dalyviai;
- Veiklos sritys ir duomenų tvarkymo mastai.

2 lentelėje pateikiami klausimai, susiję su grėsmių atsiradimo tikimybe ir skirti įvertinti organizacijos asmens duomenų tvarkymo aplinką bei galimas grėsmes.

2 lentelė. Grėsmių ir jų atsiradimo tikimybės vertinimo klausimai

Tinklo ir techniniai ištekliai		
1.	Ar organizacijoje yra sistemų ar įrenginių su asmens duomenimis, kurie prieinami internetu?	☐ Taip ☐ Ne
2.	Ar galima internetu prisijungti prie vidinių asmens duomenų tvarkymo sistemų (pvz., tam tikriems vartotojams arba vartotojų grupėms)?	☐ Taip ☐ Ne
3.	Ar organizacijos sistemos, kuriose tvarkomi asmens duomenys, yra tarpusavyje sujungtos, integruotos su kitomis išorinėmis ar vidinėmis (Jūsų organizacijos) informacinių technologijų (IT) sistemomis arba paslaugomis?	☐ Taip ☐ Ne
4.	Ar neįgalioti asmenys gali lengvai prieiti prie duomenų tvarkymo aplinkos (pvz., neužtikrinamas tinkamas fizinės prieigos prie IT įrangos saugumas)?	☐ Taip ☐ Ne
5.	Ar organizacijoje yra asmens duomenų tvarkymui naudojamų IT sistemų, kurios sukurtos ar įdiegtos nesilaikant gerosios praktikos (pvz., Agile, ISO 27000, ITIL ir kt.)?	☐ Taip ☐ Ne
Procesai ir procedūros, susiję su asmens duomenų tvarkymu		
6.	Ar organizacijoje prieigos ir (ar) atsakomybės yra neaiškios arba neaiškiai apibrėžtos?	☐ Taip ☐ Ne
7.	Ar organizacijoje yra / pasitaiko neaiškumų (dviprasmiškai suprantamų instrukcijų) dėl tinklo, sistemų ar fizinių išteklių naudojimo?	☐ Taip ☐ Ne
8.	Ar darbuotojams leidžiama naudoti asmeninius prietaisus, įrenginius ir jais prisijungti prie organizacijos asmens duomenų tvarkymo sistemų?	☐ Taip ☐ Ne
9.	Ar darbuotojams leidžiama perkelti, saugoti ar kitaip tvarkyti organizacijos asmens duomenis už organizacijos ribų (pvz., nešiojamuosiuose įrenginiuose, laikmenose)?	☐ Taip ☐ Ne
10.	Ar asmens duomenų tvarkymo veiksmai gali būti atliekami, nefiksuojant jų (be veiksmų atsekamumo) sistemų žurnalų įrašuose (angl. *log files*)?	☐ Taip ☐ Ne
Duomenų tvarkymo dalyviai		
11.	Ar asmens duomenis tvarko neapibrėžtas (nenustatytas konkrečiai) darbuotojų skaičius?	☐ Taip ☐ Ne
12.	Ar yra organizacijos valdomų asmens duomenų, kuriuos tvarko duomenų tvarkytojai (pvz., rangovai, trečiosios šalys)?	☐ Taip ☐ Ne
13.	Ar organizacijoje yra dviprasmiškai arba neaiškiai apibrėžtų asmens duomenų tvarkymo prievolių, susijusių su trečiosiomis šalimis / asmenimis?	☐ Taip ☐ Ne
14.	Ar organizacijoje yra darbuotojų, dalyvaujančių asmens duomenų tvarkyme, bet kuriems trūksta kompetencijų konfidencialiai tvarkyti informaciją techniniu ar asmeninio sąžiningumo požiūriu?	☐ Taip ☐ Ne
15.	Ar organizacijoje yra darbuotojų arba kitų duomenų tvarkytojų, dalyvaujančių asmens duomenų tvarkyme, kurie neturi galimybių tinkamai sunaikinti asmens duomenų laikmenas?	☐ Taip ☐ Ne
Veiklos sritys ir duomenų tvarkymo mastai		
16.	Ar manote, kad Jūsų organizacija, atsižvelgiant į jos veiklos sritį, potencialiai galėtų tapti dažnesniu kibernetinių atakų taikiniu?	☐ Taip ☐ Ne
17.	Ar per pastaruosius dvejus metus Jūsų organizacijoje buvo įvykęs asmens duomenų saugumo pažeidimas ar kitas saugumo incidentas?	☐ Taip ☐ Ne
18.	Ar per pastaruosius metus gavote kokius nors pranešimus ir (arba) skundus dėl IT sistemų, naudojamų asmens duomenų tvarkymui, saugumo?	☐ Taip ☐ Ne
19.	Ar organizacija tvarko asmens duomenis dideliu mastu?	☐ Taip ☐ Ne

	(Atsižvelgiama į šiuos veiksnius: susijusių duomenų subjektų skaičių – konkretų skaičių arba atitinkamo gyventojų skaičiaus procentinę dalį; duomenų vienetų kiekį ir (arba) intervalą; duomenų tvarkymo veiklos trukmę arba pastovumą; geografinę duomenų tvarkymo aprėptį (pvz., duomenys tvarkomi regioniniu, nacionaliniu ar tarpvalstybiniu lygmeniu).	
20.	Ar yra veiklai (veiklos sričiai) būdingos gerosios saugumo praktikos ar standartų, kurių Jūsų organizacijoje nesilaikoma?	☐ Taip ☐ Ne

Kiekvienai vertinamai sričiai gali būti nustatytas grėsmės atsiradimo tikimybės lygis:

- **Žemas**: mažai tikėtina, kad grėsmė pasitvirtins (jeigu iš penkių klausimų gautas ne daugiau kaip vienas atsakymai „Taip“);
- **Vidutinis**: yra reali galimybė, kad grėsmė pasitvirtins (jeigu iš penkių klausimų gauti ne mažiau kaip du ir ne daugiau kaip trys atsakymai „Taip“);
- **Aukštas**: tikėtina, kad grėsmė pasitvirtins (jeigu iš penkių klausimų gauti daugiau kaip trys atsakymai „Taip“).

Tuomet, pasinaudojant 3 ir 4 lentelėmis, galima nustatyti grėsmės atsiradimo tikimybę kiekvienai vertinamai sričiai ir atitinkamai apskaičiuoti jos galutinę vertę.

3 lentelė. Grėsmės atsiradimo tikimybės įvertinimas kiekvienai sričiai

Vertinimo sritis	**Tikimybė**	
	Lygis	**Balas**
Tinklo ir techniniai ištekliai	☐ Žemas	1
	☐ Vidutinis	2
	☐ Aukštas	3
Procesai ir procedūros, susiję su asmens duomenų tvarkymu	☐ Žemas	1
	☐ Vidutinis	2
	☐ Aukštas	3
Duomenų tvarkymo dalyviai	☐ Žemas	1
	☐ Vidutinis	2
	☐ Aukštas	3
Veiklos sritys ir duomenų tvarkymo mastai	☐ Žemas	1
	☐ Vidutinis	2
	☐ Aukštas	3

4 lentelė. Grėsmės atsiradimo įvertinimas

Bendra grėsmės atsiradimo balų suma	**Grėsmės atsiradimo tikimybės lygis**
4–5	Žemas
6–8	Vidutinis
9–12	Aukštas

Galutinis grėsmės atsiradimo tikimybės lygis apskaičiuojamas sudėjus kiekvienos iš keturių vertinimo sričių balus, gautus pagal 3 lentelę, ir susiejus rezultatą su 4 lentelės balais.

4 žingsnis. Rizikos įvertinimas

Įvertinus asmens duomenų tvarkymo operacijos **poveikį** ir atitinkamos **grėsmės atsiradimo tikimybę**, pasinaudojant 5 lentele galima atlikti galutinį **rizikos įvertinimą**.

5 lentelė. Rizikos įvertinimas

		Poveikio lygis		
		Žemas	**Vidutinis**	**Aukštas**
Grėsmės atsiradimo tikimybės lygis	**Žemas**			
	Vidutinis			
	Aukštas			

Rizikos lygio žymėjimas: žemas vidutinis aukštas

Organizacija, įvertinusi rizikos lygį, gali pasirinkti tinkamas saugumo priemones asmens duomenų saugumui užtikrinti. Duomenų saugumo priemonės skirstomos į dvi plačias kategorijas (organizacines ir technines), kurios toliau skirstomos pagal konkrečias priemonių rūšis ir žymimos spalvomis ir ornamentais pagal rizikos lygį (žemas – žalia, įstriži brūkšniai iš kairės pusės žemyn, vidutinis – geltona, vertikalūs brūkšniai, aukštas – raudona, įstriži brūkšniai iš dešinės žemyn).

Siekiant, kad skirtingų rizikos lygių priemonės būtų tarpusavyje suderintos, laikytina, kad visos žemam rizikos lygiui (žalios spalvos, įstriži brūkšniai iš kairės pusės žemyn) siūlomos priemonės tinka visiems lygiams. Priemonės, pateiktos vidutiniam rizikos lygiui (geltona spalva, vertikalūs brūkšniai), taikomos ir aukštam rizikos lygiui. O aukštam rizikos lygiui (raudonos spalvos, įstriži brūkšniai iš dešinės žemyn) siūlomos priemonės nėra taikomos jokiam kitam rizikos lygiui.

Nepaisant gauto galutinio rezultato, organizacija gali patikslinti gautą rizikos lygį atsižvelgdama į konkrečias duomenų tvarkymo operacijos savybes (kurių nebuvo vertinimo proceso metu) ir tinkamai pateisindama ir pagrįsdama šį koregavimą.

Pažymėtina, kad priemonių taikymas konkretiems rizikos lygiams neturėtų būti suprantamas kaip absoliutus. Priklausomai nuo asmens duomenų tvarkymo konteksto, organizacija gali svarstyti papildomų priemonių įgyvendinimą, net jei jos priskirtos aukštesniam rizikos lygiui. Be to, siūlomame priemonių sąraše neatsižvelgiama į kitus papildomai konkrečiam veiklos sektoriui taikomus ar būdingus saugumo reikalavimus ar į konkrečias įstatymų nustatytas prievoles.

Kai kuriais atvejais, įvertinus organizacijos asmens duomenų tvarkymo operacijas, **gali būti nustatomas ne bendras visos organizacijos saugumo lygis, bet atskiri saugumo lygiai** (jie gali skirtis) pagal veiklos sritis ar veiklos procesus, ir tada atitinkamai parenkamos ir įgyvendinamos techninės ir organizacinės saugumo priemonės.

Organizacinės duomenų saugumo priemonės

Eil. Nr.	Priemonės	Atitikmuo ISO 27001:2017 A priede ir galimi papildomi reikalavimai pagal ISO 27701:2019	Atitikmuo BDAR ir paaiškinimai
Asmens duomenų saugumo politika ir procedūros			
1.	Asmens duomenų ir jų tvarkymo saugumas organizacijoje turi būti dokumentuotas kaip informacijos saugumo politikos dalis.	**A.5 Informacijos saugumo politikos** **Papildomi reikalavimai dėl informacijos apsaugos ISO 27701 – 6.2**	Saugumo politika yra svarbus dokumentas, nustatantis pagrindinius informacijos saugumo ir asmens duomenų apsaugos principus organizacijoje. Tai yra visų konkrečių techninių ir organizacinių duomenų saugumo priemonių įgyvendinimo pagrindas pagal BDAR 32 straipsnį ir jį papildantį 24 straipsnį dėl duomenų valdytojo įgyvendinamos atitinkamos duomenų apsaugos politikos. Remiantis saugumo politika, konkrečios techninės ir organizacinės priemonės aprašomos detalesnėse politikose (pvz., prieigos kontrolės, įrenginių valdymo, išteklių valdymo ir kt.). Saugumo politika nustato bendrą organizacijos informacijos saugos valdymą ir joje turi būti aiškiai išskirta asmens duomenų apsauga.
2.	Saugumo politika turi būti peržiūrima ir prireikus atnaujinama ne rečiau kaip kartą per metus.		
3.	Organizacijos duomenų saugumo politika turi nustatyti bent: personalo pareigas (funkcijas) ir atsakomybes, pagrindines technines ir organizacines priemones, įdiegtas asmens duomenų saugumui užtikrinti, taip pat duomenų tvarkytojų ar trečiųjų šalių, susijusių su asmens duomenų tvarkymu, sąrašą.		
4.	Atsižvelgiant į bendrą saugumo politiką, turi būti sukurtas ir prižiūrimas		

	konkrečių su asmens duomenų saugumu susijusių politikos dokumentų, procedūrų, tvarkų aprašas.		
5.	Saugumo politika turi būti peržiūrima ir, prireikus, tikslinama kas pusmetį.		
Vaidmenys ir atsakomybės			
6.	Su asmens duomenų tvarkymu susiję vaidmenys ir atsakomybės turi būti aiškiai apibrėžti ir paskirstyti pagal saugumo politiką.	**A.6.1.1 Su informacijos saugumu susiję vaidmenys ir atsakomybės** **Papildomi reikalavimai dėl darbuotojų atsakomybės ISO 27701 – 6.3.1.1**	BDAR 32 straipsnio 4 dalis numato, kad duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Europos Sąjungos arba valstybės narės teisę. Pagrindinės asmens duomenų saugumo priemonės organizacijos personalui, turinčiam prieigą prie asmens duomenų – aiškiai apibrėžta ir dokumentuota atsakomybė bei vaidmenys, taip pat darbo su asmens duomenimis kompetencijos. Ypač svarbus vaidmuo tenka saugos specialistui (ar įgaliotiniui), kuris yra atsakingas už tinkamos saugumo politikos įgyvendinimą. Kitas svarbus vaidmuo tenka duomenų apsaugos pareigūnui (toliau – DAP), kurio viena iš užduočių yra stebėti, kaip organizacijoje laikomasi BDAR (tam tikrais atvejais pagal BDAR 37 straipsnį DAP paskyrimas yra privalomas). Tiek saugos specialistas (ar įgaliotinis), tiek DAP turi glaudžiai bendradarbiauti.
7.	Turi būti aiškiai apibrėžtas darbuotojų teisių ir pareigų atšaukimas taikant atitinkamas vaidmenų ir atsakomybių perdavimo ar perleidimo procedūras (vidaus organizacijos pertvarkymo ar darbuotojų atleidimo, funkcijų pasikeitimo metu).		
8.	Reikėtų atlikti aiškų asmenų, atsakingų už konkrečias saugumo užduotis, paskyrimą, įskaitant saugos specialisto (saugos įgaliotinio) paskyrimą.		
9.	Saugos specialistas turi būti oficialiai paskirtas (paskyrimą patvirtinant dokumentais). Saugos specialisto uždaviniai ir atsakomybės turi būti aiškiai nustatyti ir dokumentuoti.		

10.	Nesuderinamos pareigybės (funkcijos) ir atsakomybių sritys, pavyzdžiui, saugos specialisto pareigybė ir duomenų apsaugos pareigūno pareigybė, turi būti atskirtos, siekiant sumažinti neleistino ar netyčinio asmens duomenų keitimo ar netinkamo naudojimo galimybes.		
Prieigos valdymo politika			
11.	Kiekvienam vaidmeniui, susijusiam su asmens duomenų tvarkymu, turi būti priskirtos konkrečios prieigos kontrolės teisės, vadovaujantis „būtina žinoti“ (angl. *need to know*) principu.	**A.9.1.1 Prieigos valdymo politika**	Būtina nustatyti prieigos kontrolės politiką sistemoms, naudojamoms tvarkant asmens duomenis. Kontrolė turi būti grindžiama principu „būtina žinoti“, t. y. kiekvienam vaidmeniui ar naudotojui turi būti suteiktas tik toks asmens duomenų prieinamumo lygis, kuris yra būtinas jo užduotims atlikti. Šie reikalavimai glaudžiai susiję su vientisumo ir konfidencialumo principu (BDAR 5 straipsnio 1 dalies f punktas). Prieigos kontrolės politika turi būti įgyvendinama taikant technines priemones (taip pat žiūrėti technines priemones, nurodytas šių gairių 41–48 punktuose „Prieigų kontrolė ir autentifikavimas“).
12.	Prieigos kontrolės politika turi būti išsami ir dokumentuota. Organizacija šiame dokumente turi nustatyti atitinkamas prieigos kontrolės taisykles, prieigos teises ir apribojimus pagal konkrečias naudotojų pareigas, susijusias su asmens duomenų tvarkymo procesais ir procedūromis.		
13.	Prieigos kontrolę užtikrinančių funkcijų atskyrimas (pvz., prieigos užklausų, prieigos leidimų, pačios prieigos administravimas) turi būti aiškiai apibrėžtas ir dokumentuotas.		
14.	Tam tikros pareigybės (funkcijos), turinčios dideles prieigos teises, turi		

	būti aiškiai apibrėžtos ir priskirtos tik ribotam darbuotojų skaičiui.		
Išteklių ir turto valdymas			
15.	Organizacija turi turėti IT išteklių (naudojamų asmens duomenims tvarkyti) registrą (techninės, programinės ir tinklo įrangos sąrašą). IT išteklių registras turi apimti bent tokią informaciją: IT išteklių tipą (pvz., tarnybinę stotį, kompiuterinę darbo vietą), vietą (fizinę ar elektroninę). IT išteklių registro tvarkymas turi būti priskirtas konkrečiam asmeniui, pvz., IT specialistui.	**A.8 Turto tvarkymas** **Papildomi reikalavimai dėl informacijos klasifikavimo ISO 27701 – 6.5.2 ir duomenų laikmenų priežiūros ISO 27701 – 6.5.3**	Tinkamas techninės, programinės ir tinklo įrangos valdymas yra būtinas asmens duomenų saugumui ir vientisumui (vientisumo ir konfidencialumo principas apibrėžtas BDAR 5 straipsnio 1 dalies f punkte), nes tai leidžia kontroliuoti duomenų tvarkymo priemones. Išteklių valdymas būtinai turi apimti IT išteklių ir tinklo topologijos (schemos), kuri yra naudojama tvarkant asmens duomenis, registravimą.
16.	IT išteklių registras turi būti reguliariai peržiūrimas ir atnaujinamas. Rekomen-duojamas peržiūros dažnumas – kartą per 3 mėnesius.		
17.	Visos pareigybės, turinčios prieigą prie IT išteklių, turi būti apibrėžtos ir patvirtintos dokumentais.		
Keitimų valdymas			
18.	Organizacija turi užtikrinti, kad visi esminiai IT sistemų keitimai būtų stebimi ir registruojami konkretaus	**A. 12.1 Darbo procedūros ir atsakomybės**	Keitimų valdymo tikslas – sinchronizuoti ir kontroliuoti visus IT sistemose, naudojamose tvarkant asmens duomenis, atliekamus keitimus. Tai yra svarbi saugumo priemonė, nes nesėkmingas keitimų įgyvendinimas gali sukelti

	asmens (pvz., IT arba saugos specialisto).		neteisėtą duomenų atskleidimą, pakeitimą ar sunaikinimą. Keitimų valdymas yra būtinas duomenų tvarkymo vientisumui užtikrinti (BDAR 5 straipsnio 1 dalies f punktas) ir duomenų valdytojo atskaitomybės principui įgyvendinti (BDAR 5 straipsnio 2 dalis).
19.	Programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant asmens duomenis. Testuojant sistemas, reikia naudoti testinius duomenis. Tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros.		
20.	Turi būti įdiegta išsami ir dokumentais pagrįsta IT keitimų valdymo politika. Keitimų valdymo politiką turi apibrėžti: pokyčių įvedimo ir įdiegimo procedūras, pareigybes ir vartotojus, kurių teisės buvo pakeistos, pokyčių įdiegimo laiko terminus. Pokyčių valdymo politika turi būti reguliariai atnaujinama.		
Duomenų tvarkytojai			
21.	Prieš pradedant asmens duomenų tvarkymo veiklą, duomenų valdytojai turi apibrėžti, dokumentuoti ir suderinti formalias gaires ir procedūras, taikomas duomenų tvarkytojams (pvz., rangovams ar užsakomųjų paslaugų tiekėjams) dėl asmens duomenų	**A.15 Santykiai su tiekėjais** **Papildomi reikalavimai dėl saugumo**	BDAR 28 straipsnis numato, kad „duomenų valdytojas pasitelkia tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų šio reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga.“ Tame pačiame straipsnyje nurodoma, kad duomenų valdytojo ir duomenų tvarkytojo santykiai turi būti apibrėžti sutartyje ar teisės akte.

	tvarkymo. Šios gairės ir procedūros turi nustatyti tokį patį (ne žemesnį) asmens duomenų saugumo lygį, koks yra numatytas organizacijos saugumo politikoje.	**užtikrinimo susitarimų sutartyse ISO 27701 – 6.12.1.2**	
22.	Duomenų tvarkytojas privalo nedelsdamas pranešti duomenų valdytojui apie nustatytus asmens duomenų saugumo pažeidimus.		
23.	Duomenų tvarkytojas turi pateikti dokumentais pagrįstus įrodymus dėl atitikties jam keliamiems reikalavimams.		
24.	Duomenų valdytojas turi reguliariai tikrinti duomenų tvarkytojo atitiktį nustatytų reikalavimų ir įsipareigojimų lygiui.		
25.	Duomenų tvarkytojo darbuotojams, dirbantiems su asmens duomenimis, turi būti taikomi konkretūs dokumentais įtvirtinti informacijos konfidencialumo, neatskleidimo susitarimai.		
Asmens duomenų saugumo pažeidimai ir saugumo incidentai			
26.	Turi būti nustatytas reagavimo į saugumo incidentus planas, užtikrinantis veiksmingą incidentų, susijusių su asmens duomenų saugumu, valdymą.	**A.16 Informacijos saugumo incidentų valdymas**	Duomenų saugumo pažeidimo atveju organizacija turi įvertinti, ar tai turės įtakos „atsitiktiniam ar neteisėtam perduodamų, saugomų ar kitaip tvarkomų asmens duomenų sunaikinimui, praradimui, pakeitimui, neteisėtam atskleidimui ar prieigai prie jų“ (BDAR 4 straipsnio 12 dalis). Duomenų valdytojai turi būti tikri, kad jie laikosi savo įsipareigojimų pagal BDAR 33 ir 34 straipsnius,

27.	Asmens duomenų saugumo pažeidimai turi būti fiksuojami (dokumentuojami). Apie juos turi būti nedelsiant pranešama vadovybei. Turi būti nustatyta pranešimo apie asmens duomenų saugumo pažeidimus kompetentingoms institucijoms ir duomenų subjektams tvarka.	**Papildomi reikalavimai dėl atsakomybės ir procedūrų** **ISO 27701 – 6.13.1.1 ir reagavimo į incidentus** **ISO 27701 – 6.13.1.5**	susijusius su pranešimu apie asmens duomenų saugumo pažeidimus priežiūros institucijai ir duomenų subjektams. Duomenų tvarkytojai taip pat turi būti tikri, kad jie laikosi savo įsipareigojimų pagal BDAR 33 straipsnį ir galės nedelsdami pranešti duomenų valdytojui apie minėtus pažeidimus. Bet kuriuo atveju, tiek duomenų valdytojai, tiek ir duomenų tvarkytojai turi turėti tinkamas procedūras ne tik pranešti apie asmens duomenų pažeidimus, bet ir juos suvaldyti.
28.	Saugumo incidentų likvidavimo planas turi būti patvirtintas dokumentais, tarp kurių būtų galimų saugumo incidento poveikio mažinimo priemonių sąrašas ir aiškus atskirų funkcijų paskirstymas.		
29.	Visi saugumo incidentai, įskaitant ir asmens duomenų saugumo pažeidimus, turi būti fiksuojami kartu su visa susijusia informacija apie įvykį ir vėliau atliktus incidento poveikio mažinimo veiksmus.		
Veiklos tęstinumas			
30.	Organizacija turi nustatyti pagrindines procedūras, kurių reikia laikytis saugumo incidento ar asmens duomenų saugumo pažeidimo atveju, kad būtų užtikrintas reikiamas asmens duomenų tvarkymo IT sistemomis tęstinumas ir prieinamumas.	**A. 17 Veiklos tęstinumo valdymo informacijos saugumo aspektai**	Veiklos ar paslaugų tęstinumo planas yra būtinas nustatant procesus ir technines priemones, kurių organizacija turi laikytis saugumo incidento ar asmens duomenų saugumo pažeidimo atveju. Šis planas papildo organizacijos saugumo politiką. Ši priemonė aiškiai susijusi su BDAR 32 straipsnio 1 dalies c punktu, kuris įpareigoja duomenų valdytoją ir tvarkytoją „laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“.

31.	Veiklos tęstinumo planas turi būti išsamiai apibūdintas ir patvirtintas dokumentais (laikantis bendros saugumo politikos). Jame turi būti pateiktas aiškus veiksmų planas ir funkcijų paskirstymas.		
32.	Veiklos tęstinumo plane turi būti apibrėžtas garantuotos paslaugų kokybės lygis (angl. *Service-level agreement* (*SLA*), kuris nustatomas pagrindiniams veiklos procesams, kurie užtikrina asmens duomenų saugumą.		
33.	Turi būti paskirti darbuotojai, turintys reikiamą atsakomybę, įgaliojimus ir kompetenciją valdyti veiklos tęstinumą saugumo incidento, asmens duomenų saugumo pažeidimo atveju.		
34.	Turi būti numatyta alternatyvi infrastruktūros priemonė organizacijos darbui, atsižvelgiant į organizaciją ir jai priimtiną IT sistemų prastovą.		
Personalo konfidencialumas			
35.	Organizacija turi užtikrinti, kad visi darbuotojai suprastų savo atsako-mybes ir įsipareigojimus, susijusius su asmens duomenų tvarkymu. Vaidmenys ir atsakomybės turi būti aiškiai išdėstyti darbuotojui prieš	**A.7 Žmogiškųjų išteklių saugumas** **Papildomi reikalavimai dėl**	Siekiant užtikrinti asmens duomenų konfidencialumą pagal BDAR 32 straipsnį, organizacija turi užtikrinti, kad jos darbuotojai gebėtų konfidencialiai tvarkyti informaciją tiek techniniu, tiek asmeninio sąžiningumo požiūriu. Be to, BDAR 32 straipsnio 4 dalis (atitinkamai BDAR 29 straipsnis) numato, kad „duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo,

	pradedant vykdyti jam paskirtas funkcijas ir darbus.	**darbuotojų sąmoningumo ISO 27701 – 6.4.2.2**	galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Sąjungos arba valstybės narės teisę“. Šiuo tikslu turi būti nustatytos specialios priemonės, užtikrinančios, kad asmenys, dalyvaujantys tvarkant asmens duomenis, būtų tinkamai informuojami apie savo pareigą laikytis konfidencialumo. Taip pat turi būti užtikrinta, kad šios pareigos būtų pakankamai apibrėžtos organizacijos žmogiškųjų išteklių politikoje.
36.	Darbuotojai, prieš pradėdami eiti savo pareigas, turi būti pasirašytinai supažindinti su organizacijos saugumo politika, taip pat pasirašyti atitinkamus informacijos konfidencialumo ir neatskleidimo susitarimus.		
37.	Darbuotojai, atsakingi už aukštos rizikos asmens duomenų tvarkymo operacijas, turi laikytis konkrečių jiems taikomų konfidencialumo sąlygų (pagal jų darbo sutartį ar kitą teisės aktą).		
Mokymai			
38.	Organizacija turi užtikrinti, kad visi darbuotojai būtų tinkamai informuoti apie IT sistemų saugumo reikalavimus, susijusius su jų kasdieniu darbu. Darbuotojai, susiję su asmens duomenų tvarkymu, turi būti mokomi apie atitinkamus duomenų saugumo reikalavimus ir atsakomybes, rengiant reguliarius mokymus, informavimo renginius ar instruktažus. Siūlomas mokymų periodiškumas – kartą per metus.	**A.7.2.2 Informacijos saugumo supratimas, švietimas ir mokymas**	Personalo mokymai apie duomenų apsaugos ir saugumo procedūras (pvz., slaptažodžių naudojimas ir prieiga prie konkrečių IT sistemų) yra svarbūs tinkamam organizacinių ir techninių duomenų saugumo priemonių įgyvendinimui ir prevencijai dėl „netyčinio duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų“ (BDAR 32 straipsnio 2 dalis). Žinios apie konkrečius duomenų apsaugos teisinius įsipareigojimus taip pat yra svarbios, ypač tiems asmenims, kurie dalyvauja didelės rizikos asmens duomenų tvarkymo procesuose.
39.	Organizacija turi rengti struktūrines nuolatines personalo mokymų		

	programas, tarp kurių būtų ir speciali programa, skirta mokyti naujus darbuotojus (duomenų apsaugos tema).		
40.	Kiekvienais metais turi būti parengtas ir įgyvendintas mokymų planas, kuriame būtų nustatyti siektini tikslai ir uždaviniai.		

Techninės duomenų saugumo priemonės

Eil. Nr.	Priemonės	Atitikmuo ISO 27001:2017 A priede ir galimi papildomi reikalavimai pagal ISO 27701:2019	Atitikmuo BDAR ir paaiškinimai, galimos grėsmės
Prieigų kontrolė ir autentifikavimas			
41.	Turi būti įdiegta, įgyvendinta Prieigų kontrolės sistema, kuri taikoma visiems IT sistemos naudotojams. Prieigų kontrolės sistema turi leisti kurti, patvirtinti, peržiūrėti ir panaikinti naudotojų paskyras.	**A.9 Prieigos valdymas** **Papildomi reikalavimai dėl vartotojų registravimo ir išregistravimo ISO 27701 – 6.6.2.1 ir dėl identifikavimo techninės kontrolės ISO 27701 – 6.6.2.2**	Prieigų kontrolė ir autentifikavimas yra esminiai saugos reikalavimai, siekiant apsisaugoti nuo neautorizuotos prieigos prie IT sistemos, kurioje yra tvarkomi asmens duomenys. Šie saugos reikalavimai įgyvendina organizacijos prieigų kontrolės politiką (taip pat žiūrėti organizacines priemones, nurodytas šių gairių 11–14 punktuose „Prieigos valdymo politika“) techniškai panaudojant specifinius, techninius komponentus ir taikomąsias programas. **Galimos grėsmės ir pavojai** Nesukontroliuojamos neautorizuotų naudotojų prieigos prie asmens duomenų; neautorizuotas duomenų bazės turinio (asmens duomenų) atskleidimas, peržiūrėjimas, kopijavimas, redagavimas, naikinimas (angl. *broken access control; broken authentification*). Naudotojų atliktų veiksmų kontrolė, atsekamumas bendroje paskyroje; naudotojo prisijungimo duomenų prie bendros paskyros atskleidimas; neteisėtas bendros paskyros naudotojo teisių eskalavimas į aukštesnes pareigas (administratoriaus). Neteisėto turinio kaupimas ir vykdymas. Sudėtingas naudotojų atliktų veiksmų atsekamumas nesant autentifikacijos, autorizacijos mechanizmo; neautorizuotos naudotojų prieigos prie duomenų
42.	Turi būti vengiama naudoti bendras naudotojų paskyras. Vietose, kur bendra naudotojų paskyra yra būtina, turi būti užtikrinta, kad visi bendros paskyros naudotojai turi tokias pat teises ir pareigas.		
43.	Turi būti veikiantis autentifikavimo mechanizmas, leidžiantis prieigą prie IT sistemos (paremtas Prieigų kontrolės politika). Minimalus reikalavimas naudotojui prisijungti prie IT sistemos – naudotojo prisijungimo vardas ir		

	slaptažodis. Slaptažodis sudaromas atsižvelgiant į tam tikrą kompleksiškumo lygį.		bazės turinio (asmens duomenų); neautorizuotas asmens duomenų peržiūrėjimas, kopijavimas, redagavimas, naikinimas. IT infrastruktūros, informacinių sistemų, duomenų bazės tiesioginė prieiga kompiuterių tinklais, internetu, be autorizacijos. Nekontroliuojant slaptažodžių politikos ir (ar) nesilaikant slaptažodžių kompleksiškumo yra neužtikrinamas duomenų saugumas, slaptažodžiai nėra atsparūs slaptažodžių parinkinėjimo (angl. *bruteforce*) kibernetinei atakai.
44.	Prieigų kontrolės sistema turi turėti galimybę aptikti ir neleisti naudoti slaptažodžių, kurie neatitinka tam tikro kompleksiškumo lygio.		
45.	Vartotojo slaptažodžiai turi būti saugomi naudojant kodavimo formą (angl. *hash form*).		
46.	Turi būti nustatytos ir dokumentais patvirtintos slaptažodžių naudojimo taisyklės. Taisyklėse turi būti apibrėžtas slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius.		
47.	Privilegijuotiems vartotojams (pvz., sistemų administratoriams) prisijungimui prie asmens duomenų tvarkymo sistemų turi būti taikomas dviejų veiksnių autentifikavimas. Visais atvejais, kai į tokias sistemas jungiamasi ne iš vidinio kompiuterių tinklo, turi būti naudojamas dviejų veiksnių autentifikavimas. Autentifikavimo veiksniais gali būti slaptažodžiai, saugumo žetonai, USB raktai su slapta žyma, biometriniai duomenys ir kt.		
48.	Turi būti naudojamas įrenginio autentifikavimas, garantuojantis, kad		

	asmens duomenys tvarkomi tik naudojant konkrečius tinklo įrenginius (pvz., 802.1X, RADIUS ir kt.).		
Techninių žurnalų įrašai ir stebėsena			
49.	Techninių žurnalų įrašai turi būti įgyvendinti kiekvienai IT sistemai, naudojamai asmens duomenims tvarkyti. Techninių žurnalų įrašuose turi būti matoma visa įmanoma prieigų prie asmens duomenų informacija (pvz., data, laikas, peržiūrėjimo, keitimo, panaikinimo veiksmai). Rekomenduojamas saugojimo terminas – ne trumpiau kaip 6 mėnesiai.	**A.12.4 Įvykių registravimas ir stebėsena** **Papildomi reikalavimai dėl įvykių registravimo ISO 27701 – 6.9.4.1 ir dėl registruotos informacijos apsaugos ISO 27701 – 6.9.4.2**	Techninių žurnalų įrašai yra esminis saugos reikalavimas, kuris leidžia identifikuoti ir stebėti, sekti naudotojų veiksmus (kurie susiję su asmens duomenų tvarkymu), taip užtikrinant atskaitingumą (jei įvyktų neautorizuotas asmens duomenų atskleidimas, keitimas ar panaikinimas). Taip pat svarbu nuolat stebėti techninių žurnalų įrašus, kurie leistų identifikuoti potencialius vidinius ar išorinius bandymus pažeisti sistemos saugumą ir integralumą. **Galimos grėsmės ir pavojai** Sudėtingas autorizuotų ir neautorizuotų naudotojų atliktų veiksmų atsekamumas, galimas atliktų veiksmų slėpimas, užmaskavimas; esamų ir sukauptų techninių žurnalų įrašų redagavimas, klastojimas, naikinimas (angl. *log file cleaning*). Datos ir laiko redagavimas, klastojimas techninių žurnalų įrašuose (nenaudojant bendro, sinchronizuoto atskaitos mechanizmo); nenaudojama, neaktyvi techninių žurnalų įrašų pokyčių stebėsena, monitoringas.
50.	Techninių žurnalų įrašai turi turėti laiko žymas ir būti apsaugoti nuo galimo sugadinimo, suklastojimo ar neautorizuotos prieigos. IT sistemose naudojami laiko apskaitos mechanizmai turi būti sinchronizuoti pagal bendrą laiko atskaitos šaltinį.		
51.	Visi sistemų administratorių ir operatorių veiksmai (taip pat ir jų atliekamas vartotojo teisių papildymas, panaikinimas, keitimas) turi būti registruojami.		
52.	Turi būti neįmanoma ištrinti ar pakeisti techninių įrašų turinio. Prieiga prie įrašų		

	taip pat turi būti registruojama, siekiant atlikti neįprastų veiksmų susekimo stebėseną.		
53.	Stebėsenos sistema turi apdoroti techninius įrašus, ruošti sistemos būklės ataskaitas ir įspėti apie galimus pavojus.		
Tarnybinių stočių, duomenų bazių apsauga			
54.	Duomenų bazės ir taikomųjų programų tarnybinės stotys turi būti sukonfigūruotos taip, kad veiktų naudodamos atskiras paskyras su priskirtomis žemiausiomis operacinės sistemos (OS) privilegijomis.	**A.12 Darbo saugumas** **Papildomi reikalavimai dėl atsarginių kopijų, susijusių su asmens duomenimis** **ISO 27701 – 6.9.3.1**	Informacinių sistemų pagrindas yra tarnybinės stotys ir duomenų bazės. Jų apsauga privalo būti sustiprinta, siekiant užtikrinti saugią darbo aplinką. **Galimos grėsmės ir pavojai** Nekorektiški naudojamų operacinių sistemų, taikomųjų programų konfigūracijos nustatymai; gamyklinių nustatymų (angl. *default settings*), perteklinių funkcijų naudojimas, atnaujinimo funkcijų nepalaikymas. Programinės įrangos, servisų, perteklinių funkcijų vykdymas OS administratoriaus (angl. *root*) teisėmis; tiesioginė prieiga internetu prie tarnybinės stoties ir duomenų bazės įgyjant administratoriaus teises; neteisėtas tarnybinės stoties užvaldymas, duomenų bazės turinio peržiūrėjimas, kopijavimas, redagavimas, naikinimas. Atskiroje paskyroje (ne administratoriaus), su žemiausiomis operacinėmis sistemos privilegijomis, naudojant kelias, keliolika skirtingų taikomųjų programų, duomenų bazių iš skirtingų IT sistemų, neteisėtas tarnybinės stoties ir (ar) taikomosios programos užvaldymas suteiks prieigas prie visų tarnybinėje stotyje esančių duomenų bazių turinio. Galimas duomenų bazių turinio peržiūrėjimas, kopijavimas, redagavimas, naikinimas.
55.	Duomenų bazėse ir taikomųjų programų tarnybinėse stotyse turi būti tvarkomi tik tie asmens duomenys, kurie yra reikalingi darbui, atitinkančiam duomenų tvarkymo tikslus.		
56.	Konkrečioms saugomoms byloms ar įrašams apsaugoti turėtų būti naudojamas šifravimas, įdiegiant atitinkamą programinę ar techninę įrangą.		
57.	Duomenų bazėse turi būti taikomi pseudonimizavimo metodai, atskiriant tiesioginius identifikatorius nuo esamų sąsajų su kitais duomenimis.		

58.	Duomenų bazėje turi būti taikomi autorizuotų užklausų, šifruotos paieškos ir kiti privatumo užtikrinimo metodai.		
Darbo vietų apsauga			
59.	Naudotojams negalima turėti galimybės išjungti ar apeiti, išvengti IT sistemų saugos nustatymų.	**A.14.1 Informacinių sistemų saugumo reikalavimai** **Papildomi reikalavimai dėl viešųjų tinklų naudojimo** **ISO 27701 – 6.11.1.2**	Šis reikalavimas yra susijęs su saugos nustatymais naudotojų darbo stotyse ar kituose įrenginiuose. Yra svarbu priverstinai nustatyti specifinę saugos politiką ir apriboti naudotojų veiksmus, siekiant apsaugoti IT sistemas (pvz., antivirusinės programinės įrangos išjungimas, neautorizuotos programinės įrangos diegimas). **Galimos grėsmės ir pavojai** Galimybė apeiti, išjungti saugos nustatymus, antivirusines sistemas; vykdyti, kaupti neleistiną turinį; neteisėtai įgyti privilegijuotas naudotojo teises (administratoriaus). Neteisėtas tarnybinių, darbo stočių užvaldymas, neautorizuotos prieigos prie duomenų bazės turinio. Negebėjimas aptikti, užkardyti ir informuoti apie nustatytus netinkamus, piktybiškus naudotojų veiksmus, naudotojų kaupiamą neleistiną turinį, išorės atakas. Neleistinos, kenksmingos programinės įrangos diegimas, vykdymas, siekiant užvaldyti tarnybinę, darbo stotį, neteisėtai atskleisti informaciją apie kitus naudotojus ar įgyti prieigą prie duomenų bazės turinio. Apsaugos, antivirusinės programinės įrangos šalinimas, išjungimas, papildomų neteisėtų naudotojų paskyrų kūrimas. Nenutraukiant neaktyvaus naudotojo sesijos, galimi įvairūs socialinės inžinerijos metodai nukreipiant naudotojų dėmesį į pašalines detales, dėl to galimas neautorizuotas informacijos atskleidimas, neteisėtas programinės įrangos vykdymas, kenksmingos išorės laikmenos panaudojimas.
60.	Antivirusinės taikomosios programos ir jų informacijos apie virusus duomenų bazės turi būti atnaujinamos ne rečiau kaip kas savaitę, rekomenduojama kartą per parą ar dažniau.		
61.	Naudotojams negalima turėti privilegijų (teisių) diegti, šalinti, administruoti neautorizuotos programinės įrangos.		
62.	IT sistemos turi turėti nustatytą sesijos laiką, t. y. naudotojui esant neaktyviam sistemoje nustatytą laiką, jo sesija privalo būti nutraukta. Rekomenduojamas neaktyvios sesijos laikas – ne ilgiau kaip 15 min.		
63.	Kritiniai operacinės sistemos saugos atnaujinimai privalo būti diegiami reguliariai ir nedelsiant.		
64.	Antivirusinės taikomosios programos ir jų informacijos apie virusus bei kenkimo		

	programinę įrangą duomenų bazės turi būti atnaujinamos ne rečiau kaip kartą per parą.		Didelė grėsmė neteisėtai užvaldyti operacines sistemas tarnybinėse stotyse, kompiuterinėse darbo vietose, neteisėtai užvaldyti programinę įrangą, atskleisti duomenų bazių turinį.
65.	Turi būti uždrausta perduoti asmens duomenis iš kompiuterinių darbo vietų į išorinius saugojimo įrenginius (pvz., USB raktai, DVD, išorinius standžiuosius diskus ir kt.).		
66.	Pageidautina, kad asmens duomenų tvarkymui naudojamos kompiuterinės darbo vietos nebūtų prijungtos prie interneto, nebent būtų imamasi saugumo priemonių, kad būtų išvengta neteisėto asmens duomenų tvarkymo, kopijavimo ir perdavimo.		
67.	Kompiuterinėse darbo vietoje naudojamuose operacinės sistemos diskuose turi būti įgalintas pilnas standžiojo disko šifravimas (angl. *full-disk encryption*).		
Tinklo ir komunikacijos sauga			
68.	Kai prieiga prie naudojamų IT sistemų yra vykdoma internetu, privaloma naudoti šifruotą komunikacijos kanalą, t. y. kriptografinius protokolus (pvz., TLS/SSL).	**A.13 Ryšių saugumas** **Papildomi reikalavimai dėl informacijos perdavimo politikų ir procedūrų**	Tinklo ir komunikacijos sauga yra ypač svarbi, siekiant užtikrinti asmens duomenų saugą (tiek vidinių, tiek išorinių tinklų). Komunikacijai naudojamose susirašinėjimo programose, esant galimybei, rekomenduojama aktyvuoti ištisinio šifravimo (angl. *end-to-end encryption*) nuostatas. BDAR 32 straipsnis numato, kad „[...]atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo
69.	Belaidis ryšys prie IT sistemų turi būti leidžiamas tik tam tikriems vartotojams		

	ir procesams. Belaidžio ryšio potinklis turi būti atskirtas nuo kitų potinklių. Belaidė prieiga turi būti apsaugota patikimais šifravimo mechanizmais.	**ISO 27701 – 6.10.2.1 ir viešųjų tinklų naudojimo ISO 27701 – 6.11.1.2**	pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant *inter alia*, jei reikia: - pseudonimų suteikimą asmens duomenims ir jų šifravimą; - gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą [...]“. **Galimos grėsmės ir pavojai** Galimybė klausytis (angl. *sniff*) duomenų srautų, keliaujančių komunikacijos kanalu, bei galimybė perimti, modifikuoti keliaujančią informaciją (angl. *man-in-the-middle*). Pvz., vieši, belaidžiai, nemokamą interneto prieigą teikiantys taškai *(WiFi)* bei interneto svetainės, neužtikrinančios *SSL/TLS (HTTPS)* kriptografinių protokolų. Taip pat vidiniai įstaigų, organizacijų kompiuterių tinklai, nenaudojantys MAC adresų filtravimo, susiejimo su fiziniais *Ethernet* prievadais; nevykdomas kompiuterių tinklų duomenų srautų monitoringas, nevykdomas įsilaužimų aptikimas ir prevencija (pvz., *IDS/IPS*).
70.	Reikėtų vengti nuotolinės prieigos prie IT sistemų. Tais atvejais, kai ši prieiga yra išties reikalinga, ji yra galima tik organizacijos paskirtam darbuotojui (pvz., sistemų administratoriui, saugumo specialistui) kontroliuojant ir stebint jos veikimą per iš anksto nustatytus įrenginius.		
71.	Bet koks duomenų judėjimas iš, į IT sistemą turi būti stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo ir prevencijos sistemas.		
72.	Prisijungimas prie interneto neturi būti leidžiamas tarnybinėms stotims ir jose esančiai programinei įrangai, naudojamai asmens duomenims tvarkyti.		
73.	Informacinės sistemos tinklas turi būti atskirtas nuo kitų duomenų valdytojo tinklų.		
74.	Prieiga prie IT sistemos turi būti atliekama tik iš patvirtintų įrenginių ir terminalų, naudojant tam skirtas		

	technologijas, pvz., MAC adresų filtravimą arba tinklo prieigos kontrolę.		
	Atsarginės kopijos		
75.	Atsarginės kopijos ir duomenų atstatymo procedūros privalo būti apibrėžtos, dokumentuotos ir aiškiai susietos su vaidmenimis ir pareigomis.	**A.12.3 Atsarginės kopijos** **Papildomi reikalavimai dėl atsarginių kopijų, susijusių su asmens duomenimis** **ISO 27701 – 6.9.3.1**	Atsarginių kopijų sistema yra esminis veiksnys, užtikrinantis organizacijos darbo ir procesų atstatymą, įvykus duomenų praradimui ar sugadinimui. Duomenų kopijų darymo dažnumas ir poreikis priklauso nuo organizacijos ir joje tvarkomų asmens duomenų. BDAR 32 straipsnis numato „gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju“. **Galimos grėsmės ir pavojai** Esant nepakankamai apibrėžtai duomenų atstatymo procedūrai, galimas konfidencialios informacijos nutekėjimas, neteisėtas duomenų bazės turinio atskleidimas, programinės įrangos, operacinių sistemų informacijos, informacijos apie naudotojus atskleidimas. Neautorizuotų asmenų patekimas į patalpas; įvairūs socialinės inžinerijos panaudojimo metodai. Nekorektiškas atsarginių kopijų atlikimo bei duomenų iš atsarginių kopijų atstatymo procesas lemia negrįžtamą duomenų praradimą, neužtikrinamą duomenų prieinamumą, nutekėjimą.
76.	Atsarginių kopijų laikmenoms privalo būti užtikrintas tinkamas fizinis aplinkos, patalpų saugos lygis, priklausantis nuo saugomų duomenų.		
77.	Atsarginių kopijų darymo procesas turi būti stebimas, siekiant užtikrinti užbaigtumą ir išsamumą.		
78.	Pilnos atsarginės duomenų kopijos privalo būti daromos reguliariai. Rekomenduojamas atsarginių kopijų darymo dažnumas: - kasdien – pridedamoji kopija; - kas savaitę – pilna kopija.		
79.	Atsarginės kopijos turi būti reguliariai testuojamos, siekiant užtikrinti, kad jos galėtų būti patikimai naudojamos ekstremalioje situacijoje.		
80.	Reguliarus atsarginių kopijų kūrimas ar bent reguliarus papildantysis (angl. *incremental*) atsarginių kopijų kūrimas turi būti atliekamas bent kartą per parą.		

81.	Atsarginės kopijos turi būti saugiai laikomos skirtingose vietose, kurios turi būti geografiškai nutolusios viena nuo kitos.		
82.	Atsarginės kopijos turi būti šifruojamos ir saugiai laikomos visiškai atjungus (angl. *offline*) nuo kompiuterinių tinklų.		
Mobilieji, nešiojamieji įrenginiai			
83.	Mobiliųjų, nešiojamųjų įrenginių administravimo procedūros privalo būti nustatytos ir dokumentuotos, aiškiai aprašant tinkamą tokių įrenginių naudojimą.	**A.6.2 Mobilieji įrenginiai ir nuotolinis darbas** **Papildomi reikalavimai dėl saugumo politikos ISO 27701 – 6.2.1**	Mobilieji, nešiojamieji įrenginiai gali išplėsti paslaugas, kurias teikia duomenų valdytojas, tačiau padidina juose esančių duomenų nutekėjimo riziką. Mobiliuosius ir nešiojamuosius įrenginius, tokius kaip išmanieji telefonai ar planšetiniai kompiuteriai, naudotojai gali panaudoti savo asmeninėms reikmėms, todėl reikia užtikrinti, kad naudotojų asmens duomenys ir organizacijoje administruojami asmens duomenys nebūtų atskleisti. **Galimos grėsmės ir pavojai** Galimi įvairūs socialinės inžinerijos metodai, siekiant surinkti patalpų, darbo aplinkos informaciją, informaciją apie darbuotojus; neteisėtas fotografijų, vaizdo, garso įrašų darymas. Pvz., IT infrastruktūros fotografavimas, naudojamos kompiuterinės, programinės įrangos, prisijungimų (slaptažodžių) informacijos surinkimas. Mobilieji ir nešiojami įrenginiai be naudotojo žinios gali persiųsti informaciją trečiosioms šalims, galimas neautorizuotas informacijos atskleidimas, nutekėjimas.
84.	Mobilieji ir nešiojamieji įrenginiai, kuriais bus naudojamasi darbui su informacinėmis sistemomis, prieš naudojimąsi turi būti užregistruoti ir autorizuoti.		
85.	Mobilieji, nešiojamieji įrenginiai turi būti pakankamo prieigos kontrolės procedūrų lygio, kaip ir kita naudojama įranga asmens duomenims tvarkyti.		
86.	Mobiliųjų, nešiojamųjų įrenginių valdymo funkcijos ir atsakomybės turi būti aiškiai apibrėžtos.		
87.	Organizacija turi turėti galimybę nuotoliniu būdu ištrinti asmens duomenis mobiliajame, nešiojamame		

	įrenginyje, kurio saugumas buvo sukompromituotas (pvz., pažeistos saugumo nuostatos, prarastas patikimumas).		
88.	Mobiliuosiuose, nešiojamuosiuose įrenginiuose turi būti atskirti privatūs ir organizacijos veiklos duomenys, naudojant saugias programinės įrangos talpyklas (konteinerius).		
89.	Nenaudojami mobilieji, nešiojamieji įrenginiai turi būti fiziškai apsaugoti nuo vagystės.		
90.	Prieigai prie mobiliųjų, nešiojamųjų įrenginių turėtų būti naudojamas dviejų veiksnių autentifikavimas.		
91.	Asmens duomenys, saugomi mobiliajame įrenginyje (kaip organizacijos duomenų tvarkymo operacijos dalis), turi būti užšifruoti.		
Programinės įrangos sauga			
92.	Informacinėse sistemose naudojama programinė įranga (asmens duomenims tvarkyti) turi atitikti programinės įrangos saugos gerąją praktiką, programinės įrangos kūrime taikomą saugos gerąją praktiką, programinės įrangos kūrimo struktūras (angl.	**A.12.6 Techninio pažeidžiamumo valdymas ir A.14.2 Kūrimo ir priežiūros procesų saugumas**	Visuose programinės įrangos kūrimo ir administravimo etapuose organizacija turi užtikrinti duomenų saugos laikymąsi, asmens duomenų apsaugą. BDAR 25 straipsnyje yra aprašomi duomenų apsaugos principai kuriant programinę įrangą, baziniai programinės įrangos saugumo nustatymai, kurių reikalaujama iš duomenų valdytojų, užtikrinant griežčiausius privatumo nustatymus. Projektuojant ir kuriant naujas programinės įrangos sistemas, kuriose numatoma tvarkyti asmens duomenis, būtina laikytis BDAR 25 straipsnyje

	frameworks), standartus (pvz., Agile, OWASP ir kt.).	**Papildomi reikalavimai dėl viešųjų tinklų naudojimo** **ISO 27701 – 6.11.1.2,** **saugaus įrangos kūrimo politikos** **ISO 27701 – 6.11.2.1,** **sistemų inžinerijos saugumo principų** **ISO 27701 – 6.11.2.5,** **nuotolinio programinės įrangos kūrimo** **ISO 27701 – 6.11.2.7** **ir testinių duomenų** **ISO 27701 – 6.11.3.1**	(Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga – angl. *Privacy by Design and Privacy by Default*) numatytų principų. **Galimos grėsmės ir pavojai** Galimos programinės įrangos spragos (angl. *bug*), sutrikimai (angl. *malfunction*). Galimybės pasinaudoti programinės įrangos spragomis siekiant apeiti, išjungti programinės įrangos saugą, užvaldyti programinę įrangą, įgyti privilegijuotas teises (administratoriaus), administruoti naudotojų paskyras, tarnybines, darbo stotis, kuriose yra talpinama programinė įranga.
93.	Specifiniai saugos reikalavimai, susiję su organizacijos veiklos ypatumais, turi būti apibrėžti pradiniuose programinės įrangos kūrimo etapuose.		
94.	Turi būti laikomasi duomenų saugą užtikrinančių programavimo standartų ir gerosios praktikos.		
95.	Po programinės įrangos kūrimo, testavimo ir verifikacijos, pradedant sistemos įdiegimą ir eksploataciją, jau turi būti laikomasi pagrindinių saugos reikalavimų.		
96.	Prieš paleidžiant programinę įrangą, turi būti atliktas programinės įrangos ir infrastruktūros pažeidžiamumo ir atsparumo skverbimuisi įvertinimas. Programinė įranga negali būti priimta naudoti, kol nėra pasiektas reikiamas saugumo lygis.		
97.	Turi būti atliekami periodiški infrastruktūros atsparumo skverbimuisi testavimai.		
98.	Programinės įrangos atnaujinimai turi būti ištestuoti ir įvertinti prieš juos diegiant į darbo aplinką atitinkamomis veiklos sąlygomis.		

Duomenų naikinimas, šalinimas			
99.	Prieš pašalinant bet kokią duomenų laikmeną, turi būti sunaikinti visi joje esantys duomenys, naudojant tam skirtą programinę įrangą, kuri palaiko patikimus duomenų naikinimo algoritmus. Jei to padaryti neįmanoma (pvz., DVD laikmenos), turi būti įvykdytas fizinis duomenų laikmenos sunaikinimas be galimybės atstatyti.	**A.8.3.2 Duomenų laikmenų naikinimas ir A.11.2.7 Saugus įrangos naikinimas arba pakartotinis naudojimas** **Papildomi reikalavimai dėl naikinimo ir pakartotinio naudojimo ISO 27701 – 6.8.2.7 ir dėl popierinių laikmenų ISO 27701 – 6.8.2.9**	Pagrindinis duomenų naikinimo tikslas yra negrįžtamas asmens duomenų šalinimas, sunaikinimas be teorinės ir praktinės galimybės juos pakartotinai nuskaityti ar atstatyti. Kai yra šalinama pasenusi, nenaudojama, nebereikalinga techninė įranga, duomenų valdytojas privalo užtikrinti, kad visi prieš tai joje buvę sukaupti asmens duomenys būtų negrįžtamai sunaikinti. Pagal BDAR 5 straipsnį asmens duomenys neturi būti saugomi, kaupiami ilgiau, negu tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi. Kai kuriais atvejais duomenų subjektai turi teisę reikalauti duomenis sunaikinti anksčiau, negu yra nustatytas duomenų saugojimo, kaupimo terminas. **Galimos grėsmės ir pavojai** Nekorektiškai naikinant informaciją iš duomenų laikmenų (kai laikmenos be patikros tiesiogiai išmetamos kartu su kita elektronine įranga; laikmenos, be patikros yra perduodamos sunaikinti trečiosioms šalims; laikmenos, be patikros, yra parduodamos varžytinėse ir pan.), atsiranda galimybė atkurti neautorizuotą turinį (pvz., standieji diskai, DVD laikmenos, USB raktai ir kt.). Galimi socialinės inžinerijos metodai, kai popierinės laikmenos, išorinės laikmenos (kietieji diskai ir pan.) nėra fiziškai sunaikinami, o tiesiogiai šalinami (išmetami) į atitinkamus popierinės ar elektroninės įrangos konteinerius esančius šalia įstaigos, įmonės.
100.	Popierinės ir nešiojamosios duomenų laikmenos (pvz., DVD laikmenos), kuriose buvo saugomi, kaupiami asmens duomenys, turi būti naikinamos tam skirtais smulkintuvais arba kitomis mechaninėmis priemonėmis		
101.	Prieš šalinant laikmenas, turi būti atlikti visų šalinamų laikmenų daugybiniai programinės įrangos perrašymai (angl. *Multiple passes of software-based overwriting*).		
102.	Jei saugiems duomenų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti sudaryta atitinkama paslaugų sutartis ir atliekamas sunaikintų įrašų protokolavimas.		

103.	Po duomenų ištrynimo reikėtų imtis papildomų priemonių, pvz., gali būti atliktas nepageidaujamos magnetinės informacijos pašalinimas (išmagnetinimas). Priklausomai nuo konkretaus atvejo, reikėtų įvertinti fizinio sunaikinimo galimybes.		
104.	Jei saugiems įrašų naikinimo ir šalinimo duomenų laikmenose ar popieriniuose dokumentuose darbams atlikti yra pasitelkiamos trečiosios šalies paslaugos, turi būti užtikrinta, kad šis procesas vyktų duomenų valdytojo ir (ar) tvarkytojo patalpose, siekiant išvengti duomenų perdavimo trečiosioms šalims. Atskirais atvejais, kai to neįmanoma atlikti duomenų valdytojo ir (ar) tvarkytojo patalpose, sunaikinimas gali būti atliekamas kitoje fizinėje vietoje, tačiau tik stebint įgaliotam duomenų valdytojo atstovui.		
Fizinė sauga			
105.	Turi būti įgyvendinta fizinė aplinkos, patalpų, kuriose yra IT sistemų infrastruktūra, apsauga nuo neautorizuotos prieigos.	**A.11 Fizinis ir aplinkos saugumas**	Fizinė apsauga yra ne mažiau svarbi, negu technologinės saugumo priemonės, nes tiesioginės fizinės prieigos kontrolė prie IT infrastruktūros yra visos taikomos saugos strategijos pagrindas. **Galimos grėsmės ir pavojai**
106.	Būtina naudoti aiškią visų darbuotojų ir lankytojų identifikavimo sistemą,		

	naudojant tinkamas priemones, pvz., visiems norintiems patekti į organizacijos patalpas tapatybę patvirtinančius darbo leidimus.		Dažnai tarnybinės stotys (su IT sistemomis) ir tinklo įranga nėra specialioje izoliuotoje, saugomoje spintoje ar patalpoje; tarnybinės stotys yra fiziškai prieinamos, pasiekiamos naudotojams ar pašaliniams asmenims. Galimas neautorizuotas tarnybinės stoties užvaldymas, konfidencialios informacijos atskleidimas.
107.	Atitinkamos saugios zonos turėtų būti apibrėžtos ir apsaugotos tinkamomis patekimo kontrolės priemonėmis. Popierinis ar elektroninis registravimo rinkmenų žurnalas turi būti saugiai laikomas, prižiūrimas ir stebimas.		
108.	Įsilaužimo (įsibrovimo) aptikimo sistemos turi būti įdiegtos visose saugumo zonose.		
109.	Prireikus turi būti kuriamos fizinės kliūtys, kad būtų užkirstas kelias neteisėtam fiziniam prieinamumui.		
110.	Laisvos saugios zonos turi būti fiziškai rakinamos ir periodiškai patikrinamos.		
111.	Tarnybinių stočių patalpoje turėtų būti įdiegta automatinė gaisro gesinimo sistema, uždara valdoma oro kondicionavimo sistema ir nepertraukiamo maitinimo šaltinis.		
112.	Išorės subjektų personalui, įgyvendinančiam teikiamas palaikymo paslaugas, turi būti suteikta ribota prieiga prie saugių zonų.		