Organizacinių ir techninių
kibernetinio saugumo reikalavimų,
taikomų kibernetinio saugumo
subjektams, aprašo
priedas

TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ, TAIKOMŲ SUBJEKTAMS, VALDANTIEMS IR (ARBA) TVARKANTIEMS VALSTYBĖS INFORMACINIUS IŠTEKLIUS, YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VALDYTOJAMS, SĄRAŠAS

Eil. Nr.	Reikalavimas, taikomas subjektui, valdančiam ir (arba) tvarkančiam valstybės informacinį išteklių (VII) ar ypatingos svarbos informacinę infrastruktūrą (YSII)	YSII	VII rūšys pagal duomenų svarbą			
			Ypatingos svarbos	Svarbūs	Vidutinės svarbos	Mažos svarbos
I SKYRIUS. ATPAŽINTIES, TAPATUMO PATVIRTINIMO IR NAUDOJIMOSI SAUGUMAS IR KONTROLĖ						
1.	VII ar YSII priežiūrą vykdančio asmens (toliau – administratorius) funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms VII ar YSII naudotojo funkcijoms atlikti	x	x	x	x	x
2.	VII ar YSII naudotojams negali būti suteikiamos administratoriaus teisės	x	x	x	x	x
3.	Kiekvienas VII ar YSII naudotojas turi būti atpažįstamas	x	x	x	x	x
4.	Viešaisiais elektroninių ryšių tinklais perduodamos informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualųjį privatų tinklą (angl. *Virtual private network, VPN*)	x	x	x	x	x
5.	VII ar YSII naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone	x	x	x	x	x
6.	VII ar YSII naudotojų ir administratorių tapatumui patvirtinti turi būti naudojamos dviejų veiksnių tapatumo patvirtinimo priemonės (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x		
7.	VII ar YSII naudotojo teisė dirbti su konkrečiu VII ar YSII turi būti sustabdoma, kai VII ar YSII naudotojas nesinaudoja VII ar YSII ilgiau kaip tris mėnesius (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x	x	x
8.	Administratoriaus teisė dirbti su VII ar YSII turi būti sustabdoma, kai administratorius nesinaudoja VII ar YSII ilgiau kaip 2 mėnesius (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x	x	x
9.	Kai VII ar YSII naudotojas ar administratorius nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų VII ar YSII naudotojo ar administratoriaus kvalifikacinių reikalavimų, taip	x	x	x	x	x

	pat pasibaigia jo darbo (tarnybos) santykiai, jis praranda patikimumą, jo teisė naudotis VII ar YSII turi būti panaikinta nedelsiant					
10.	Nereikalingos ar nenaudojamos VII ar YSII naudotojų ir administratoriaus paskyros turi būti blokuojamos nedelsiant ir ištrinamos praėjus audito duomenų nustatytam saugojimo terminui	x	x	x	x	x
11.	Baigus darbą arba VII ar YSII naudotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri tvarkoma VII ar YSII, negalėtų susipažinti pašaliniai asmenys: turi būti atsijungiama nuo VII ar YSII, įjungiama ekrano užsklanda su slaptažodžiu (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x	x	x
12.	VII ar YSII naudotojui VII ar YSII neatliekant jokių veiksmų, darbo stotis turi užsirakinti, kad toliau naudotis VII ar YSII būtų galima tik pakartotinai patvirtinus savo tapatybę (jeigu VII ar YSII dalys palaiko tokį funkcionalumą). Laikas, per kurį VII ar YSII naudotojui neatliekant jokių veiksmų darbo stotis užsirakina, nustatomas kibernetinio saugumo politikos ir jos įgyvendinimo dokumentuose, tačiau negali būti ilgesnis kaip 15 minučių. Šis reikalavimas netaikomas, jeigu, atlikus ryšių ir informacinių sistemų rizikos vertinimą, nustatomos kitos nustatytą riziką atitinkančios techninės kibernetinio saugumo priemonės	x	x	x	x	x
13.	Prisijungimo prie VII ar YSII slaptažodžių reikalavimai:					
13.1.	slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių	x	x	x	x	x
13.2.	slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai)	x	x	x	x	x
13.3.	draudžiama slaptažodžius atskleisti kitiems asmenims	x	x	x	x	x
13.4.	VII ar YSII dalys, patvirtinančios VII ar YSII naudotojo tapatumą, turi drausti išsaugoti slaptažodžius (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x	x	x
13.5.	turi būti nustatytas didžiausias leistinas VII naudotojo mėginimų įvesti teisingą slaptažodį skaičius (ne daugiau kaip 5 kartai) (jeigu VII palaiko tokį funkcionalumą). Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta, VII naudotojo paskyra turi užsirakinti ir neleisti VII naudotojui patvirtinti tapatybės kibernetinio saugumo politikos ir jos įgyvendinimo dokumentuose nustatytą laiką – ne trumpiau kaip penkiolika minučių (jeigu VII dalys palaiko tokį funkcionalumą)			x	x	x
13.6.	turi būti nustatytas didžiausias leistinas VII ar YSII naudotojo mėginimų įvesti teisingą slaptažodį skaičius – ne daugiau kaip 3 kartai (jeigu VII ar YSII dalys palaiko tokį funkcionalumą). Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta, VII ar YSII naudotojo paskyra turi užsiblokuoti ir turi būti informuojamas administratorius (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x			
13.7.	slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Kompetentingo asmens ar	x	x	x	x	x

	padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jeigu VII ar YSII naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių VII ar YSII naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu					
14.	Papildomi VII ar YSII naudotojo slaptažodžių reikalavimai:					
14.1.	slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius	x	x	x	x	x
14.2.	slaptažodį turi sudaryti ne mažiau kaip 8 simboliai (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x	x	x
14.3.	keičiant slaptažodį, VII ar YSII neturi leisti sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x	x	x
14.4.	pirmąkart jungiantis prie VII ar YSII, turi būti reikalaujama, kad VII ar YSII naudotojas pakeistų slaptažodį (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x	x	x
15.	Papildomi administratorių slaptažodžių reikalavimai:					
15.1.	slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius	x	x	x	x	x
15.2.	slaptažodį turi sudaryti ne mažiau kaip 12 simbolių (jeigu VII ar YSII dalys palaiko tokį funkcionalumą) arba slaptažodį turi sudaryti ne mažiau kaip 8 simboliai, jeigu naudojamos dviejų veiksnių tapatumo patvirtinimo priemonės	x	x	x	x	x
15.3.	keičiant slaptažodį, taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 3 paskutinių slaptažodžių (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x	x	x
15.4.	turi būti patvirtinti asmenų, kuriems suteiktos administratoriaus teisės prisijungti prie VII ar YSII, sąrašai, periodiškai peržiūrimi kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą. Sąrašas turi būti nedelsiant peržiūrėtas, kai administratorius nušalinamas arba pasibaigia jo darbo (tarnybos) santykiai	x	x	x	x	
16.	Turi būti vykdoma administratorių paskyrų kontrolė:					
16.1.	periodiškai tikrinama, ar administratoriaus paskyros atitinka šiame skyriuje nustatytus reikalavimus				x	x
16.2.	naudojamos administratorių paskyrų kontrolės priemonės, kurios tikrina administratoriaus paskyras. Apie administratoriaus paskyras, kurios neatitinka šiame skyriuje nustatytų reikalavimų, turi būti pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą	x	x	x		
17.	Vykdoma VII ar YSII naudotojų paskyrų kontrolė:					
17.1.	tikrinama, ar VII ar YSII naudotojų paskyros atitinka šiame skyriuje nustatytus reikalavimus, ir pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, apie VII ar YSII naudotojų paskyras, kurios neatitinka šiame skyriuje				x	x

	nustatytų reikalavimų					
17.2.	naudojamos VII ar YSII naudotojų paskyrų kontrolės priemonės, kurios periodiškai tikrina VII ar YSII naudotojų paskyras. Apie VII ar YSII naudotojų paskyras, kurios neatitinka šiame skyriuje nustatytų reikalavimų, turi būti pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą	x	x	x		
17.3.	draudžiama VII ar YSII techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į šiame skyriuje nustatytus reikalavimus	x	x	x	x	x
II SKYRIUS. NAUDOTOJŲ IR ADMINISTRATORIŲ ATLIEKAMŲ VEIKSMŲ AUDITAS IR KONTROLĖ						
18.	Auditui atlikti turi būti fiksuojama ši informacija:					
18.1.	VII ar YSII elementų įjungimas, išjungimas ar perkrovimas (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x	x	x
18.2.	VII ar YSII naudotojų, administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti), atsijungimas	x	x	x	x	x
18.3.	VII ar YSII naudotojų, administratorių teisių naudotis sistemos, tinklo ištekliais pakeitimai (jeigu VII ar YSII dalys palaiko tokį funkcionalumą)	x	x	x		
18.4.	audito funkcijos įjungimas, išjungimas	x	x	x	x	x
18.5.	audito įrašų trynimas, kūrimas ar keitimas	x	x	x	x	x
18.6.	laiko ir (ar) datos pakeitimai	x	x	x		
18.7.	audituojamų įrašų laiko žymos turi būti sinchronizuotos ne mažiau kaip vienos sekundės tikslumu	x	x	x		
18.8.	turi būti naudojami mažiausiai 2 laiko sinchronizavimo šaltiniai	x	x			
19.	Kiekviename audito duomenų įraše turi būti fiksuojama:					
19.1.	įvykio data ir tikslus laikas	x	x	x	x	x
19.2.	įvykio rūšis, pobūdis	x	x	x		
19.3.	VII ar YSII naudotojo / administratoriaus ir (arba) VII ar YSII įrenginio, susijusio su įvykiu, duomenys	x	x	x	x	x
19.4.	įvykio rezultatas	x	x	x	x	x
20.	Priemonės, naudojamos VII ar YSII sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais	x	x	x		
21.	VII ar YSII fiksuojami įvykiai turi būti saugomi techninėje ar programinėje įrangoje, pritaikytoje audito duomenims saugoti	x	x	x		
22.	Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant, bet ne vėliau kaip per vieną darbo dieną turi būti informuojamas administratorius ir kompetentingas asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	x	x	x		

23.	Audito duomenys turi būti saugomi ne trumpiau kaip 60 kalendorinių dienų, užtikrinant šio priedo 19 punkte nurodytas turinio reikšmes	x	x	x		
24.	Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas	x	x	x	x	x
25.	Audito duomenų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo	x	x	x		
26.	Naudojimasis audito duomenimis turi būti kontroliuojamas ir fiksuojamas. Audito duomenys turi būti pasiekiami tik administratoriui ir kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą (peržiūros teisėmis)	x	x	x		
27.	Audito įrašų duomenys turi būti analizuojami administratoriaus ne rečiau kaip kartą per mėnesį ir apie analizės rezultatus informuojamas kompetentingas asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	x	x	x		
III SKYRIUS. ĮSIBROVIMŲ APTIKIMAS IR PREVENCIJA						
28.	Turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų į VII ar YSII įeinantį ir iš jo išeinantį duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų	x	x	x	x	x
29.	Įtartina veikla turi būti užfiksuojama audito įrašuose ir kuriamas pranešimas, kurį matytų administratorius	x	x	x		
30.	Sukurtas pranešimas turi būti klasifikuojamas pagal užfiksuotą įvykį	x	x	x		
31.	Įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu VII ar YSII valdytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio VII ar YSII veiklai vertinimas (testavimas)	x	x	x		
32.	Pagrindinėse tarnybinėse stotyse turi būti įjungtos saugasienės, sukonfigūruotos visam įeinančiam ir išeinančiam, išskyrus su VII ar YSII funkcionalumu ir administravimu susijusiam, duomenų srautui blokuoti	x	x	x	x	x
33.	VII elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant saugasienę; saugasienės įvykių žurnalai (angl. *Logs*) turi būti reguliariai analizuojami, o saugasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos		x	x	x	x
34.	VII tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenkimo kodo		x	x	x	x
35.	Įsilaužimo aptikimo konfigūracijos ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo VII ar YSII techninės įrangos (kartu nurodant atitinkamas datas	x	x	x	x	x

	(įgyvendinimo, atnaujinimo ir panašiai), atsakingus asmenis, taikymo periodus ir panašiai)					
IV SKYRIUS. BELAIDŽIO TINKLO SAUGUMAS IR KONTROLĖ						
36.	Leidžiama naudoti tik su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidžio tinklo įrenginius (toliau – belaidis įrenginys), atitinkančius techninius kibernetinio saugumo reikalavimus	x	x	x	x	x
37.	Turi būti vykdoma belaidžių įrenginių kontrolė:					
37.1.	tikrinami VII ar YSII eksploatuojami belaidžiai įrenginiai, kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, pranešama apie neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius	x	x	x	x	x
37.2.	naudojamos priemonės, kurios apribotų neleistinų ar saugumo reikalavimų neatitinkančių belaidžių įrenginių naudojimą arba informuotų kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą	x	x	x		
37.3.	leidžiama naudoti tik su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidės prieigos taškus	x	x	x	x	x
38.	Belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, kontroliuojamoje zonoje	x	x	x	x	x
39.	Prisijungiant prie belaidžio tinklo, turi būti taikomas ryšių ir informacinių sistemų naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas	x	x	x	x	x
40.	Turi būti uždrausta belaidėje sąsajoje naudoti SNMP (angl. *Simple Network Management Protocol*) protokolą	x	x	x	x	x
41.	Turi būti uždrausti visi nebūtini valdymo protokolai	x	x	x	x	x
42.	Turi būti išjungti nenaudojami TCP (angl. *Transmission Control Protocol*) / UDP (angl. *User Datagram Protocol*) prievadai	x	x	x	x	x
43.	Turi būti uždraustas lygiarangis (angl. *peer to peer*) funkcionalumas, neleidžiantis belaidžiais įrenginiais palaikyti ryšio tarpusavyje	x	x	x	x	x
44.	Belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu	x	x	x	x	x
45.	Prieš pradedant šifruoti belaidį ryšį, belaidės prieigos stotelėje turi būti pakeisti standartiniai gamintojo raktai	x	x	x	x	
46.	Kompiuteriuose, mobiliuosiuose įrenginiuose turi būti išjungta belaidė prieiga, jeigu jos nereikia darbo funkcijoms atlikti, išjungtas lygiarangis (angl. *peer to peer*) funkcionalumas, belaidė periferinė prieiga	x	x	x		
V SKYRIUS. MOBILIŲJŲ ĮRENGINIŲ, NAUDOJAMŲ PRISIJUNGTI PRIE VII AR YSII, SAUGUMAS IR KONTROLĖ						
47.	Atpažinties, tapatumo patvirtinimo ir naudojimosi VII ar YSII saugumo ir kontrolės reikalavimai, nurodyti šio priedo 1–19.3 punktuose, taikytini pagal VII ar YSII svarbos kategoriją	x	x	x	x	x

48.	Leidžiama naudoti tik mobiliuosius įrenginius, atitinkančius VII ar YSII valdytojo arba jo įgalioto tvarkytojo nustatytus saugumo reikalavimus	x	x	x	x	x
49.	VII ar YSII valdytojas turi turėti teises valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą	x	x	x	x	
50.	Turi būti vykdoma mobiliųjų įrenginių kontrolė:					
50.1.	tikrinami VII ar YSII naudojami mobilieji įrenginiai, kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, pranešama apie neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius	x	x	x	x	x
50.2.	naudojamos priemonės, kurios apribotų neleistinų ar saugumo reikalavimų neatitinkančių mobiliųjų įrenginių naudojimą ar kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, informuotų apie neleistinos mobiliosios įrangos prijungimą prie VII ar YSII	x	x	x		
51.	Mobiliuosiuose įrenginiuose privalo būti naudojamos centralizuotai valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, užkardymo ir stebėjimo priemonės	x	x			
52.	Turi būti įdiegiamos operacinės sistemos ir kiti naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai	x	x	x	x	x
53.	Mobiliuosiuose įrenginiuose turi būti naudojamos vykdomojo kodo (angl. *Executable code*) kontrolės priemonės, apribojančios neleistino vykdomojo kodo naudojimą ar informuojančios administratorių apie neleistino vykdomojo kodo naudojimą	x	x			
54.	Turi būti parengti mobiliųjų įrenginių operacinių sistemų atvaizdai su saugumo nuostatomis. Atvaizde turi būti nustatyti tik veiklai būtini operacinių sistemų komponentai (administravimo paskyros, paslaugos (angl. *Services*), taikomosios programos, tinklo prievadai, atnaujinimai, sisteminės priemonės). Atvaizdai turi būti reguliariai peržiūrimi ir atnaujinami, iškart atnaujinami nustačius naujų pažeidžiamumų ar atakų	x	x	x		
55.	Pagal parengtus atvaizdus į mobiliuosius įrenginius turi būti įdiegiama operacinė sistema su saugumo nuostatomis	x	x	x		
56.	Mobilieji įrenginiai, kuriais naršoma internete, turi būti apsaugoti nuo judriųjų programų (angl. *Mobile code*) keliamų grėsmių	x	x	x		
57.	Prie mobiliųjų įrenginių draudžiama prijungti jiems nepriklausančius įrenginius	x	x	x		
58.	VII ar YSII valdytojo arba jo įgalioto tvarkytojo sprendimu prie mobiliųjų įrenginių gali būti jungiami kiti įrenginiai. Administratoriaus parengtą, su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintą leistinų jungti įrenginių sąrašą tvirtina VII ar YSII valdytojas arba jo įgaliotas tvarkytojas	x	x			
59.	Duomenys, perduodami tarp mobiliojo įrenginio ir VII ar YSII, turi būti šifruojami taikant	x	x	x	x	

	virtualaus privataus tinklo (angl. *VPN*) technologiją					
60.	Jungiantis prie VII ar YSII, turi būti patvirtinamas tapatumas; mobiliajame įrenginyje ar jo taikomojoje programinėje įrangoje turi būti uždrausta išsaugoti slaptažodį	x	x	x	x	
61.	Nešiojamasis prietaisas, gaunantis energiją iš integruoto energijos šaltinio ir turintis galimybę perduoti ir (ar) priimti ir apdoroti elektroninius duomenis, siunčiamus fizine terpe, elektromagnetinėmis bangomis ir šviesa, kuriuo nesinaudojama nustatytą laiką (pavyzdžiui, penkias minutes), turi automatiškai užsirakinti	x	x	x		
62.	Mobiliuosiuose įrenginiuose privalo būti įdiegtos priemonės, leisiančios nuotoliniu būdu neatkuriamai ištrinti duomenis	x	x			
63.	Turi būti užtikrinta kompiuterinių laikmenų apsauga	x	x	x	x	x
64.	Turi būti šifruojami duomenys ir mobiliųjų įrenginių laikmenose, ir išorinėse kompiuterinėse laikmenose	x	x	x		
VI SKYRIUS. VII AR YSII NAUDOJAMOS INTERNETO SVETAINĖS, PASIEKIAMOS IŠ VIEŠŲJŲ ELEKTRONINIŲ RYŠIŲ TINKLŲ, SAUGUMAS IR KONTROLĖ						
65.	Taikomi atpažinties, tapatumo patvirtinimo ir naudojimosi VII ar YSII saugumo ir kontrolės reikalavimai, nurodyti šio priedo I skyriuje	x	x	x	x	x
66.	Papildomi atpažinties, tapatumo patvirtinimo ir naudojimosi kontrolės reikalavimai:					
66.1.	draudžiama slaptažodžius saugoti programiniame kode	x	x	x	x	x
66.2.	svetainės, patvirtinančios nuotolinio prisijungimo tapatumą, turi drausti išsaugoti slaptažodžius	x	x	x	x	
67.	Turi būti įgyvendinti svetainės kriptografijos reikalavimai:					
67.1.	atliekant svetainės administravimo darbus, ryšys turi būti šifruojamas naudojant ne trumpesnį kaip 128 bitų raktą	x	x	x	x	x
67.2.	šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų	x	x	x	x	
67.3.	turi būti naudojamas TLS (angl. *Transport Layer Security*) standartas (1.2 versija arba naujesnė)	x	x	x		
67.4.	svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. *Hardware security module*)	x	x	x	x	
67.5.	visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. *fail securely*)	x	x	x		
67.6.	kriptografiniai raktai ir algoritmai turi būti valdomi pagal VII ar YSII valdytojo arba jo įgalioto tvarkytojo nustatytus reikalavimus	x	x	x	x	x
68.	Tarnybinės stoties, kurioje yra svetainė, svetainės saugos parametrai turi būti teigiamai įvertinti naudojant Nacionalinio kibernetinio saugumo centro rekomenduojamą testavimo priemonę	x	x	x		
69.	Draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai	x	x	x	x	x

70.	Turi būti naudojama svetainės saugasienė (angl. *Web Application Firewall*). Įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu VII ar YSII valdytojo arba jo įgalioto tvarkytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio VII ar YSII veiklai vertinimas (testavimas)	x	x	x		
71.	Turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: struktūrizuotų užklausų kalbos įskverbties (angl. *SQL injection*), įterptinių instrukcijų atakų (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), paskirstyto atsisakymo aptarnauti (angl. *DDOS*) ir kitų, priemonės; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP)*) interneto svetainėje www.owasp.org	x	x	x	x	x
72.	Turi būti naudojama svetainės naudotojo įvedamų duomenų tikslumo kontrolė (angl. *Validation*)	x	x	x	x	
73.	Tarnybinė stotis, kurioje yra svetainė, neturi rodyti svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį	x	x	x	x	
74.	Svetainės saugumo priemonės turi gebėti uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir panašiai)	x	x	x		
75.	Taikomi atliekamų veiksmų audito ir kontrolės reikalavimai, nurodyti šio priedo II skyriuje	x	x	x	x	x
76.	Tarnybinė stotis, kurioje yra svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus protokolo (angl. *HTTP*) metodus	x	x	x	x	x
77.	Turi būti uždrausta naršyti svetainės aplankuose (angl. *Directory browsing*)	x	x	x	x	x
78.	Turi būti įdiegta svetainės turinio nesankcionuoto pakeitimo (angl. *Defacement*) stebėsenos sistema	x	x	x		
VII SKYRIUS. VII AR YSII NAUDOJAMO INTERNETO SAUGUMAS IR KONTROLĖ						
79.	VII ar YSII valdytojas arba jo įgaliotas tvarkytojas su interneto paslaugos teikėju (-ais) turi būti sudaręs šias sutartis:					
79.1.	reagavimo į kibernetinius incidentus įprastomis darbo valandomis	x	x	x	x	x
79.2.	reagavimo į kibernetinius incidentus po darbo valandų	x	x	x		
79.3.	nepertraukiamo interneto paslaugos teikimo:					
79.3.1.	įprastomis darbo valandomis				x	x
79.3.2.	24 valandas per parą, 7 dienas per savaitę	x	x	x		
79.4.	interneto paslaugos sutrikimų registravimo:					

79.4.1.	įprastomis darbo valandomis				x	x
79.4.2.	24 valandas per parą, 7 dienas per savaitę	x	x	x		
79.5.	apsaugos nuo VII ar YSII trikdymo taikymo (angl. *Denial of Service, DoS*)	x	x	x	x	x
VIII SKYRIUS. KITI VII REIKALAVIMAI						
80.	VII valdytojas arba jo įgaliotas tvarkytojas turi nustatyti maksimalų VII ar jos dalies neveikimo laikotarpį, kuris, siekiant užtikrinti tinkamą VII valdytojo ir tvarkytojo (-ų) funkcijų, kurioms atlikti buvo sukurtas VII, vykdymą, negali tęstis ilgiau nei:					
80.1.	mažos svarbos VII – 24 val.					x
80.2.	vidutinės svarbos VII – 16 val.				x	
80.3.	svarbūs VII – 12 val.			x		
80.4.	ypatingos svarbos VII – 8 val.		x			
81.	Reikalavimai VII techninei ir programinei įrangai ir patalpoms:					
81.1.	pagrindinė VII kompiuterinė įranga turi turėti įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį VII pagrindinės kompiuterinės įrangos veikimą		x	x	x	x
81.2.	svarbiausia kompiuterinė įranga ir duomenų perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį šios įrangos veikimą ne mažiau kaip 30 min.		x	x		
81.3.	jei VII tarnybinių stočių patalpose esančios įrangos bendras galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga		x	x	x	x
81.4.	tarnybinių stočių patalpose turi būti oro kondicionavimo ir drėgmės kontrolės įranga		x	x		
81.5.	VII tarnybinėse stotyse ir VII naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, stebėjimo realiu laiku priemonės; šios priemonės automatiškai turi informuoti VII administratorių apie tai, kurių VII posistemių, funkciškai savarankiškų sudedamųjų dalių kenkimo programinės įrangos aptikimo priemonių atsinaujinimo laikas yra pradelstas; VII komponentai be kenkimo programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu rizikos vertinimo metu patvirtinama, kad šių komponentų rizika yra priimtina		x	x	x	x
81.6.	turi būti operatyviai testuojami ir įdiegiami VII tarnybinių stočių ir VII naudotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai; VII administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie į VII posistemius, funkciškai savarankiškas sudedamąsias dalis, VII naudotojų darbo vietų kompiuterinę įrangą neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumų svarbos lygius		x	x	x	x
81.7.	VII tarnybinėse stotyse ir kompiuterinėje įrangoje turi būti naudojama tik legali programinė įranga, kurios sąrašą tvirtina VII valdytojas arba jo įgaliotas tvarkytojas; leistinos programinės įrangos		x	x	x	x

	sąrašas ne rečiau kaip kartą per metus peržiūrimas ir prireikus atnaujinamas					
81.8.	VII techninė ir programinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų		x	x	x	x
81.9.	VII techninės ir programinės įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai		x	x	x	x
81.10.	VII tarnybinių stočių patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas		x	x	x	x
81.11.	VII tarnybinių stočių patalpose turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir (arba) apsaugos tarnybos stebėjimo pulto		x	x	x	x
81.12.	visose patalpose, kuriose yra VII naudotojų ir VII techninė įranga, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų įrangos		x	x		
82.	Per metus turi būti užtikrintas VII prieinamumas:					
82.1.	mažos svarbos VII – ne mažiau kaip 70 proc. laiko darbo metu darbo dienomis					x
82.2.	vidutinės svarbos VII – ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis				x	
82.3.	svarbiems VII – ne mažiau kaip 96 proc. laiko visą parą			x		
82.4.	ypatingos svarbos VII – ne mažiau kaip 99 proc. laiko visą parą		x			
83.	VII valdytojo arba jo įgalioto tvarkytojo nustatyta tvarka turi būti daromos atsarginės elektroninės informacijos kopijos (toliau – kopijos), kurios turi būti saugomos kitose patalpose arba kitame pastate, nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota		x	x	x	x
84.	Elektroninė informacija kopijose turi būti užšifruota (šifravimo raktai turi būti saugomi atskirai nuo kopijų) arba turi būti imtasi kitų priemonių, neleidžiančių panaudoti kopijų elektroninei informacijai neteisėtai atkurti		x	x	x	x
85.	Atsarginės laikmenos su VII programinės įrangos kopijomis turi būti laikomos kitose patalpose arba kitame pastate, nei yra VII tarnybinės stotys		x	x	x	x
86.	VII turi perspėti VII administratorių, kai pagrindinėje VII kompiuterinėje įrangoje iki nustatytos pavojingos ribos sumažėja laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja		x	x	x	
87.	VII turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemones		x	x	x	
88.	VII valdytojo arba jo įgalioto tvarkytojo nustatyta tvarka turi būti kontroliuojamas patekimas į tarnybinių stočių patalpas ir patalpas, kuriose saugomos kopijos		x	x	x	
89.	Patekimas prie VII naudotojų darbo vietų turi būti kontroliuojamas		x	x		
90.	Turi būti numatytos atsarginės patalpos, į kurias galima būtų laikinai perkelti VII įrangą, nesant galimybių tęsti veiklą pagrindinėse patalpose; VII veiklos tęstinumo valdymo planas turi užtikrinti VII veiklos atnaujinimą atsarginėse patalpose per laikotarpį, ne ilgesnį, nei nustatyta 82 punkte		x	x	x	
91.	Atsarginės patalpos turi atitikti pagrindinėms patalpoms keliamus reikalavimus arba VII veiklos		x	x	x	

	tęstinumo valdymo plane turi būti nustatyta, kaip per minimalų laikotarpį pasiekti atitiktį šiems reikalavimams					
92.	Atsarginės laikmenos su programinės įrangos kopijomis turi būti laikomos nedegioje spintoje, kitose patalpose arba kitame pastate, nei yra VII tarnybinės stotys		x	x	x	
93.	Programinę įrangą turi diegti tik VII valdytojo ar tvarkytojo įgalioti asmenys		x	x	x	
94.	Programinė įranga turi būti testuojama naudojant atskirą testavimui skirtą aplinką		x	x	x	
95.	Gali būti naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (pavyzdžiui, USB, CD/DVD ir kt.); šios laikmenos negali būti naudojamos veiklai, nesusijusiai su teisėtu informacinės sistemos tvarkymu		x	x		
96.	Svarbiausia kompiuterinė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima		x	x		
97.	Svarbiausios kompiuterinės įrangos gedimai turi būti registruojami, taip pat turi būti paskirtas asmuo, atsakingas už gedimų registravimą		x	x		
98.	Pagrindinėse VII tarnybinėse stotyse turi būti naudojamos vykdomo kodo kontrolės priemonės, automatiškai apribojančios ar informuojančios apie neautorizuoto programinio kodo vykdymą		x	x		
99.	Turi būti įgyvendintos Lietuvos standarte LST ISO/IEC 27002:2017 nurodytos saugos priemonės, išskyrus priemones, kurios netaikytinos dėl VII valdytojo ir (ar) tvarkytojo veiklos, VII ar naudojamos VII techninės įrangos pobūdžio, ir Lietuvos standarte LST ISO/IEC 27001:2017 nurodyti informacijos saugumo valdymo sistemos reikalavimai		x			
100.	VII informacinių technologijų saugos atitikties vertinimas (toliau – atitikties vertinimas) turi būti atliekamas ne rečiau kaip kartą metus, jei kituose teisės aktuose nenustatyta kitaip		x	x	x	x
101.	Ne rečiau kaip kartą per trejus metus atitikties vertinimą turi atlikti nepriklausomi, visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų auditoriai		x			

_____