NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
prie Krašto apsaugos ministerijos
Gedimino pr. 40, Vilnius, tel. 1843, www.nksc.lt, el. p. info@nksc.lt

Tinklų ir informacinių sistemų kibernetinio saugumo politikos dokumento (-ų) galimas turinys

Kibernetinio saugumo reikalavimų aprašo skirsnio pavadinimas	Galimas (-i) tinklų ir informacinių sistemų (toliau – TIS) kibernetinio saugumo politikos dokumento (-ų) skyriaus (-ių) pavadinimas (-ai)[1]	Kibernetinio saugumo reikalavimų aprašo punktai[2]
01 TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO POLITIKA	Tinklų ir informacinių sistemų kibernetinio saugumo politikos dokumentas (1)[3]	Kibernetinio saugumo tikslai, teisės aktai, įsipareigojimai darbuotojams ir trečiosioms šalims, reguliari politikos dokumentų peržiūra ir atnaujinimas [4]
02 KIBERNETINIO SAUGUMO RIZIKOS ANALIZĖ	Rizikos vertinimo ir valdymo proceso tvarka (2) Rizikos vertinimo ataskaita (3) Rizikos valdymo priemonių planas (4)	Rizikos vertinimo ir valdymo proceso tvarka [7–9] Rizikos vertinimo ataskaita, rizikos valdymo priemonių planas [9–15]
03 UŽ KIBERNETINĮ SAUGUMĄ ATSAKINGŲ ASMENŲ IR KIBERNETINIO SAUGUMO SUBJEKTO VADOVO AR JO ĮGALIOTO ASMENS PAREIGOS	Atsakingų asmenų ir jų funkcijų sąrašas (5)	Už kibernetinį saugumą atsakingų asmenų paskyrimas [16–18] Atsakingų asmenų funkcijos ir atsakomybės [19–21]
04 KIBERNETINIŲ INCIDENTŲ VALDYMAS	Kibernetinių incidentų valdymo planas (6) Žurnalinių įrašų valdymo tvarka (7) Kibernetinių incidentų valdymo plano veiksmingumo išbandymo ataskaita (8)	Kibernetinių incidentų valdymo plano turinys (incidentų nustatymo būdai, valdymo organizavimas ir vertinimas, atsakomybės, veiksmai, komunikacija) [22–24] Žurnalinių įrašų reikalavimai (saugojimo ir administravimo, įsibrovimų aptikimo ir prevencijos sistemų reikalavimai) [25]
05 VEIKLOS TĘSTINUMAS	TIS veiklos tęstinumo valdymo planas (9) Atsarginių duomenų kopijų valdymo tvarka (10) Veiklos tęstinumo valdymo plano išbandymo ataskaita (11)	Veiklos tęstinumo valdymo plano turinys (taikymo sąlygos, atkūrimo kriterijai, atsakingi asmenys, valdymo ir atkūrimo grupės, atkūrimo planas, testavimas, ataskaitos, RTO/RPO) [27] Atsarginių duomenų kopijų kūrimo, saugojimo ir duomenų atkūrimo reikalavimai [28] Veiklos tęstinumo valdymo plano išbandymo ataskaita [27.8, 29]
06 TIEKIMO GRANDINĖS SAUGUMAS	Tiekimo grandinės saugumo valdymo ir tiekėjų atrankos kriterijų tvarka (12) Tiekėjų sąrašas (13) Sutartys su tiekėjais (įskaitant interneto paslaugų teikėjus) (14)	Saugumo valdymo tvarka nustato paslaugų, darbų ar įrangos pirkimą, TIS projektavimą, kūrimą, diegimą, naudojimą, priežiūrą, modernizavimą ir (ar) kibernetinio saugumo užtikrinimą [32, 33, 35] Tiekėjų atrankos kriterijai, sutarties reikalavimai [34, 36, 37]. Tiekėjų kontrolė ir priežiūra [38, 39]
07 TINKLŲ IR INFORMACINIŲ SISTEMŲ ĮSIGIJIMAS, PLĖTOJIMAS IR PRIEŽIŪROS SAUGUMAS, ĮSKAITANT SPRAGŲ VALDYMĄ IR ATSKLEIDIMĄ	TIS saugos valdymo užtikrinimo tvarka (15) Leistinos programinės įrangos sąrašas (16) TIS pokyčių ir pataisų valdymo tvarka (17) Spragų valdymo nuostatos (18)	TIS įsigijimo, plėtojimo ir priežiūros saugumo užtikrinimo tvarka [40, 41] Pokyčių ir pataisų valdymas [42–44] Spragų valdymas, skenavimas [45, 46]
08 KIBERNETINIO SAUGUMO REIKALAVIMŲ VEIKSMINGUMO VERTINIMAS	Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarka, taikomų priemonių veiksmingumo vertinimo rodikliai ir kriterijai (19) Atitikties vertinimo ataskaita (20) Neatitikčių šalinimo planas (21) Kibernetinio saugumo audito ataskaita (22)	Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarka, reguliarus atitikties vertinimas ir auditas [48, 51] Kibernetinio saugumo taikomų priemonių veiksmingumo vertinimo reikalavimai [49]
09 KIBERNETINĖS HIGIENOS PRAKTIKA IR KIBERNETINIO SAUGUMO MOKYMAI	Kibernetinės higienos, mokymų organizavimo ir valdymo tvarka (23) Mokymų ataskaita (24)	Kibernetinės higienos praktikos organizavimo, kibernetinio saugumo mokymų organizavimo vykdymo tvarka [52–53] Mokymų ataskaita (mokymų tema, dalyvių skaičius) [54]
10 KRIPTOGRAFIJOS IR ŠIFRAVIMO NAUDOJIMO POLITIKA IR PROCEDŪROS	Kriptografijos ir šifravimo naudojimo tvarka (25)	Naudojimo tvarka ir raktų valdymas [55, 56]
11 ŽMOGIŠKŲJŲ IŠTEKLIŲ SAUGUMAS, FIZINĖS PRIEIGOS POLITIKA IR TURTO VALDYMAS	Žmogiškųjų išteklių saugumo, fizinės prieigos reikalavimai ir turto valdymo tvarka (26) TIS turto sąrašas (27) Techninės įrangos gedimų registracijos dokumentas (28)	Žmogiškųjų išteklių saugumo reikalavimai [58, 62] Fizinės prieigos kontrolės reikalavimai [59] Turto valdymo tvarka [61] Įrangos priežiūra ir gedimų registravimas [63]
12 PRIEIGOS VALDYMAS IR KELIŲ VEIKSNIŲ TAPATUMO NUSTATYMO PRIEMONĖS	Prieigos valdymo tvarka (29) Asmenų, kuriems suteiktos administratoriaus teisės prisijungti prie TIS sąrašas (30)	Naudotojų, administratorių, paslaugų tiekėjų prieigos teisių valdymas, slaptažodžių saugumo reikalavimai, kelių veiksnių autentifikavimo naudojimas [65–68]

[1] TIS valdytojas / savininkas gali išdėstyti TIS kibernetinio saugumo politikos nuostatas viename arba keliuose TIS kibernetinio saugumo politikos dokumentuose

[2] Kibernetinio saugumo reikalavimų aprašas

[3] (1–30) nurodo TIS kibernetinio saugumo politikos dokumento skyrių, jei reikalavimai dėstomi viename dokumente, arba dokumentų kiekį, jei reikalavimai dėstomi keliuose dokumentuose