Dažniausiai užduodami klausimai* – atsakymai apie informacines sistemas

* Sąrašas parengtas atsižvelgiant į institucijų bei įstaigų klausimus, pateiktus konsultacijų metu

Eil. Nr.	Klausimas	Atsakymas
1.	Kam taikomi kibernetinio saugumo reikalavimai ir elektroninės informacijos saugos reikalavimai, išdėstyti LRV nutarimuose Nr. 818 ir Nr. 716?	Taikomi LR valstybės informacinių išteklių valdymo įstatymo 1 str. 3 d. nurodytoms institucijoms.
2.	Kokie teisės aktai reglamentuoja reikalavimus, kuriuos reikia įgyvendinti?	Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, Bendrųjų elektroninės informacijos saugos reikalavimų aprašas ir Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas.
3.	Norime įsteigti informacinę sistemą. Nuo ko pradėti?	Rengiamas informacinės sistemos nuostatų projektas pagal Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašą ir informacinės sistemos duomenų saugos nuostatų projektas pagal Saugos dokumentų turinio gairių aprašą. Patvirtinus informacinės sistemos nuostatus ir duomenų saugos nuostatus, rengiamas techninio aprašymo (specifikacijos) projektas pagal Valstybės informacinių sistemų gyvavimo ciklo valdymo metodiką. Vėliau rengiami saugos politiką įgyvendinantieji dokumentai pagal Saugos dokumentų turinio gairių aprašą.
4.	Ar techninio aprašymo (specifikacijos) projektas turi būti derinamas su NKSC?	Ne, techninio aprašymo (specifikacijos) projektas yra derinamas su Informacinės visuomenės plėtros komitetu.
5.	Kokie dokumentai turi būti derinami su NKSC?	Nuostatų, Duomenų saugos nuostatų, Saugaus elektroninės informacijos tvarkymo taisyklių, Naudotojų administravimo taisyklių, Veikos tęstinumo valdymo plano projektai arba kiti, kibernetinį saugumą organizacijoje apibrėžiantys ir įgyvendinantys dokumentai (jei tokie rengiami).
6.	Kokius informacinės sistemos dokumentus privaloma turėti?	Nuostatus, Duomenų saugos nuostatus, Techninį aprašymą (specifikaciją), Saugaus elektroninės informacijos tvarkymo taisykles, Naudotojų administravimo taisykles, Veikos tęstinumo valdymo planą.
7.	Ar galima Organizacinių ir techninių kibernetinio saugumo reikalavimų (LRV nutarimas Nr. 818) įgyvendinimą apsibrėžti	Taip. Tam, kad būtų išvengiama papildomos dokumentacijos rengimo, šių reikalavimų

	Duomenų saugos nuostatuose, Saugaus elektroninės informacijos tvarkymo taisyklėse, Naudotojų administravimo taisyklėse, Veikos tęstinumo valdymo plane?	įgyvendinimą rekomenduojama apsibrėžti šiuose dokumentuose.
8.	Kokie atsakingi asmenys organizacijoje turi būti paskirti?	Duomenų valdymo įgaliotinis (rekomenduojama paskirti įsakymu, kuriuo tvirtinami nuostatai), Saugos įgaliotinis (rekomenduojama paskirti įsakymu, kuriuo tvirtinami Duomenų saugos nuostatai), administratorius / -iai (rekomenduojama paskirti įsakymu, kuriuo tvirtinami Duomenų saugos nuostatai). Papildomai gali būti paskirti ir kiti atsakingi asmenys (kibernetinio saugumo vadovas, asmuo, atsakingas už incidentų valdymą, asmuo, atsakingas už rizikos vertinimą ar pan.)
9.	Ką reikia teikti į ARSIS sistemą?	Patvirtintų Duomenų saugos nuostatų, Saugaus elektroninės informacijos tvarkymo taisyklių, Naudotojų administravimo taisyklių, Veikos tęstinumo valdymo plano kopijas per 5 darbo dienas nuo šių dokumentų patvirtinimo. Rizikos įvertinimo ataskaitas, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas informacinių technologijų saugos atitikties vertinimo ataskaitas, pastebėtų trūkumų šalinimo plano kopijas ne vėliau kaip per 5 darbo dienas nuo šių dokumentų priėmimo.
10.	Ar privaloma informaciją teikti į ARSIS sistemą?	Taip, tai yra privaloma LR valstybės informacinių išteklių valdymo įstatymo 1 str. 3 d. nurodytoms institucijoms.
11.	Kokius dar dokumentus reikia teikti NKSC?	Veiklos tęstinumo valdymo planų veiksmingumo išbandymo ir pastebėtų trūkumų ataskaitų kopijos ne vėliau kaip per 5 darbo dienas nuo šių dokumentų priėmimo.
12.	Kuo vadovaujantis atlikti rizikos ir saugos atitikties vertinimą?	Rizikos ir IT saugos atitikties vertinimą galima atlikti ARSIS sistemoje arba naudojant kitą pasirinktą metodiką. IS saugos atitikties vertinimas atliekamas vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika. Rizikos vertinimui atlikti rekomenduojama vadovautis metodine medžiaga – Rizikos analizės vadovu.
13.	Į ką dar svarbu atkreipti dėmesį, rengiant saugos dokumentus?	Saugos reikalavimus reglamentuojantys teisės aktai periodiškai keičiami, todėl svarbu patikrinti ar yra vadovaujamasi aktualia teisės akto redakcija.
14.	Ar 4 kategorijos informacinių sistemų saugos dokumentai taip pat turi būti derinami su NKSC?	Taip, derinimo tvarka galioja tokia pati, kaip ir kitų kategorijų informacinių sistemų saugos dokumentams. Šių dokumentų kopijos taip pat turi būti pateikiamos į ARSIS sistemą.