Ką reikia žinoti apie atnaujintą Kibernetinio saugumo įstatymą: praktiniai patarimai

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

2025 m.

KSS taikomi teisės aktai

Kibernetinio saugumo įstatymas

Kibernetinio saugumo reikalavimų aprašas

Nacionalinis kibernetinių incidentų valdymo planas

Kibernetinio saugumo mokymų tvarkos aprašas

Valstybės informacinių išteklių įstatymas

KSS taikomi teisės aktų reikalavimai

Organizaciniai

1. Paskirti atsakingus asmenis
2. Įsteigti Saugumo operacijų centrą (SOC)
3. Parengti ir pavirtinti kibernetinės saugos politikos dokumentus ir pateikti jų duomenis į KSIS
4. Atlikti rizikos vertinimą, parengti ir patvirtinti rizikos vertinimo ataskaitą, rizikos valdymo planą
5. Išbandyti veiklos tęstinumo valdymo planą
6. Atlikti atitikties KSĮ, KSRA ir politikos dokumentams vertinimą, parengti vertinimo ataskaitą ir neatitikčių valdymo planą
7. Kas 3 metus atlikti nepriklausomą auditą
8. Dalyvauti kibernetinės higienos mokymuose ir parengti organizuotų mokymų ataskaitą

Techniniai

Įgyvendinti kibernetinio saugumo techninius reikalavimus (KSRA 26, 31, 47, 57, 60, 64, 69, punktai):

a) žurnalinių įrašų valdymas

b) fizinės ir loginės prieigos valdymas

c) kriptografijos naudojimas

d) atsarginių kopijų valdymo reikalavimus

e) TIS saugaus valdymo reikalavimus

KSS taikomi teisės aktų reikalavimai – atsakomybės

Kibernetinio saugumo subjekto vadovas

- Paskirti kibernetinio saugumo vadovą / saugos įgaliotinį
- Patvirtinti kibernetinio saugumo politiką ir ją įgyvendinamuosius dokumentus
- Ne rečiau kaip kartą per 2 metus Nacionalinio kibernetinio saugumo centro vadovo nustatyta tvarka išklausyti kibernetinio saugumo mokymus ir užtikrinti kibernetinio saugumo subjekto darbuotojų, jeigu tokių yra, nuolatinį švietimą kibernetinio saugumo srityje.

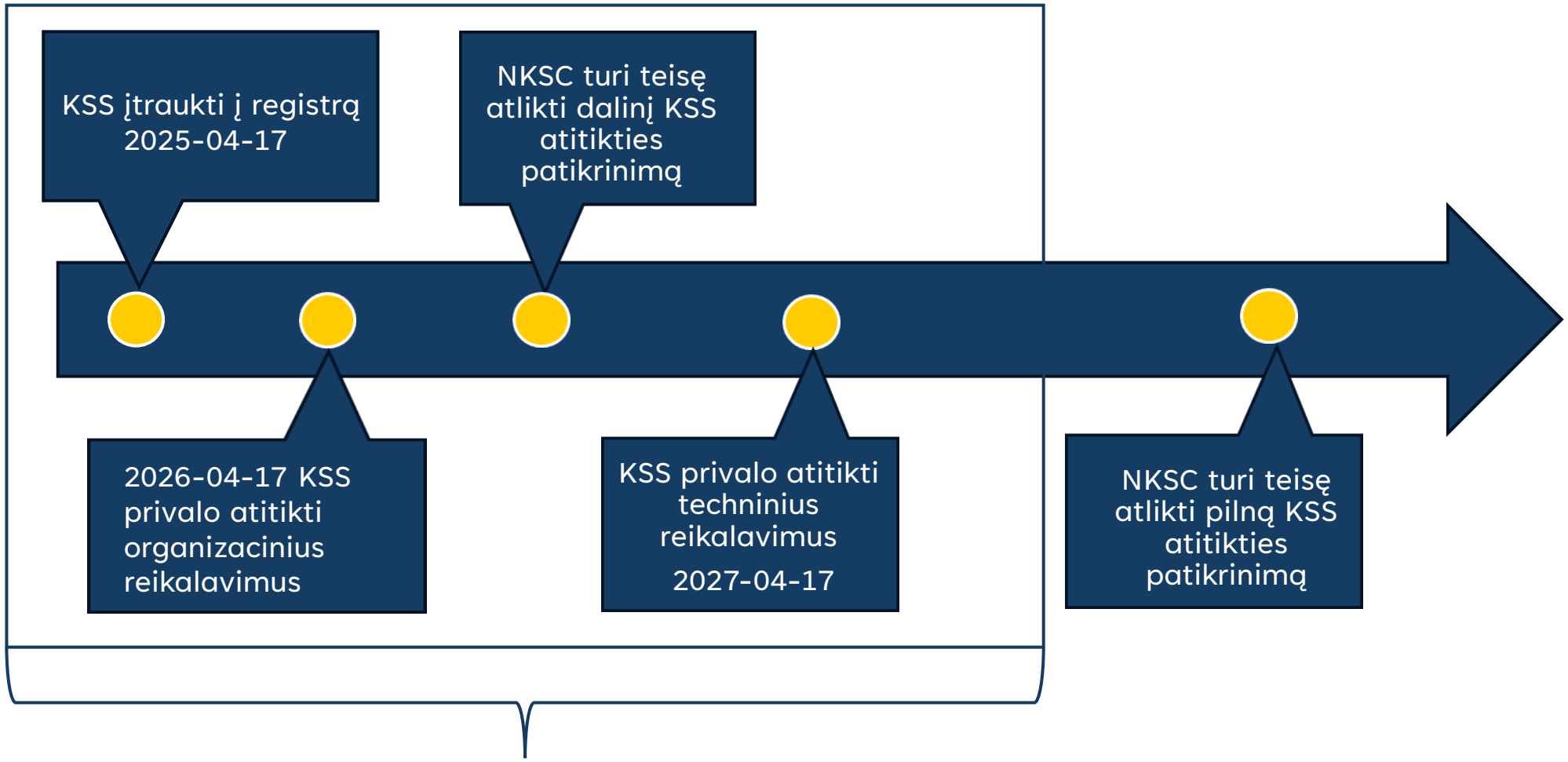
Kibernetinio saugumo vadovas/saugos įgaliotinis

- Atitikti VTĮ keliamus reikalavimus dėl nepriekaištingos reputacijos
- Turėti ne mažiau kaip 2 metų patirtį TIS, KS srityse ARBA turėti patvirtinamą kvalifikaciją ARBA praeiti mokymus ir būti išlaikius kibernetinio saugumo vadovo egzaminą
- KSRA 19, 21 p. nurodytos funkcijos ir jų ribojimai

Administratorius

- Atlieka tinklų ir informacinių sistemų techninę priežiūrą
- Diegia saugumo priemones, valdo prieigas
- KSRA 21 p.

Laiko juosta



NKSC parama KSS

Mokymų platforma: [Pagrindinis | Mokymai]

Kibernetinė higiena darbe
Sudėtingumo lygis: pagrindai

Kibernetinis saugumas organizacijų vadovams
Sudėtingumo lygis: strategas

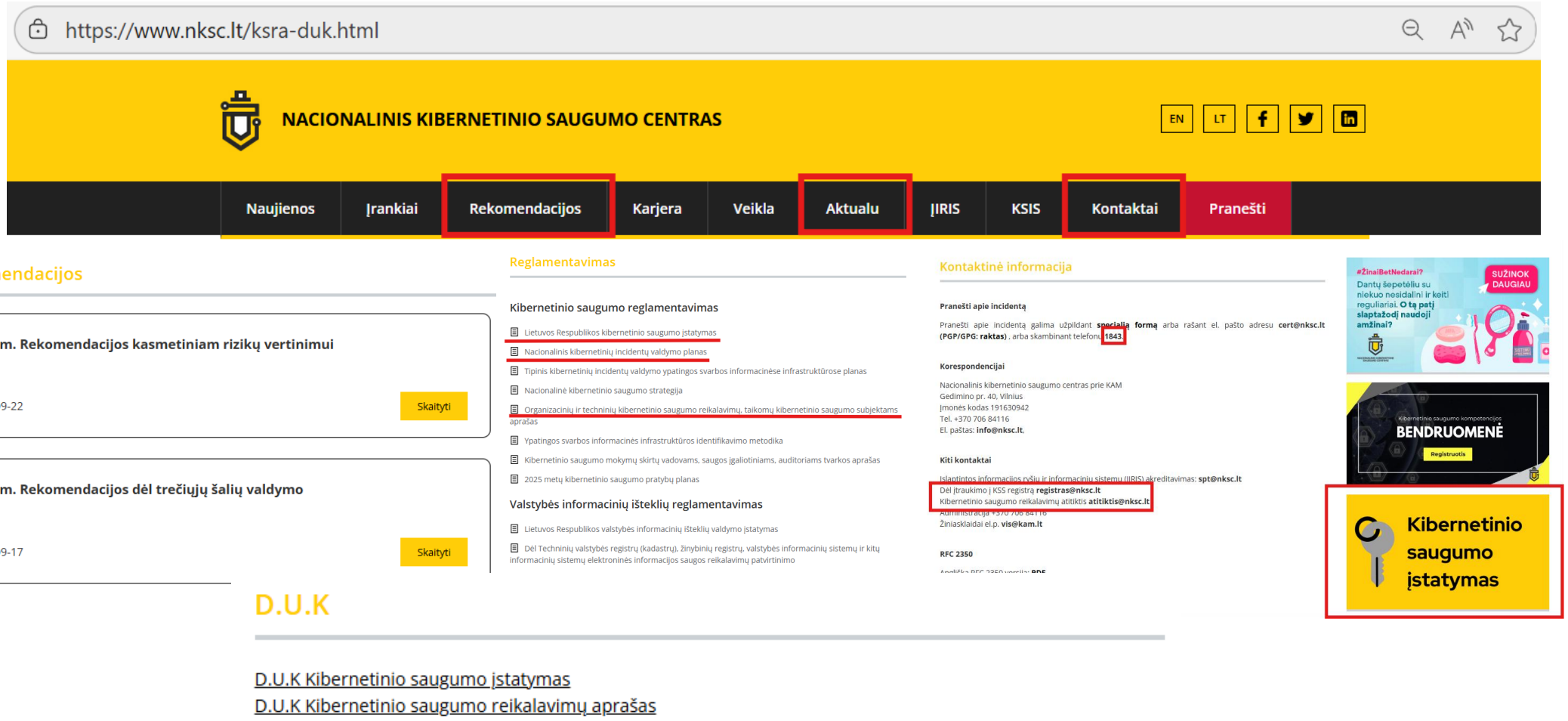
Informacijos saugumo vadovo kursas
Sudėtingumo lygis: ekspertas

Saugumo operacijų centro analitiko kursas
Sudėtingumo lygis: ekspertas

Įvadas į kibernetinių incidentų tyrimus
Sudėtingumo lygis: specialistams

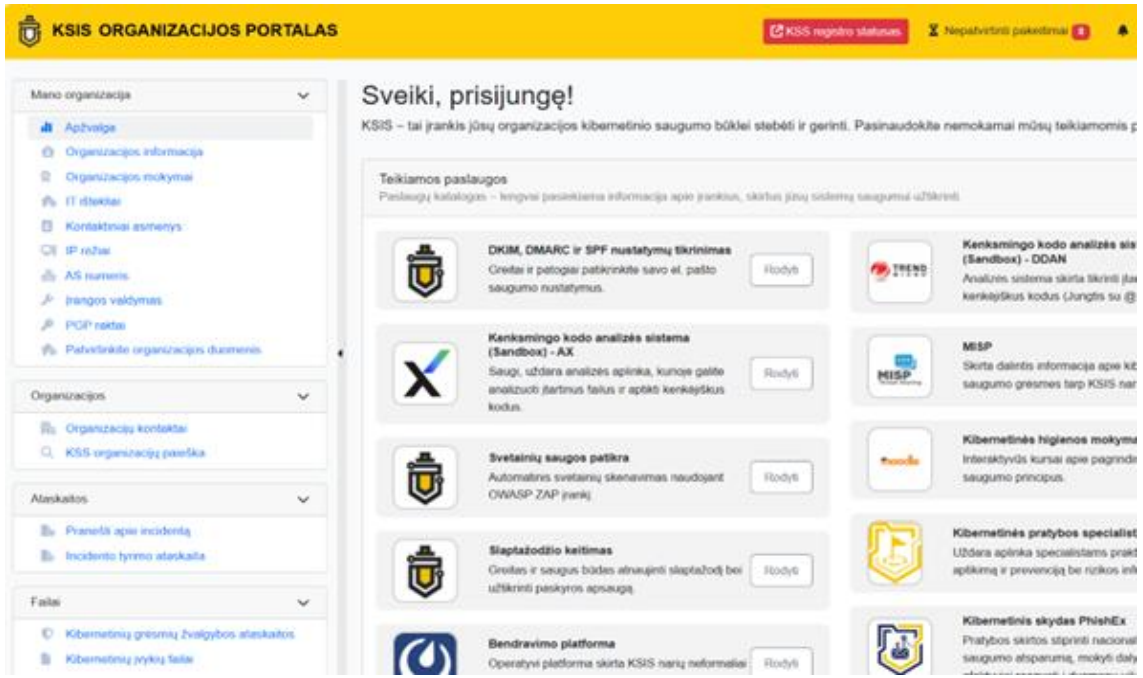
NKSC parama KSS

Aktuali informacija, rekomendaciniai leidiniai, konsultacijos: www.nksc.lt



NKSC parama KSS

Kibernetinio saugumo informacinė sistema (KSIS): V-998 Dėl Kibernetinio saugumo informacinio tinklo nuostatų patvirtinimo



Planuojama NKSC parama KSS

Rizikos valdymo metodika

Politikos dokumentų šablonai

Kibernetinio saugumo politikos dokumentų šablonai

Šis dokumentas yra rekomendacinio pobūdžio. Organizacija, įvertinusi veiklos ir informacijos valdymo procesus, turi dokumentą pakoreguoti taip, kad jis atitiktų organizacijoje taikomą praktiką.

PATVIRTINTA
[Organizacijos pavadinimas]
[Tvarkos tvirtintojas]
[Metai, data ir diena] įsakymu
Nr. [Įsakymo numeris]

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų kibernetinio saugumo politikos dokumentas (toliau – Kibernetinio saugumo politikos dokumentas) yra pagrindinis [organizacijos pavadinimas] (toliau – [Organizacijos pavadinimo trumpinys]) kibernetinio saugumo valdymo dokumentas, kuris apibrėžia kibernetinio saugumo tikslus, teisės aktus, atsakingų asmenų funkcijas ir atsakomybes, įsipareigojimus darbuotojams ir trečiosioms šalims.

2. Kibernetinio saugumo politikos dokumento tikslas – užtikrinti kibernetinį saugumą, kuris apima tris pagrindinius aspektus:

2.1. Konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo;

2.2. Vientisumą – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;

2.3. Prieinamumą – užtikrinimą, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti [Organizacijos pavadinimo trumpinys] veiklą.

3. [Organizacijos pavadinimo trumpinys] kibernetinis saugumas grindžiamas kibernetinio saugumo principais, kurie numatyti Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje.

4. Kibernetinio saugumo politikos dokumente vartojamos sąvokos:

4.1. **Atitikties vertinimas** – [Organizacijos pavadinimo trumpinys] atitikties reikalavimams, nustatytiems Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nutarimas Nr. 818), šiame Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose bei standartuose vertinimas;

4.2. **Kibernetinio saugumo vadovas** – [Organizacijos pavadinimo trumpinys] darbuotojas atsakingas už kibernetinio saugumo subjekto atitikties Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

4.3. **Rizikos vertinimas** – rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal [Organizacijos pavadinimo trumpinys] patvirtintą Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarką;

4.4. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.

5. Kitos šiame Kibernetinio saugumo politikos dokumente vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

II SKYRIUS
TEISĖS AKTAI

6. Kibernetinį saugumą reglamentuojančių teisės aktų ir standartų, kuriais vadovaujasi [Organizacijos pavadinimo trumpinys], sąrašas:

6.1. Kibernetinio saugumo įstatymas;

6.2. Lietuvos Respublikos komercinių paslapčių teisinės apsaugos įstatymas;

6.3. Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

6.4. Lietuvos Respublikos konkurencijos įstatymas;

6.5. Lietuvos Respublikos viešųjų pirkimų įstatymas;

6.6. Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

6.7. Nutarimas Nr. 818;

6.8. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

6.9. [*Pildymo instrukcija.* (Turite įvertinti, kokiais kitais kibernetinio saugumo teisės aktais vadovaujatės atsižvelgiant į organizacijos veiklos sektorių – energetikos, bankininkystės ir finansų rinkų, sveikatos priežiūros ir kt. ir veiklos sritis. Organizacijai gali būti taikomi, be pagrindinių kibernetinio saugumo teisės aktų, specifiniai kibernetinio saugumo teisės aktai atitinkamai pagal jos veiklos sektorių ir veiklos sritis., pvz.:

1) Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl atsparumo ypatingos svarbos subjektams (DORA reglamentas);

2) Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

3) Lietuvos banko valdybos 2020 m. lapkričio 26 d. nutarimas Nr. 03-174 „Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašo patvirtinimo“;

4) ir t.t.)];

6.10. Lietuvos standartas LST ISO/IEC ISO 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“;

6.11. Lietuvos standartas LST ISO/IEC 27002:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“;

6.12. [*Pildymo instrukcija.* Turite įvertinti, kokiais kibernetinio saugumo standartais vadovaujatės atsižvelgiant į organizacijos veiklos sektorių – energetikos, bankininkystės ir finansų rinkų, sveikatos priežiūros ir kt. ir veiklos sritis. Organizacija gali taikyti įvairius kibernetinio saugumo standartus atitinkamai pagal jos veiklos sektorių ir veiklos sritis., pvz.:

1) Mokėjimo kortelių duomenų apsaugos standartas (angl. *Payment Card Industry Data Security Standard, PCI DSS)*;

2) Standartas LST EN ISO/IEC 27799:2016 „Sveikatos informatika. Informacijos saugumo valdymas sveikatos priežiūros srityje, taikant ISO/IEC 27002“;

3) Standartas LST EN ISO/IEC 27017:2021 „Informacinės technologijos. Saugumo

saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.

5. Kitos šiame Kibernetinio saugumo politikos dokumente vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

II SKYRIUS
TEISĖS AKTAI

6. Kibernetinį saugumą reglamentuojančių teisės aktų ir standartų, kuriais vadovaujasi [Organizacijos pavadinimo trumpinys], sąrašas:

6.1. Kibernetinio saugumo įstatymas;

6.2. Lietuvos Respublikos komercinių paslapčių teisinės apsaugos įstatymas;

6.3. Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

6.4. Lietuvos Respublikos konkurencijos įstatymas;

6.5. Lietuvos Respublikos viešųjų pirkimų įstatymas;

6.6. Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

6.7. Nutarimas Nr. 818;

6.8. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

6.9. [*Pildymo instrukcija.* (Turite įvertinti, kokiais kitais kibernetinio saugumo teisės aktais vadovaujatės atsižvelgiant į organizacijos veiklos sektorių – energetikos, bankininkystės ir finansų rinkų, sveikatos priežiūros ir kt. ir veiklos sritis. Organizacijai gali būti taikomi, be pagrindinių kibernetinio saugumo teisės aktų, specifiniai kibernetinio saugumo teisės aktai atitinkamai pagal jos veiklos sektorių ir veiklos sritis., pvz.:

1) Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl atsparumo ypatingos svarbos subjektams (DORA reglamentas);

2) Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

3) Lietuvos banko valdybos 2020 m. lapkričio 26 d. nutarimas Nr. 03-174 „Dėl Informacinių ir ryšių technologijų ir saugumo rizikos valdymo reikalavimų aprašo patvirtinimo“;

4) ir t.t.)];

6.10. Lietuvos standartas LST ISO/IEC ISO 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“;

6.11. Lietuvos standartas LST ISO/IEC 27002:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“;

6.12. [*Pildymo instrukcija.* Turite įvertinti, kokiais kibernetinio saugumo standartais vadovaujatės atsižvelgiant į organizacijos veiklos sektorių – energetikos, bankininkystės ir finansų rinkų, sveikatos priežiūros ir kt. ir veiklos sritis. Organizacija gali taikyti įvairius kibernetinio saugumo standartus atitinkamai pagal jos veiklos sektorių ir veiklos sritis., pvz.:

1) Mokėjimo kortelių duomenų apsaugos standartas (angl. *Payment Card Industry Data Security Standard, PCI DSS)*;

2) Standartas LST EN ISO/IEC 27799:2016 „Sveikatos informatika. Informacijos saugumo valdymas sveikatos priežiūros srityje, taikant ISO/IEC 27002“;

3) Standartas LST EN ISO/IEC 27017:2021 „Informacinės technologijos. Saugumo

Kibernetinio saugumo politikos dokumentai

Nėra pareigos su NKSC derinti dokumentus

Dokumentų tvirtinimo duomenų teikimas į KSIS

Galimybė pasinaudoti dokumentų šablonais

Dokumentų teikimas per 5 d. d. į KSIS patikrinimo metu

Rizikos vertinimas

- **Atliekamas ne rečiau kaip kartą per metus**, įvykus esminiams KSS organizaciniams ar kt. reikšmingiems pokyčiams, taip pat įvykus dideliam kibernetiniam incidentui.
- Pateikti rizikos vertinimo dokumentų duomenis (**Rizikos vertinimo ataskaita** ir **Rizikos valdymo planas**) **į KSIS per 5 d. d.** nuo dokumentų patvirtinimo ir apibendrintus duomenis: identifikuotas grėsmes, jų tikimybę ir poveikį veiklai, rizikos lygius ir valdymo priemones.
- Patvirtintos Rizikos vertinimo ataskaitos ir Rizikos valdymo planai turi būti **saugomi ne mažiau kaip 3 metus.**

Rizikos valdymo priemonių įgyvendinimas

- **Rizikos valdymo planas apima:**
  - KS rizikos valdymo priemones
  - Išteklius reikalingus valdymo priemonių įgyvendinimui
  - Asmenis, atsakingus už priemonių įgyvendinimą laiku
  - Priemonių įgyvendinimo terminus
- Rizikos valdymo planas turi būti **periodiškai atnaujinamas** nurodant priemonių įgyvendinimo statusą
- Numatytų priemonių įgyvendinimo laikotarpis įprastai neturėtų viršyti 1 metų

Kibernetinio saugumo rizikų vertinimo metodika

- Dokumentų šablonai: turto (kategorijų), grėsmių ir spragų registravimui
- Pavyzdiniai grėsmių ir spragų sąrašai
- Valdymo priemonių sąrašai (pagal KSRA, ISO27001, CIS18 reikalavimus)
- Rizikų registro forma
- Pildymo pavyzdys
- Mokomoji medžiaga

Atitikties vertinimas, savideklaracija

KSS įsipareigojimai *(KSĮ, KSRA)*

- Visi KSS ne rečiau kaip kartą metuose turi atlikti atitikties vertinimą
- Rengti ir tvirtinti atitikties vertinimo ataskaitas
- Rengti ir tvirtinti neatitikčių šalinimo planus bei vykdyti jų įgyvendinimo kontrolę
- NKSC patikrinimo metu per 5 d. d. pateikti atitikties vertinimo ir neatitikčių šalinimo plano kopijas į KSIS
- Esminiai KSS kasmet užpildo savideklaracijos klausimynus KSIS

Kibernetinio saugumo auditas

KSS įsipareigojimai *(KSĮ, KSRA)*

- Ne rečiau kaip kartą per 3 metus, atlikti kibernetinio saugumo auditą, kurį turi atlikti **nepriklausomi sertifikuoti auditoriai**
- Esant NKSC patikrinimui **per 5 d. d. pateikti** kibernetinio saugumo audito ataskaitos kopiją į KSIS
- Auditas turi būti atliktas pagal **NKSC patvirtintą kibernetinio saugumo audito atlikimo metodiką** (numatoma viešinti 2025 IV ketvirtyje)

Kibernetinio saugumo audito metodikos turinys

REIKALAVIMAI AUDITORIAMS

Apibrėžti nepriklausomumo, nešališkumo, nepriekaištingos reputacijos reikalavimai

AUDITORIŲ IR KSS TEISĖS IR PAREIGOS

PASIRENGIMAS KIBERNETINIO SAUGUMO AUDITO ATLIKIMUI

Apibrėžti reikalavimai audito plano sudarymui, audito tikslų ir apimties nustatymui, reikalingų išteklių skyrimui

INFORMACIJOS, ĮRODYMŲ IR DUOMENŲ REIKALINGŲ AUDITO ATLIKIMUI RINKIMAS

Nustatyta audito atlikimo eiga, nurodyti informacijos surinkimo būdai

AUDITO VERTINIMO KRITERIJAI

Pateikti vertinimo kriterijai, kaip nustatyti KSS kibernetinio saugumo reikalavimų įgyvendinimo lygį

AUDITO IŠVADŲ RENGIMAS

Pateikti reikalavimai audito išvadų rengimui

KIBERNETINIO SAUGUMO AUDITO ATASKAITOS RENGIMAS

Pateikti reikalavimai audito ataskaitai

METODIKOS PRIEDE PATEIKIAMI MINIMALŪS REIKALAVIMAI, KURIE TURI BŪTI ĮVERTINTI AUDITO METU

Papildomai dėl atitikties vertinimo:

- Atitikties vertinimą gali atlikti KS vadovas, saugos įgaliotinis, kitas darbuotojas turintis kompetenciją, trečioji šalis
- Atitikties vertinimas apima KSĮ, KSRA ir KSS politikos dokumentuose apibrėžtų reikalavimų įgyvendinimą
- Kiekvienas KSS galės atlikti KSRA atitikties vertinimą KSIS sistemoje
- Atlikdami atitikties vertinimą, KSS galės vadovautis Kibernetinio saugumo audito atlikimo metodika

Klausimai-atsakymai

- **Ar rekomendacijos gali būti taikomos kaip privalomi kriterijai pirkimo sąlygose?**

Rekomendacijos nurodytos NKSC puslapyje yra neprivalomos ir neturi teisinės galios, bet turėtų būti numatyti tiekėjų atrankos kriterijai (KSRA 33 p.):

33.1. tiekėjo atitiktį Apraše nustatytiems kibernetinio saugumo reikalavimams;

33.2. kokybės reikalavimus tinklų ir informacinių sistemų produktams, paslaugoms;

33.3. prieigų valdymą, įskaitant prieigų laikotarpio ribojimą.

- **Kokiu mastu infrastruktūros statusas (ypatingos svarbos ar esminė) lemia techninių ir organizacinių priemonių apimtį?**

Kibernetinio saugumo subjektai yra skirstomi į esminius ir svarbius ir pagal šį skirstymą yra nustatoma techninių reikalavimų apimtis Kibernetinio saugumo reikalavimų apraše. Organizacinių reikalavimų apimtis nesiskiria.

- **Kaip teisingai pasirinkti kibernetinio saugumo paslaugų specializuotą įmonę? Į ką reikia atkreipti dėmesį, sudarant sutartį?**

Vadovaujantis Kibernetinio saugumo reikalavimų aprašo 33 p., kibernetinio saugumo subjektas turi apibrėžti tiekėjų atrankos kriterijus ir pagal juos atrinkti tiekėjus, taip pat svarbu paminėti, kad priklausomai nuo pirkimo imties – tiekėjas turi atitikti Kibernetinio saugumo reikalavimų aprašą. Į sutartį pagal pirkimo imtį, reikėtų įsitraukti Kibernetinio saugumo reikalavimų aprašo 34 p.

Ačiū už dėmesį.

Gal turite klausimų?

Parengta NKSC, 2025 m.

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS