PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2018 m. rugpjūčio 13 d. nutarimu Nr. 818
(Lietuvos Respublikos Vyriausybės
nutarimo Nr. redakcija)

NACIONALINIS KIBERNETINIŲ INCIDENTŲ VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinis kibernetinių incidentų valdymo planas (toliau – Planas) nustato kibernetinių incidentų valdymą, poveikio vertinimą ir informavimą apie juos.

2. Plane vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatyme, Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Europos Parlamento ir Tarybos 2019 m. balandžio 17 d. reglamente (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013.

II SKYRIUS
KIBERNETINIŲ INCIDENTŲ VALDYMAS

3. Kibernetinių incidentų valdymo organizavimą kibernetinio saugumo subjekto lygmeniu užtikrina kibernetinio saugumo subjektas. Kibernetinių incidentų valdymo organizavimas užtikrinamas vykdant šiuo Vyriausybės nutarimu tvirtinamo Kibernetinio saugumo reikalavimų aprašo 24 ir 25 punktuose numatytas funkcijas ir kibernetinio saugumo subjekto vadovui ar jo įgaliotam asmeniui paskiriant šias funkcijas vykdančius asmenis (toliau – Saugumo operacijų centras). Kibernetinio saugumo subjektas užtikrina, kad Saugumo operacijų centro funkcijos nebūtų pavedamos kibernetinio saugumo subjekto arba paslaugų teikėjo darbuotojui, atsakingam už tinkamą to kibernetinio saugumo subjekto tinklų ir (ar) informacinių sistemų veiklą.

4. Kibernetinio saugumo subjektas kibernetinių incidentų valdymą organizuoja pagal kibernetinio saugumo subjekto patvirtintą kibernetinių incidentų valdymo planą. Šis planas privalo apimti Tipinio kibernetinių incidentų valdymo proceso schemoje (Plano 1 priedas) ir Tipiniame kibernetinių incidentų valdymo proceso aprašyme (Plano 2 priedas) numatytus dalyvius, etapus, veiksmus, terminus ir rezultatus.

5. Kibernetinis incidentas laikomas suvaldytu, kai yra atkurtos kibernetinio saugumo subjektų tinklų ir informacinėmis sistemomis teikiamos paslaugos.

6. Nacionaliniu lygmeniu kibernetinių incidentų valdymą pagal Nacionalinio kibernetinių incidentų valdymo proceso schemą (Plano 3 priedas) ir aprašymą (Plano 4 priedas) užtikrina Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC).

7. NKSC, pagal kibernetinio saugumo subjekto prašymą spręsdamas dėl resursų skyrimo dideliam kibernetiniam incidentui valdyti, sprendimą priima įvertinęs tikimybę, kad didelis kibernetinis incidentas taps ekstremaliuoju įvykiu. Prioritetas skiriamas kibernetiniams incidentams, kurių padariniai labiausiai atitinka arba daugiausiai viršija Vyriausybės nustatytus ekstremaliojo įvykio kriterijus.

8. Įvykus arba kilus grėsmei įvykti dideliam kibernetiniam incidentui, atitinkančiam ekstremaliojo įvykio kriterijus, NKSC apie tai informuoja Vyriausybės kanceliarijos Nacionalinį krizių valdymo centrą (toliau – NKVC).

III SKYRIUS
KIBERNETINIŲ INCIDENTŲ POVEIKIO VERTINIMAS IR INFORMAVIMAS APIE KIBERNETINIUS INCIDENTUS

9. Jei Europos Komisijos įgyvendinamieji teisės aktai neapibrėžia išsamiau, laikoma, kad įvyko didelis kibernetinis incidentas, kaip jis suprantamas pagal Kibernetinio saugumo įstatymo 18 straipsnio 2 dalį, kai:

9.1. kibernetinio saugumo subjektas patiria ar gali patirti didelių paslaugų teikimo sutrikimų ir kibernetinis incidentas atitinka bent vieną iš šių kriterijų:

9.1.1. paslaugos trikdomos visoje Lietuvos teritorijoje ir (ar) bent vienoje Europos Sąjungos arba NATO šalyje;

9.1.2. tinklų ir informacinės sistemos veikla trikdoma 2 ar daugiau valandų;

9.1.3. paveiktų paslaugų gavėjų ar kompiuterizuotų darbo vietų skaičius lygus arba didesnis nei 1 000, arba 25 procentai (atsižvelgiant į tai, kuris dydis yra mažesnis);

9.1.4. paveikti 1 000 arba 25 procentų (atsižvelgiant į tai, kuris dydis yra mažesnis) paslaugų gavėjų asmens duomenys ar kiti kibernetinio saugumo subjekto saugomi paslaugų gavėjų duomenys;

9.1.5. kibernetinio saugumo subjektas nebegali užtikrinti teisės aktuose jo veiklai nustatytų reikalavimų įgyvendinimo;

9.1.6. prarastos arba atskleistos komercinės paslaptys arba įslaptinta informacija;

9.1.7. per 6 mėnesius patiriamas daugiau nei vienas analogiškas kibernetinis incidentas, incidentų pagrindinė priežastis sutampa, o finansinių nuostolių dydis siekia 9.2 papunktyje numatytas vertes;

9.2. kibernetinio saugumo subjektas patiria ar gali patirti didelių finansinių nuostolių, lygių arba didesnių nei 500 000 Eur, arba 5 procentų kibernetinio saugumo subjekto praėjusių finansinių metų apyvartos (atsižvelgiant į tai, kuri suma yra mažesnė);

9.3. kibernetinis incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą, atitinkančią bent vieną iš šių kriterijų:

9.3.1. galimos turtinės žalos dydis yra lygus arba didesnis nei 400 bazinių socialinių išmokų;

9.3.2. galimos neturtinės žalos dydis lygus arba didesnis nei 10 000 Eur;

9.3.3. sutrikdyta bent vieno žmogaus sveikata arba bent vienas žmogus žuvo.

10. Kibernetinio saugumo subjekto Saugumo operacijų centras apie kibernetinius incidentus informuoja NKSC, juos registruodamas Kibernetinio saugumo informacinės sistemos posistemyje – Nacionalinėje kibernetinių incidentų valdymo platformoje (toliau – Platforma).

11. Kibernetinio saugumo subjekto Saugumo operacijų centras, dėl kibernetinio incidento neturintis galimybės apie kibernetinius incidentus informuoti automatizuotu būdu per Platformą, NKSC informuoja užpildydamas formą Platformoje, NKSC interneto svetainėje, NKSC nurodytu elektroninio pašto adresu arba telefonu.

12. Kibernetinio saugumo subjekto Saugumo operacijų centras apie didelį kibernetinį incidentą NKSC informuoja Kibernetinio saugumo įstatymo 18 straipsnio 4 dalyje nustatytais terminais pateikdamas toje pačioje dalyje nurodytą informaciją. Kibernetinio saugumo subjekto Saugumo operacijų centras turi teisę teikti ir kitą, Kibernetinio saugumo įstatymo 18 straipsnio 4 dalyje nenurodytą, tačiau dideliam kibernetiniam incidentui suvaldyti ar tirti reikšmingą informaciją.

13. Kibernetinio saugumo subjekto Saugumo operacijų centras apie kitus kibernetinius incidentus, neatitinkančius Kibernetinio saugumo įstatymo 18 straipsnio 2 dalies ir Plano 9 punkto nuostatų (toliau – nedidelis kibernetinis incidentas), NKSC informuoja pateikdamas:

13.1. nedelsdamas, bet ne vėliau kaip per 72 valandas nuo sužinojimo apie kibernetinį incidentą momento, pranešimą apie nedidelį kibernetinį incidentą, jame pateikdamas Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 2 punkte nurodytą informaciją;

13.2. per vieną mėnesį nuo pranešimo apie kibernetinį incidentą registravimo dienos galutinę ataskaitą apie nedidelį kibernetinį incidentą, joje pateikdamas Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 4 punkte nurodytą informaciją. Galutinė ataskaita apie nedidelį kibernetinį incidentą neteikiama, jei pranešime apie kibernetinį incidentą pateikta visa galutinės ataskaitos informacija.

14. Kibernetinio saugumo subjekto Saugumo operacijų centras, teikdamas NKSC Kibernetinio saugumo įstatymo 18 straipsnio 2 dalyje nurodytą informaciją apie kibernetinio incidento pradinį vertinimą, įvardija:

14.1. kokių paslaugų sutrikimų patyrė ar gali patirti kibernetinio saugumo subjektas – nurodomos paslaugos ir sutrikimų apimtys;

14.2. kokių finansinių nuostolių patyrė ar gali patirti kibernetinio saugumo subjektas – nurodomas nuostolių dydis;

14.3. ar kibernetinis incidentas paveikė arba gali paveikti kitus asmenis, sukeldamas turtinę arba neturtinę žalą, – jei taip, nurodomi asmenys ir žalos dydis;

14.4. neteisėtų ar piktavališkų veiksmų įrodymus (jei tokių yra);

14.5. ar incidentas suvaldytas;

14.6. kitą svarbią informaciją (pavyzdžiui, kibernetinio incidento vietą, tikslų nustatymo laiką).

15. Jei kibernetinis incidentas tęsiasi ilgiau nei vieną mėnesį, kibernetinio saugumo subjektai kas mėnesį atnaujina Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 2 punkte nurodytą informaciją.

16. NKSC prašymu kibernetinio saugumo subjektas NKSC nurodytais terminais privalo teikti tarpines atitinkamų atnaujintų padėties duomenų ataskaitas apie didelius kibernetinius incidentus. NKSC turi teisę paprašyti pateikti ir kitus dideliam kibernetiniam incidentui suvaldyti reikalingus ir reikšmingus duomenis.

17. Asmenys, neturintys pareigos NKSC pranešti apie kibernetinius incidentus, apie kibernetinius incidentus, kibernetines grėsmes, vos neįvykusius kibernetinius incidentus ir (ar) taikytas kibernetinių incidentų valdymo priemones NKSC savanoriškai praneša:

17.1. kibernetinio saugumo subjekto Saugumo operacijų centras – tokia pat tvarka, kaip ir apie kibernetinius incidentus;

17.2. asmenys, kurie nėra kibernetinio saugumo subjektai – NKSC interneto svetainėje skelbiamais būdais.

18. Teikiant Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 4 punkto b papunktyje nurodytą informaciją, parenkama viena iš išvardytų kibernetinių grėsmių ir pagrindinių incidentų priežasčių:

18.1. nepageidaujamų laiškų ir (ar) klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content, spam*) ir (ar) tinklų informacinės sistemos veiklos trikdymas;

18.2. kenkimo programinė įranga (angl. *malicious software / code*): programinė įranga ar jos dalis, kuri padeda neteisėtai prisijungti prie tinklų ir informacinės sistemos, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti skaitmeninius duomenis, panaikinti ar apriboti galimybę jais naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešus skaitmeninius duomenis tokios teisės neturintiems asmenims ir kuri identifikuota kaip:

18.2.1. pažangi kenkimo programinė įranga (angl. *advanced persistent threat, APT*);

18.2.2. tinklų ir informacinės sistemos duomenis šifruojantis ir naikinantis (angl. *wiper*) ar išpirkos reikalaujantis programinis kodas (angl. *ransomware*);

18.2.3. tinklų ir informacinės sistemos dalys, aktyviai kontroliuojamos įsibrovėlių;

18.2.4. kenkimo programinės įrangos platinimas;

18.3. informacijos rinkimas (angl. *information gathering*): žvalgyba ar kita įtartina veikla, manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. *social engineering*), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti naudotoją atskleisti informaciją (angl. *phishing*) arba atlikti norimus veiksmus. Naudojami socialinės inžinerijos metodai, siekiant išvilioti prisijungimo prie tinklų ir informacinės sistemos ir (ar) kitą svarbią informaciją;

18.4. mėginimas įsilaužti (angl. *intrusion attempts*). Mėginimas įsilaužti arba sutrikdyti tinklų ir informacinės sistemos veikimą išnaudojant žinomas spragas (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą įsilaužimo būdą (angl. *new attack signature*), kurie gali būti skirstomi į:

18.4.1. išnaudojama viena ar kelios nežinomos spragos (angl. *zero day*);

18.4.2. tinklų ir informacinės sistemos žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita);

18.4.3. išnaudojamos žinomos ir viešai publikuotos spragos;

18.5. įsilaužimas (angl. *intrusions*). Sėkmingas įsilaužimas ir (ar) neteisėtas tinklų ir informacinės sistemos, taikomosios programinės įrangos ar paslaugos naudojimas (angl. *privileged account compromise, unprivileged account compromise, application compromise*), kuris skirstomas taip:

18.5.1. veiksmai prieš tinklų ir informacinę sistemą ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, tinklų ir informacinės sistemos ar jos dalies pažeidimas, sutrikdantis tinklų ir informacinės sistemos teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti tinklų ir informacinės sistemos naudotojų pasitikėjimą jais;

18.5.2. gaunama neteisėta prieiga prie tinklų ir informacinės sistemos, taikomosios programinės įrangos ar paslaugos;

18.6. paslaugų trikdymas, prieinamumo pažeidimai (angl. *availability*): veiksmai, kuriais trikdoma tinklų ir informacinės sistemos veikla, teikiamos paslaugos (angl. *DoS, DDoS*), tinklų ir informacinės sistemos ar jos dalies pažeidimas, sutrikdantis tinklų ir informacinės sistemos ir (ar) jos teikiamas paslaugas, kuris skirstomas taip:

18.6.1. teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas;

18.6.2. teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui;

18.7. tiekimo grandinės atakos (angl. *supply chain attack*): išnaudojama trečiųjų šalių, teikiančių paslaugas tinklų ir informacinės sistemos valdytojui ir (ar) tvarkytojui, infrastruktūra, siekiant įgauti ar turėti įtaką paslaugos gavėjo tinklų ir informacinės sistemos infrastruktūrai;

18.8. informacijos turinio saugumo pažeidimai (angl. *information content security*): neteisėta prieiga prie informacijos, galinčios turėti įtakos tinklų ir informacinės sistemos veiklai ir (ar) teikiamoms paslaugoms, ar jos neteisėtas keitimas;

18.9. neteisėta veikla, sukčiavimas (angl. *fraud*): vagystė, apgavystė, neteisėtas išteklių (angl. *unauthorized use of resources*), nelegalios programinės įrangos ar autorių teisių (angl. *copyright*) naudojimas, tapatybės klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai;

18.10. kitos grėsmės ar priežastys.

19. Užregistravus incidentą, informacija apie galimą nusikalstamą veiką ar asmens duomenų apsaugos pažeidimą, naudojantis Platforma, pateikiama atitinkamai Lietuvos policijai ir

(ar) Valstybinei duomenų apsaugos inspekcijai. Gavę informaciją apie kibernetinį incidentą, NKSC ir kitos šiame punkte nurodytos institucijos priima sprendimus dėl tyrimų pagal kompetenciją pradėjimo. Duomenys apie kibernetinius incidentus, reikalingi institucijų tyrimams atlikti, išskyrus ikiteisminio tyrimo duomenis, teikiami ir tvarkomi Platformoje.

20. NKSC, Lietuvos policija ir Valstybinė duomenų apsaugos inspekcija, gavę informacijos apie kibernetinius incidentus arba juos nustatę, nedelsdami, bet ne vėliau kaip per 24 valandas nuo informacijos gavimo ar nustatymo momento kibernetinius incidentus registruoja Platformoje teikdami visą turimą informaciją ir apie tai informuoja kibernetinio saugumo subjektų Saugumo operacijų centrą. Apie institucijų užregistruotus kibernetinius incidentus kibernetinio saugumo subjektų Saugumo operacijų centrai informuojami per Platformą. Kibernetinio saugumo subjekto Saugumo operacijų centras Plane nustatytais terminais privalo pateikti Kibernetinio saugumo įstatymo 18 straipsnio 4 dalies 1 arba 2 punkte nurodytą informaciją.

21. NKSC, įvertinęs Platformoje esančią informaciją apie kibernetinius incidentus ir nustatęs, kad nedidelis kibernetinis incidentas turėtų būti priskirtas dideliam kibernetiniam incidentui, kibernetinį incidentą Platformoje priskiria dideliam kibernetiniam incidentui ir apie tai nedelsdamas, bet ne vėliau kaip per 24 valandas nuo šiame punkte nurodyto incidento nustatymo informuoja kibernetinio saugumo subjektą.

22. Kai didelis kibernetinis incidentas yra susijęs su dviem ar daugiau valstybių narių, NKSC apie didelį kibernetinį incidentą ne vėliau kaip per 24 valandas nuo sužinojimo apie jį momento informuoja kitas paveiktas valstybes nares ir Europos Sąjungos tinklų ir informacijos apsaugos agentūrą (toliau – ENISA).

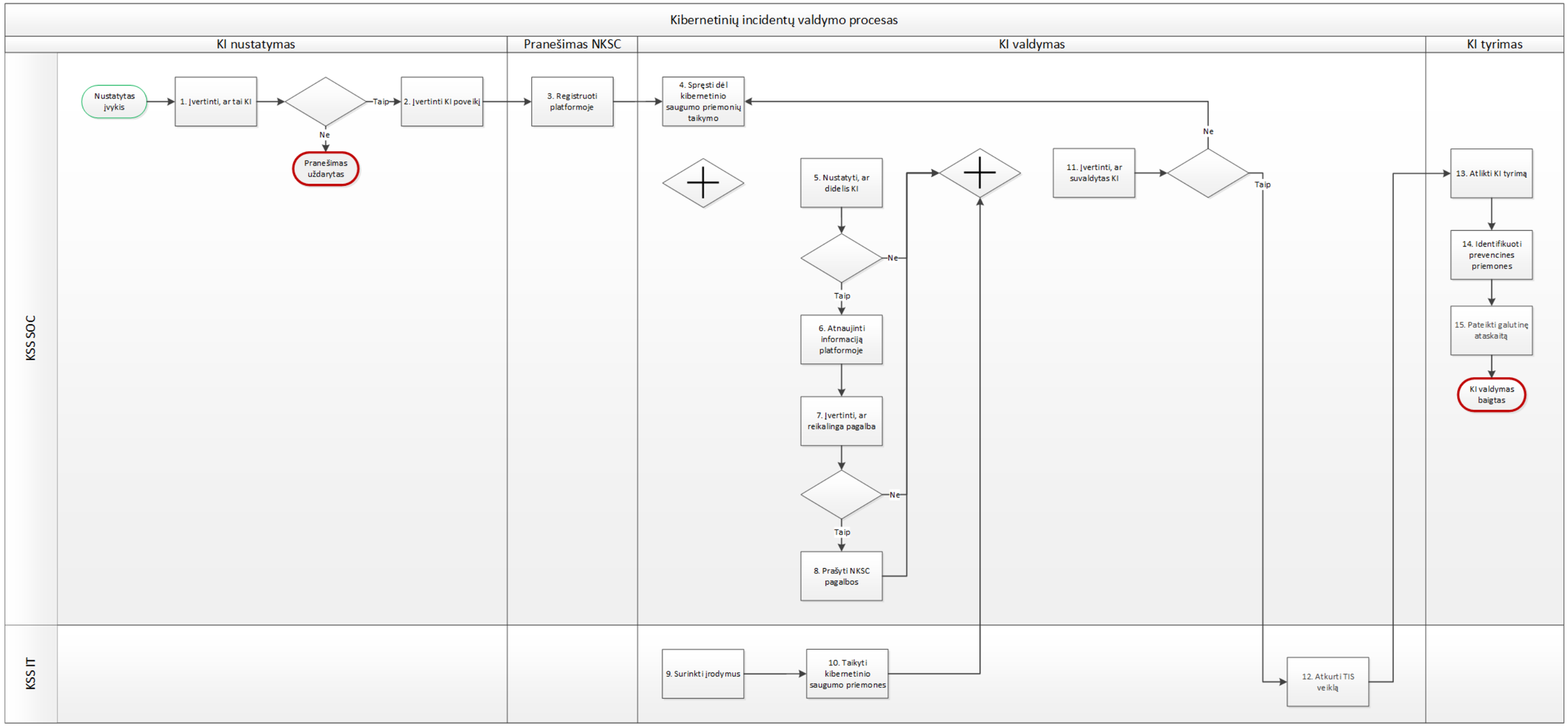
23. NKSC kas 3 mėnesius teikia ENISA suvestinę ataskaitą, į kurią įtraukiami nuasmeninti ir suvestiniai duomenys apie kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus.

24. Informaciją apie didelius kibernetinius incidentus, kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus, apie kuriuos pranešė kibernetinio saugumo subjektai, kurie Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka buvo pripažinti ypatingos svarbos subjektais, NKSC praneša NKVC ne vėliau kaip per 24 valandas nuo sužinojimo apie juos momento. Apie užregistruotus didelius kibernetinius incidentus kibernetinio saugumo subjektuose, kurie Krizių valdymo ir civilinės saugos įstatymo nustatyta tvarka buvo pripažinti ypatingos svarbos subjektais, NKSC praneša NKVC nedelsdamas, bet ne vėliau kaip per 1 valandą nuo kibernetinio incidento užregistravimo. Suvestinę informaciją apie kibernetinius incidentus, kibernetines grėsmes ir vos neįvykusius kibernetinius incidentus šiame punkte nurodytuose kibernetinio saugumo subjektuose NKSC pateikia NKVC kas 3 mėnesius.

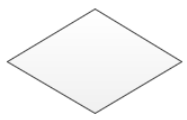
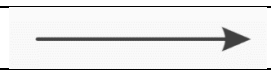
_____

Nacionalinio kibernetinių incidentų valdymo plano
1 priedas

TIPINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PROCESO SCHEMA



Schemos grafiniai simboliai, santrumpos ir jų reikšmės:

Grafinis simbolis / santrumpa	**Reikšmė**
	Proceso pradžia
	Proceso pabaiga
	Veiksmas, skirtas organizacijoje atliekamai veiklai atvaizduoti
	Duomenimis pagrįstas sprendimas, kai pasirenkama tolesnė proceso eiga
	Lygiagrečiai vykdomos proceso eigos
	Proceso eiga tarp veiksmų, sprendimų ir kt.
KI	Kibernetinis incidentas
KSS	Kibernetinio saugumo subjektas
KSS SOC	Kibernetinio saugumo subjekto Saugumo operacijų centras arba jo funkcijas vykdantys asmenys
KSS IT	Kibernetinio saugumo subjekto tinklų ir informacinių sistemų veiklą užtikrinantis padalinys arba jo funkcijas atliekantys asmenys
NKSC	Nacionalinis kibernetinio saugumo centras
TIS	Tinklų ir informacinė sistema

Nacionalinio kibernetinių incidentų valdymo plano
2 priedas

TIPINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PROCESO APRAŠYMAS

Eil. Nr.	Veiksmo aprašymas	Dalyvis	Terminas	Rezultatas
Pradžia (nustatytas įvykis)				
1.	Įvertinti, ar tai kibernetinis incidentas. Gavus pranešimą apie įvykį arba jį nustačius, sprendžiama, ar jis galėtų būti laikomas kibernetiniu incidentu.	Kibernetinio saugumo subjekto saugumo operacijų centras (toliau – Kibernetinio saugumo subjekto SOC)	Kibernetinio saugumo subjekto kibernetinių incidentų valdymo plane nustatytais terminais.	Priimtas sprendimas, ar įvyko kibernetinis incidentas.
2.	Įvertinti kibernetinio incidento poveikį. Priėmus sprendimą, kad įvykis laikomas kibernetiniu incidentu, pagal Kibernetinio saugumo įstatyme ir Nacionaliniame kibernetinių incidentų valdymo plane (toliau – Planas) nustatytus kriterijus įvertinama, ar įvyko didelis kibernetinis incidentas.	Kibernetinio saugumo subjekto SOC	Ne vėliau kaip per 24 val. nuo įvykio registravimo.	Įvertintas kibernetinio incidento poveikis.
Pranešimas Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – NKSC)				
3.	Registruoti Nacionalinėje kibernetinių incidentų valdymo platformoje (toliau – Platforma). Nustačius, kad įvyko kibernetinis incidentas, apie tai informuojamas Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), Platformoje pateikiant Kibernetinio saugumo įstatyme numatytą informaciją.	Kibernetinio saugumo subjekto SOC	Ankstyvasis perspėjimas (apie didelį incidentą) – nedelsiant, bet ne vėliau kaip per 24 val. nuo sužinojimo. Pranešimas apie (nedidelį) kibernetinį incidentą – nedelsiant, bet ne vėliau kaip per 72 val. nuo sužinojimo.	Kibernetinis incidentas užregistruotas Platformoje.

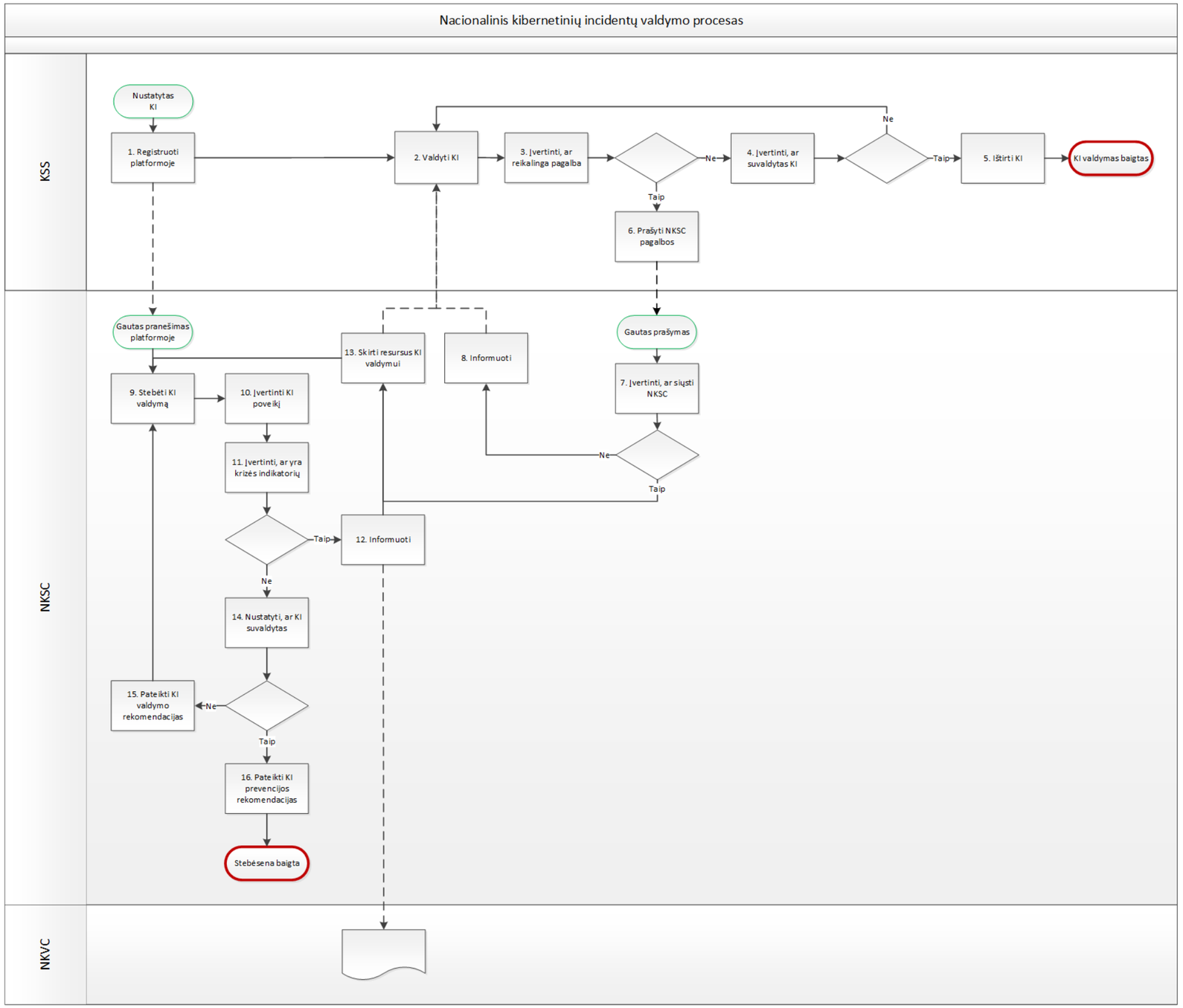
Kibernetinio incidento valdymas				
4.	Spręsti dėl kibernetinio saugumo priemonių taikymo. Užregistravus kibernetinį incidentą sprendžiama dėl tinkamiausių priemonių jam suvaldyti. Apie šias priemones informuojamas kibernetinio saugumo subjekto tinklų ir informacinių sistemų veiklą užtikrinantis padalinys arba jo funkcijas atliekantys asmenys (toliau – Kibernetinio saugumo subjekto IT)	Kibernetinio saugumo subjekto SOC	Kibernetinio saugumo subjekto kibernetinių incidentų valdymo plane nustatytais terminais.	Priimtas sprendimas dėl kibernetinio saugumo priemonių taikymo.
5.	Nustatyti, ar didelis kibernetinis incidentas. Vertinama, ar nedidelis kibernetinis incidentas netampa dideliu. Didelių kibernetinių incidentų pakartotinis vertinimas atliekamas tik patikslinant jo poveikį, nustatant pagrindinę priežastį, bet nekeičiant rūšies.	Kibernetinio saugumo subjekto SOC	Kibernetinio saugumo subjekto kibernetinių incidentų valdymo plane nustatytais terminais.	Įvertintas arba patikslintas kibernetinio incidento poveikis.
6.	Atnaujinti informaciją Platformoje. Nustačius, kad kibernetinis incidentas atitinka didelio kibernetinio incidento kriterijus, atnaujinama informacija pagal Kibernetinio saugumo įstatymo reikalavimus ir pateikiama tarpinė atitinkamų atnaujintų padėties duomenų ataskaita (toliau – tarpinė ataskaita) arba pažangos ataskaita.	Kibernetinio saugumo subjekto SOC	Tarpinė ataskaita – NKSC nurodytais terminais. Pažangos ataskaita apie didelį kibernetinį incidentą – kas mėnesį, iki bus suvaldytas kibernetinis incidentas.	Platformoje užregistruota tarpinė arba pažangos ataskaita.
7.	Įvertinti, ar reikalinga NKSC pagalba. Valdant didelį kibernetinį incidentą sprendžiama dėl turimų vidinių ir pasitelktų išorinių resursų	Kibernetinio saugumo subjekto SOC	Nuolat, iki bus suvaldytas kibernetinis incidentas.	Įvertintos kibernetinio saugumo subjekto galimybės suvaldyti

	pakankamumo kibernetiniam incidentui suvaldyti.			kibernetinį incidentą.
8.	Prašyti NKSC pagalbos. Nepavykstant didelio kibernetinio incidento suvaldyti turimais vidiniais ir pasitelktais išoriniais resursais, vertinamas poreikis kreiptis pagalbos į NKSC dėl kibernetinio incidento suvaldymo.	Kibernetinio saugumo subjekto SOC	Priėmus sprendimą kreiptis – nedelsiant.	Pateiktas pagalbos prašymas NKSC.
9.	Surinkti įrodymus. Valdant kibernetinius incidentus surenkami visi įrodymai, reikalingi pagrindinei kibernetinio incidento priežasčiai ar grėsmei nustatyti.	Kibernetinio saugumo subjekto IT	Nuolat, iki bus suvaldytas kibernetinis incidentas.	Surinkti įrodymai.
10.	Taikyti kibernetinio saugumo priemones. Taikomos būtinos priemonės, kad būtų užkirstas kelias kibernetiniam incidentui plisti ar tęstis.	Kibernetinio saugumo subjekto IT	Nuolat, iki bus suvaldytas kibernetinis incidentas.	Įgyvendinamas kibernetinio saugumo subjekto kibernetinio saugumo incidentų valdymo planas.
11.	Įvertinti, ar suvaldytas kibernetinis incidentas. Vertinamas taikomų techninių ir organizacinių priemonių veiksmingumas, ar kibernetinis incidentas tęsiasi, ar suvaldytas. Kibernetinio incidento nesuvaldžius, toliau tęsiamas jo poveikio vertinimas ir techninių ir organizacinių priemonių taikymas.	Kibernetinio saugumo subjekto SOC	Nuolat.	Priimtas sprendimas, ar kibernetinis incidentas suvaldytas.
12.	Atkurti tinklų ir informacinių sistemų veiklą.	Kibernetinio saugumo subjekto IT	Kibernetinio saugumo subjekto tinklų ir	Paslaugos kibernetinio saugumo

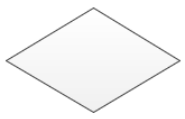
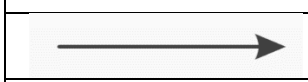
	Tinklų ir informacinių sistemų veikla atkuriama pagal jų veiklos atkūrimo planus.		informacinių sistemų veiklos atkūrimo planuose nustatytais terminais.	subjekto tinklų ir informacinėmis sistemomis teikiamos įprastine tvarka ir terminais.
Kibernetinio incidento tyrimas				
13.	Atlikti kibernetinio incidento tyrimą. Suvaldžius kibernetinį incidentą, pagal surinktus įrodymus identifikuojama pagrindinė jį sukėlusi priežastis.	Kibernetinio saugumo subjekto SOC	Kibernetinio saugumo subjekto veiklos atkūrimo planuose nustatytais terminais.	Nustatyta pagrindinė kibernetinio incidento priežastis.
14.	Identifikuoti prevencines priemones. Nustačius pagrindinę priežastį, pateikiamos išvados ir rekomendacijos, kaip ateityje išvengti tokio pobūdžio kibernetinių incidentų.	Kibernetinio saugumo subjekto SOC	Kibernetinio saugumo subjekto veiklos atkūrimo planuose nustatytais terminais.	Pateiktos išvados ir rekomendacijos.
15.	Pateikti galutinę ataskaitą. Vadovaujantis Kibernetinio saugumo įstatymo ir Plano reikalavimais parengiama galutinė ataskaita ir registruojama Platformoje.	Kibernetinio saugumo subjekto SOC	Galutinė ataskaita – per 1 mėnesį nuo ankstyvojo perspėjimo (didelio kibernetinio incidento atveju), pranešimo apie kibernetinį incidentą gavimo (nedidelio kibernetinio incidento atveju) arba nuo kibernetinio incidento suvaldymo.	Platformoje užregistruota galutinė ataskaita.

Nacionalinio kibernetinių incidentų valdymo plano
3 priedas

NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PROCESO SCHEMA



Schemos grafiniai simboliai, santrumpos ir jų reikšmės:

Grafinis simbolis / santrumpa	**Reikšmė**
	Proceso pradžia
	Proceso pabaiga
	Veiksmas, skirtas organizacijoje atliekamai veiklai atvaizduoti
	Duomenų objektas, teikiantis informaciją (dokumentai, duomenys ir kt.)
	Duomenimis pagrįstas sprendimas, kai pasirenkama tolesnė proceso eiga
	Proceso eiga tarp veiksmų, sprendimų ir kt.
KI	Kibernetinis incidentas
NKSC	Nacionalinis kibernetinio saugumo centras
KSS	Kibernetinio saugumo subjektas
NKVC	Nacionalinis krizių valdymo centras

Nacionalinio kibernetinių
incidentų valdymo plano
4 priedas

NACIONALINIO KIBERNETINIŲ INCIDENTŲ VALDYMO PROCESO APRAŠYMAS

Eil. Nr.	Veiksmo aprašymas	Dalyvis	Terminai	Rezultatas
1.	Registruoti Nacionalinėje kibernetinių incidentų platformoje (toliau – Platforma). Kibernetinio saugumo įstatyme nustatytais terminais kibernetinis incidentas užregistruojamas Platformoje.	Kibernetinio saugumo subjekto Saugumo operacijų centras (toliau – Kibernetinio saugumo subjekto SOC)	Ankstyvasis perspėjimas apie didelį kibernetinį incidentą – nedelsiant, bet ne vėliau kaip per 24 val. nuo sužinojimo apie didelį kibernetinį incidentą momento. Pranešimas apie kibernetinį incidentą – nedelsiant, bet ne vėliau kaip per 72 val. nuo sužinojimo apie kibernetinį incidentą momento. Tarpinė ataskaita – Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) nurodytais terminais.	Kibernetinis incidentas užregistruotas Platformoje

			Pažangos ataskaita – kas mėnesį, iki bus suvaldytas didelis kibernetinis incidentas. Galutinė ataskaita – per 1 mėnesį nuo ankstyvojo perspėjimo (didelio kibernetinio incidento atveju), pranešimo apie kibernetinį incidentą (nedidelio kibernetinio incidento atveju) arba nuo kibernetinio incidento suvaldymo.	
2.	Valdyti kibernetinį incidentą. Užregistruotas kibernetinis incidentas pradedamas valdyti. Techninės ir organizacinės priemonės taikomos, iki kibernetinis incidentas bus suvaldytas.	Kibernetinio saugumo subjekto SOC	Terminai nustatomi kibernetinio saugumo subjekto kibernetinių incidentų valdymo plane.	Taikomas kibernetinio saugumo subjekto kibernetinių incidentų valdymo planas.
3.	Įvertinti, ar reikalinga NKSC pagalba. Valdant kibernetinį incidentą sprendžiama dėl turimų vidinių ir pasitelktų išorinių resursų pakankamumo kibernetiniam incidentui suvaldyti.	Kibernetinio saugumo subjekto SOC	Nuolat, iki bus suvaldytas kibernetinis incidentas.	Įvertintos kibernetinio saugumo subjekto galimybės suvaldyti kibernetinį incidentą.

4.	Įvertinti, ar suvaldytas kibernetinis incidentas. Nustačius, kad kibernetinis incidentas suvaldytas, stebėsena baigiama. Nustačius, kad kibernetinis incidentas tęsiasi – stebėsena tęsiama.	Kibernetinio saugumo subjekto SOC	Nuolat.	Priimtas sprendimas dėl stebėsenos pabaigos arba pratęsimo.
5.	Ištirti kibernetinį incidentą. Kibernetinis incidentas ištiriamas ir nustatoma jo priežastis, pateikiamos išvados ir rekomendacijos, kaip ateityje išvengti tokio pobūdžio kibernetinių incidentų. Atitinkamai pagal tyrimo rezultatus koreguojami kibernetinių rizikų valdymo priemonės ir dokumentai.	Kibernetinio saugumo subjekto SOC	Kibernetinio saugumo subjekto veiklos atkūrimo planuose nustatytais terminais.	Nustatytos kibernetinį incidentą sukėlusios priežastys.
6.	Prašyti NKSC pagalbos. Valdant didelį kibernetinį incidentą, kai kibernetinio saugumo subjekto turimų vidinių ir pasitelktų išorinių resursų neužtenka, gali būti priimtas sprendimas kreiptis pagalbos į NKSC dėl kibernetinio incidento suvaldymo. NKSC priėmus sprendimą padėti kibernetinio saugumo subjektui valdyti kibernetinį incidentą, šis valdomas atsižvelgiant į NKSC rekomendacijas ir (arba) privalomus nurodymus.	Kibernetinio saugumo subjekto SOC	Nedelsiant.	Priimtas sprendimas dėl pagalbos prašymo teikimo.
7.	Įvertinti, ar siųsti NKSC. Įvertinus tikimybę kibernetiniam incidentui tapti ekstremaliuoju įvykiu, priimamas sprendimas pateikti rekomendacijas arba siųsti ekspertus (skirti resursus).	NKSC	Nedelsiant, bet ne vėliau kaip per 24 val.	Priimtas sprendimas teikti rekomendacijas arba siųsti ekspertus (skirti resursus).

8.	Informuoti Kibernetinio saugumo subjektas informuojamas apie sprendimą nesiųsti ekspertų. Šiuo atveju pateikiamos kibernetinio incidento valdymo rekomendacijos.	NKSC	Nedelsiant.	Informuotas kibernetinio saugumo subjektas, pateiktos rekomendacijos.
9.	Stebėti kibernetinio incidento valdymą. Atliekama Platformoje užregistruotų kibernetinių incidentų stebėsena, vertinamas jų valdymas.	NKSC	Nuolat.	Aptikti sisteminiai kibernetiniai incidentai.
10.	Įvertinti kibernetinio incidento poveikį. Vertinamas kibernetinio incidento poveikis ir sprendžiama, ar kibernetinis incidentas atitinka Kibernetinio saugumo įstatyme ir Nacionaliniame kibernetinių incidentų valdymo plane nustatytus didelio kibernetinio incidento kriterijus.	NKSC	Nuolat.	Nustatytas kibernetinio incidento poveikis.
11.	Įvertinti, ar yra krizės indikatorių. Vertinama, ar kibernetinis incidentas atitinka ypatingo ar ekstremaliojo įvykio kriterijus.	NKSC	Nuolat, iki bus suvaldytas kibernetinis incidentas.	Nustatyta, ar yra kibernetinės krizės indikatorių.
12.	Informuoti. Užregistravus kibernetinį incidentą, atitinkantį ekstremaliojo įvykio kriterijus, arba nustačius atitinkamą grėsmę, taip pat galimą arba susidariusią kibernetinę krizę, Vyriausybės nustatyta Pranešimo ir keitimosi informacija apie įvykį, ekstremalųjį įvykį, ypatingą įvykį, ekstremaliąją situaciją ar krizę tvarkos aprašo nustatyta tvarka	NKSC	Nedelsiant, bet ne vėliau kaip per 1 valandą.	Pateikta informacija NKVC.

	informuojamas Lietuvos Respublikos Vyriausybės kanceliarijos Nacionalinis krizių valdymo centras (toliau – NKVC).			
13.	Skirti resursus kibernetiniam incidentui valdyti. Nustačius, kad kibernetinis incidentas atitinka ypatingo ar ekstremaliojo įvykio kriterijus, šių įvykių grėsmę, taip pat galimą arba susidariusią kibernetinę krizę, sprendžiama dėl resursų, reikalingų kibernetiniam incidentui suvaldyti, skyrimo. Priėmus sprendimą skirti resursus kibernetiniam incidentui suvaldyti, siunčiami ekspertai, o kibernetinis incidentas toliau valdomas atsižvelgiant į NKSC ekspertų rekomendacijas ir įžvalgas, privalomus nurodymus.	NKSC	Nedelsiant.	Priimtas sprendimas dėl resursų skyrimo.
14.	Nustatyti, ar suvaldytas kibernetinis incidentas Vykdant kibernetinio incidento valdymo stebėseną vertinama kibernetinio saugumo subjekto pateikiama informacija ir vertinama, ar yra poreikis teikti rekomendacijas.	NKSC	Nedelsiant.	Įvertinta, ar kibernetinis incidentas suvaldytas.
15.	Pateikti kibernetinio incidento valdymo rekomendacijas. Priėmus sprendimą dėl rekomendacijų teikimo būtinumo, teikiami siūlymai pagal geriausias praktikas.	NKSC	Nedelsiant.	Pateiktos rekomendacijos.
16.	Pateikti kibernetinių incidentų prevencijos rekomendacijas.	NKSC	NKSC direktoriaus nustatytais terminais.	Parengtos ir paskelbtos kibernetinių incidentų

	Rengiamos ir viešai skelbiamos geriausios praktikos ir kibernetinių incidentų prevencijos ir valdymo rekomendacijos.			prevencijos ir valdymo rekomendacijos.

_____