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. Pažangos ataskaita – kas	Kibernetinis incidentas užregistruotas Platformoje

			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.	Kibernetinio saugumo subjekto SOC	Nuolat.	Priimtas sprendimas dėl stebėsenos

	Nustačius, kad kibernetinis incidentas suvaldytas, stebėsena baigiama. Nustačius, kad kibernetinis incidentas tęsiasi – stebėsena tęsiama.			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	NKSC	Nedelsiant.	Informuotas kibernetinio saugumo subjektas,

	pateikiamos kibernetinio incidento valdymo rekomendacijos.			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 informuojamas Lietuvos Respublikos Vyriausybės kanceliarijos Nacionalinis krizių valdymo centras (toliau – NKVC).	NKSC	Nedelsiant, bet ne vėliau kaip per 1 valandą.	Pateikta informacija NKVC.
13.	Skirti resursus kibernetiniam incidentui valdyti.	NKSC	Nedelsiant.	Priimtas sprendimas dėl

	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.			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. Rengiamos ir viešai skelbiamos geriausios praktikos ir kibernetinių incidentų prevencijos ir valdymo rekomendacijos.	NKSC	NKSC direktoriaus nustatytais terminais.	Parengtos ir paskelbtos kibernetinių incidentų prevencijos ir valdymo rekomendacijos.

_____