PATVIRTINTA
Valstybinės vaistų kontrolės tarnybos prie Lietuvos Respublikos sveikatos apsaugos ministerijos viršininko
2026 m. birželio 17 d.
įsakymu Nr. (1.4 E)1 A-837

INFORMACIJOS SAUGUMO POLITIKA

I.BENDROSIOS NUOSTATOS

1. Informacijos saugumo politika (toliau – Saugumo politika) yra pagrindinis Valstybinės vaistų kontrolės tarnybos prie Lietuvos Respublikos sveikatos apsaugos ministerijos (toliau – Tarnyba) informacijos saugumo valdymo sistemą (toliau – ISVS) reglamentuojantis dokumentas, skirtas nustatyti Tarnybos informacijos ir kibernetinio saugumo valdymo principus ir efektyvias saugumo užtikrinimo kryptis bei Tarnybos prisiimtus įsipareigojimus, siekiant tinkamai valdyti informacijos ir kibernetinio saugumo rizikas bei užtikrinti tarptautinių ir Lietuvos Respublikos teisės aktų reikalavimų bei Tarnybos prisiimtų įsipareigojimų informacijos ir kibernetinio saugumo srityje įgyvendinimą.

2. Saugumo politikos tikslas – apsaugoti Tarnybos informaciją nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos Tarnybos vykdomai veiklai ir reputacijai. Informacija – tai strategiškai svarbus Tarnybos veiklai turtas, todėl jos praradimas, neteisėtas pakeitimas, atskleidimas ar informacijos apdorojimo nutraukimas gali sukelti Tarnybos veiklos sutrikimų, padaryti žalos Tarnybai, kitiems fiziniams ir juridiniams asmenims. Atsižvelgiant į tai, Tarnyboje yra keliami ir nustatomi reikalavimai informacijos saugumui.

3. Informacijos saugumas apima tris pagrindinius aspektus:

3.1. Konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo;

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

3.3. Prieinamumą – užtikrinimą, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti Tarnybos veiklą.

4. Tarnybos informacijos ir kibernetinis saugumas grindžiamas kibernetinio saugumo principais, kurie numatyti Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje.

II. PAGRINDINĖS SĄVOKOS

5. Saugumo politikoje vartojamos sąvokos:

5.1. **Atitikties vertinimas** – Tarnybos veiklos atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo, Kibernetinio saugumo reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, šios Saugumo politikos ir jos įgyvendinimą reglamentuojančių kibernetinio saugumo teisės aktų bei standartų reikalavimams vertinimas;

5.2. **Kibernetinio saugumo vadovas** – Tarnybos darbuotojas (arba paslaugas teikianti trečioji šalis), atsakingas už Tarnybos veiklos atitikties Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

5.3. **Rizikos vertinimas** – rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal Tarnybos patvirtintą Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarką;

5.4. **Saugumo operacijų centras** – Tarnybos viršininko ar jo įgalioto asmens paskirti Tarnybos darbuotojai, jų grupė ir (ar) paslaugas teikianti trečioji šalis, atsakinga už žurnalinių įrašų, kibernetinių įvykių ir incidentų stebėseną, analizę, reagavimą ir informacijos teikimą pagal Tarnyboje nustatytas tvarkas;

5.5. **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.

6. Kitos šioje Saugumo politikoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

7. Tarnybos ISVS reikalavimai taikomi:

7.1. Visuose Tarnybos veiklos procesuose, susijusiuose su informacijos saugumu bei saugiu informacijos tvarkymu;

7.2. Visai Tarnybos informacijai, nepriklausomai nuo jos formos ir saugojimo būdo;

7.3. Visoms Tarnybos suinteresuotoms šalims, kurioms teisės aktų ir (ar) sutartinių santykių pagrindu yra suteikta prieiga prie Tarnybos informacinių išteklių teisės aktuose ar sutartyje numatytoms funkcijoms (teisėms) atlikti;

7.4. Išorinių paslaugų teikėjų teikiamoms paslaugoms.

III. TEISĖS AKTAI

8. Teisės aktai ir standartai, kuriais vadovaujamasi įgyvendinant ISVS:

8.1. Kibernetinio saugumo įstatymas;

8.2. Lietuvos Respublikos komercinių paslapčių teisinės apsaugos įstatymas;

8.3. Lietuvos Respublikos darbo kodeksas;

8.4. Lietuvos Respublikos konkurencijos įstatymas;

8.5. Lietuvos Respublikos viešųjų pirkimų įstatymas;

8.6. Lietuvos Respublikos civilinis kodeksas;

8.7. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

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

8.9. Lietuvos standartas LST ISO/IEC ISO 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ (toliau – Standartas ISO 27001);

8.10. Lietuvos standartas LST ISO/IEC 27002:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“;

8.11. kiti teisės aktai, reglamentuojantys kibernetinį saugumą.

IV. ĮSIPAREIGOJIMAI

9. Tarnybos viršininkas įsipareigoja užtikrinti ISVS įgyvendinimą, nuolatinę ISVS plėtrą bei gerinimą.

10. Tarnybos viršininko funkcijos:

10.1. nustatyti Saugumo politiką;

10.2. nustatyti ISVS tikslus bei patvirtinti ISVS planus;

10.3. sudaryti sąlygas Tarnybos darbuotojams tobulinti žinias informacijos saugumo srityje bei informuoti Tarnybos darbuotojus apie atsakomybę už informacijos saugumo pažeidimus;

10.4. užtikrinti efektyvų ISVS aprūpinimą reikiamais ištekliais: žmogiškaisiais ištekliais, infrastruktūra (patalpos, aparatinė ir programinė įranga, ryšiai ir kt.), darbo aplinka (tinkamos darbo sąlygos);

10.5. numatyti rizikos prisiėmimo ir priimtinų rizikos lygių kriterijus;

10.6. užtikrinti reguliarius ISVS vidaus auditus;

10.7. atlikti ISVS valdymo peržiūrą.

11. Tarnybos viršininkas nustato Tarnybos darbuotojams būtiną turėti kvalifikaciją, kuri nurodoma Tarnybos darbuotojų pareigybių aprašymuose.

12. Už ISVS veiklų koordinavimą atsakingas Tarnybos viršininkas, kuri užtikrina, kad apie susijusius su ISVS sprendimus būtų informuoti visi su šiais sprendimais susiję Tarnybos darbuotojai.

13. Tarnybos darbuotojai Tarnybos nustatyta tvarka privalo būti susipažinę su informacijos saugą reglamentuojančiais teisės aktais ir dalyvauti informacijos saugumo užtikrinimo procese.

14. Tarnybos viršininkas ar jo įgaliotas asmuo įsakymu paskiria:

14.1. Vadovybės atstovą ISVS;

14.2. Kibernetinio saugumo vadovą;

14.3. Informacijos saugumo valdymo grupę (ISVG);

14.4. TIS administratorius;

14.5. Fizinės saugos įgaliotinį;

14.6. Saugumo operacijų centrą;

14.7. Veiklos tęstinumo valdymo grupę;

14.8. Veiklos atkūrimo grupę.

V. INFORMACIJOS SAUGUMO ORGANIZAVIMAS

15. Tarnyboje siekiama šių pagrindinių ISVS tikslų:

15.1. apsaugoti informaciją nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos Tarnybos vykdomai veiklai ir įvaizdžiui;

15.2. užtikrinti ir valdyti informacijos saugumą, atsižvelgiant į Tarnybos veiklos strateginius tikslus;

15.3. užtikrinti ir valdyti atitikimą išoriniams ir vidiniams informacijos saugumo reikalavimams, atliekant periodinį ISVS vidaus auditą ir atitikties vertinimą bei ISVS valdymo peržiūrą (vadovybės vertinamoji analizė), šalinant nustatytus trūkumus ir įgyvendinant gerinimo veiksmus;

15.4. užtikrinti informacijos saugos incidentų sprendimą, jų priežasčių nustatymą ir pašalinimą, įgyvendinant informacijos saugos incidentų valdymo procesą;

15.5. užtikrinti efektyvų rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant įgyvendinti Rizikų valdymo priemonių planą ir suvaldyti rizikas iki priimtino lygio;

15.6. užtikrinti tinkamą informacijos saugumo ir apdorojimo priemonių parinkimą ir įgyvendinimą, atliekant kasmetinį rizikos vertinimą;

15.7. užtikrinti reikiamų informacijos saugumo valdymo priemonių įgyvendinimą ir jų veiksmingumą;

15.8. užtikrinti veiklos tęstinumo valdymo / atstatymo planų tinkamumą, atliekant jų periodinę peržiūrą ir testavimą;

15.9. įgyvendinti TIS2 ir kituose Europos Sąjungos, Lietuvos Respublikos teisės aktuose nustatytus informacijos saugumo reikalavimus, vadovautis Standarto ISO 27001 reikalavimais.

16. **Tarnybos ISVS sertifikavimo sritis** (*teisės aktų nustatyti veiksmai, susiję su vaistinių preparatų tiekimu rinkai, leidimų (licencijų) vykdyti farmacinę veiklą juridiniams ir fiziniams asmenims išdavimas ir farmacinės veiklos priežiūra*).

17. ISVS valdymas Tarnyboje yra pagrįstas rizikos valdymu. Informacijos saugumo rizikos vertinimas sudaro sąlygas, kad informacijos ir kibernetinio saugumo valdymo priemonės, taikomos Tarnybos veikloje, atitiktų pagrindinius Tarnybos veiklos bei informacijos ir kibernetinio saugumo tikslus.

18. Tarnybos informacijos saugumo rizikų vertinimas atliekamas ne rečiau kaip kartą per metus arba įvykus reikšmingiems Tarnybos pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui.

19. Tarnybos ISVS vidaus auditas atliekamas kartu su atitikties vertinimu ne rečiau kaip kartą per metus arba įvykus reikšmingiems Tarnybos pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui. Tarnyboje ne rečiau kaip kartą per 3 metus privalo atlikti atitikties vertinimą nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti auditoriai Kibernetinio saugumo įstatymo nustatyta tvarka.

20. Tarnyboje vykdomas ISVS procesų ir kontrolės priemonių stebėjimas, matavimai, analizė ir įvertinimas.

21. Tarnyboje ne rečiau kaip kartą per metus yra organizuojami arba rengiami veiklos tęstinumo valdymo plano išbandymas bei informacijos ir kibernetinio saugumo mokymai.

22. Tarnyboje atliekama ISVS valdymo peržiūra (vadovybės vertinamoji analizė).

VI. BAIGIAMOSIOS NUOSTATOS

23. Tarnybos kibernetinio saugumo vadovas reguliariai, ne rečiau kaip kartą per metus arba pasikeitus aplinkybėms, turi peržiūrėti ir, esant poreikiui, atnaujinti Saugumo politiką.

24. Saugumo politika skelbiama Tarnybos interneto svetainėje.

25. Saugumo politikos privalo laikytis visi Tarnybos valstybės tarnautojai, pagal darbo sutartis dirbantys darbuotojai ir trečiosios šalys.

26. Bet koks ISVS reikalavimų pažeidimas gali daryti neigiamą įtaką Tarnybos veiklos tęstinumui, pakenkti Tarnybos įvaizdžiui visuomenėje ir sukelti teisines pasekmes, todėl už nurodytų reikalavimų nesilaikymą ar jų pažeidimą gali būti taikoma teisės aktų numatyta atsakomybė.

27. Tarnybos suinteresuotosioms šalims pažeidus ISVS reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose, Tarnybos vidaus teisės aktuose bei sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose numatytos poveikio priemonės.

_____