VALSTYBĖS ĮMONĖS
IGNALINOS ATOMINĖS ELEKTRINĖS
FIZINĖS SAUGOS SKYRIUS

TVIRTINU
Generalinis direktorius

Linas Baužys

INFORMACIJOS SAUGUMO PAREIGŪNO KONSULTACINIŲ PASLAUGŲ PIRKIMO TECHNINĖ SPECIFIKACIJA

<Dok. data> Nr. <Reg. Nr.>
Visaginas

I SKYRIUS
PIRKIMO TIPAS

1. Paslaugų pirkimas.

II SKYRIUS
TIKSLAS

2. VĮ Ignalinos atominė elektrinė (toliau – IAE, Užsakovas, Organizacija) siekdama Organizacijoje sustiprinti informacijos saugos politiką, perka informacijos saugumo pareigūno funkcijų (angl. – CISO) paslaugas.

3. Informacijos saugumo pareigūno konsultacijų ir valdymo funkcinės srities apimtyje nebus informacijos, kuria Organizacija disponuoja pagal Valstybės ir tarnybos paslapčių įstatymo reikalavimus.

III SKYRIUS
PASLAUGŲ APRAŠYMAS IR TEIKIMO APIMTIS

4. Informacijos saugos pareigūno konsultacinių paslaugų sritys apima:

4.1. Informacijos saugos ir kibernetinio saugumo politiką;

4.2. Informacijos saugumo incidentų valdymą;

4.3. Organizacijos informacijos saugumo ir kibernetinio saugumo reikalavimų veiksmingumo vertinimą;

4.4. Informacinių sistemų, jose tvarkomos elektroninės informacijos, informacinių išteklių svarbos vertinimą;

4.5. Informacijos saugos ir kibernetinio saugumo rizikos vertinimą;

4.6. Organizacijos darbuotojų mokymus ir konsultavimą;

4.7. Saugumo operacijų centro (SOC) brandos vertinimą;

4.8. Konsultavimą įsigyjant, kuriant, prižiūrint informacinių technologijų (toliau – IT) informacines sistemas, IT technines ir programines priemones, ryšius, duomenų centro ar kitas IT paslaugas, vertinant naujausias technologijas, tiekimo grandinės saugumą ir kitais su informacijos saugumu susijusiais klausimais;

4.9. Dalyvavimą Organizacijos bendradarbiavimo su Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos procese ir komunikacijoje (pagal įgaliojimus ir poreikį).

5. **Informacijos saugos ir kibernetinio saugumo politika apima:**

5.1. Informacijos saugos ir kibernetinio saugumo politiką įgyvendinančių dokumentų ruošimą, peržiūrą pagal Organizacijoje galiojančią tvarką (ne rečiau kaip kartą per metus arba pagal poreikį);

5.2. Rolių ir atsakomybės sričių valdymą: rolių ir atsakomybės sričių tvarkos peržiūra bei rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.3. Rizikos valdymą: rizikos valdymo tvarkos peržiūra, gerinimo rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.4. Informacijos saugos ir kibernetinio saugumo incidentų valdymą: informacijos saugos ir kibernetinio saugumo incidentų valdymo plano peržiūra ir gerinimas (ne rečiau nei kartą per metus arba pagal poreikį), dalyvavimas jo išbandyme, plano išbandymo ataskaitos parengimas;

5.5. Veiklos tęstinumo valdymą: IS veiklos tęstinumo valdymo plano peržiūra ir gerinimas (ne rečiau nei kartą per metus arba pagal poreikį), dalyvavimas jo išbandyme, veiklos tęstinumo valdymo plano išbandymo ataskaitos parengimas;

5.6. Informacinių sistemų, duomenų bazių kopijų valdymą: atsarginių kopijų kūrimo politikos peržiūra, keitimas, tvarkos gerinimo rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.7. Tiekimo grandinės saugumo valdymą: tiekimo grandinės saugumo valdymo tvarkos peržiūra, gerinimo rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.8. Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo valdymą: tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo valdymo tvarkos peržiūra, gerinimo rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.9. Tinklų ir informacinių sistemų pokyčių valdymą: tinklų ir informacinių sistemų pokyčių valdymo tvarkos peržiūra, gerinimo rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.10. Pažeidžiamumų valdymą: pažeidžiamumų valdymo tvarkos peržiūra, gerinimo rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.11. Techninės ir programinės įrangos eksploatavimo ciklo valdymą: IS funkcionalumo, programinės ir techninės įrangos keitimo, atnaujinimo, naikinimo procesų tvarkos

peržiūra, koregavimas, tvarkos gerinimo rekomendacijų teikimas Organizacijai(ne rečiau kaip kartą per metus arba pagal poreikį);

5.12. Informacinės saugos ir kibernetinio saugumo supratimo valdymą: naudotojų supažindinimo su saugos politikos įgyvendinimo dokumentais ir teisės aktais organizavimas, vidinio komunikacinio informacijos saugos ir kibernetinio saugumo aktualijoms kanalo palaikymas, informacinių žinučių apie grėsmes, tendencijas, pokyčius Organizacijoje, numatomus informacijos saugumo procesų pokyčius, tvaraus kibernetinio saugumo principus kūrimas lietuvių kalba ne rečiau kaip 3 kartus per mėnesį;

5.13. Kriptografijos ir šifravimo valdymą: kriptografijos ir šifravimo naudojimo tvarkos peržiūra bei rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.14. Informacinių sistemų (toliau – IS) naudotojų ir administratorių teisių valdymą: IS naudotojų ir administratorių administravimo tvarkos peržiūra, tvarkos gerinimo rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.15. Fizinė IT infrastuktūros apsaugą: fizinės apsaugos tvarkos peržiūra, keitimas, tvarkos gerinimo rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.16. Mobiliųjų įrenginių valdymą: mobiliųjų įrenginių techninės ir programinės įrangos naudojimo politikos peržiūra, koregavimas, tvarkos gerinimo ir prevencinių priemonių rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.17. Jautrių duomenų valdymą: jautrių duomenų valdymo politikos peržiūra, koregavimas, tvarkos gerinimo ir prevencinių priemonių rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.18. Duomenų laikmenų valdymas: duomenų laikmenų politikos peržiūra, koregavimas, tvarkos gerinimo ir prevencinių priemonių rekomendacijų teikimas Organizacijai (ne rečiau kaip kartą per metus arba pagal poreikį);

5.19. Kitų informacijos saugumo pareigūno funkcijų vykdymą, kuris nustatytas Lietuvos Respublikos teisės aktuose.

6. Informacijos saugumo incidentų valdymas apima:

6.1. Dalyvavimą incidento valdymo, tyrimo, vertinimo procesuose (pagal įgaliojimus);

6.2. Informacijos saugumo incidento metu atsakingų asmenų konsultavimą.

7. Organizacijos informacijos saugumo ir kibernetinio saugumo reikalavimų veiksmingumo vertinimas apima:

7.1. Reikalavimą atlikti tinklų ir informacinių sistemų saugos atitikties Lietuvos Respublikos teisės aktams vertinimą ne rečiau kaip kartą per metus arba pagal poreikį;

7.2. Atlikus atitikties vertinimą parengti atitikties vertinimo ataskaitą;

7.3. Jeigu vertinimo metu identifikuotos neatitiktys, parengti identifikuotų neatitikčių šalinimo planą.

8. Informacinių sistemų, jose tvarkomos elektroninės informacijos, informacinių išteklių svarbos vertinimas apima:

8.1. Reikalavimą pagal Ekonomikos ir inovacijų ministerijos nustatytą metodiką atlikti informacinių išteklių svarbos vertinimą (pagal poreikį) ir, jei toks vertinimas bus atliekamas, teikti ataskaitas Organizacijai;

8.2. Reikalavimą vykdyti kitus Ekonomikos ir inovacijų ministerijos nurodymus, susijusius su skaitmeninės informacijos tvarkymu (pagal poreikį ir įgaliojimus).

9. **Informacijos saugos ir kibernetinio saugumo rizikos vertinimas apima:**

9.1. Reikalavimą ne rečiau nei kartą per metus peržiūrėti ir, esant poreikiui, atnaujinti esamą informacinių išteklių sąrašą;

9.2. Reikalavimą ne rečiau nei kartą per metus atlikti kibernetinių grėsmių ir incidentų poveikio informacijos saugai ir kibernetiniam saugumui rizikos analizę bei Organizacijai pateikti rizikos analizės ataskaitą. Rizikos vertinimas turi būti atliekamas remiantis LST ISO/IEC 27001, LST ISO/IEC 27002, LST ISO/IEC 27005 ir kitais Lietuvos ir tarptautiniais „Informacijos technologija. Saugumo metodai“ grupės standartais, NIST Cybersecurity Framework 2.0 bei kitais lygiaverčiais ir Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos rekomenduojamais standartais;

9.3. Reikalavimą, jei rizikos vertinimo metu yra nustatoma šalinamų trūkumų, parengti rizikos valdymo planą;

9.4. Reikalavimą atlikti naujos techninės ir programinės įrangos gamintojų ir tiekėjų rizikos vertinimą (pagal poreikį).

10. Saugumo operacijų centro brandos vertinimas apima:

10.1. Ne rečiau nei kartą per metus atlikti SOC brandos vertinimą pagal Security Operations Center Capability Maturity Model (SOC-CMM) metodiką;

10.2. Parengti vertinimo ataskaitą;

10.3. Parengti rekomendacijas, kaip patobulinti SOC veiklą, atsižvelgiant į SOC brandos vertinimo rezultatus;

10.4. SOC brandos vertinimas turi apimti visus 5 pagrindinių sričių (veikla, personalas, procesai, technologijos ir paslaugos) aspektus pagal SOC-CMM metodiką.

11. Organizacijos darbuotojų mokymas ir konsultavimas apima:

11.1. Ne mažiau kaip 2 mokymų kursų organizavimas ir pravedimas per metus informacijos saugumo ir kibernetinio saugumo klausimais kompiuterinių darbo vietų naudotojams (preliminarus skaičius Organizacijoje – 1100 naudotojų, kurie skirstomi į grupes). Kursų metu darbuotojai turi būti supažindinami su Organizacijai taikomais informacijos saugos ir kibernetinio saugumo reikalavimais numatytais įstatymuose bei teisės aktuose, Organizacijos patvirtinta informacijos saugos ir kibernetinio saugumo politika, elektroninės informacijos saugaus tvarkymo principų (konfidencialumas, vientisumas, prieinamumas) laikymosi tvarka, kibernetinio saugumo naujovėmis ir kt.;

11.2. Organizacijos darbuotojų konsultacijas dėl informacijos saugos politikos ir saugos taisyklių taikymo, pagal kompetenciją atsakyti į kitus su informacijos sauga susijusius klausimus;

11.3. Rekomendacijas Organizacijai kaip efektyviau kelti saugumo sąmoningumą, pagerinti darbuotojų informavimą apie saugumo politiką, kaip efektyviau organizuoti darbuotojų mokymus ir didinti darbuotojų kibernetinį raštingumą, kaip geriau užtikrinti naudotojo prisijungimo duomenų, jautrios informacijos saugumą.

12. Reikalavimai ataskaitoms:

12.1. Teikėjas privalo teikti sekančias ataskaitas:

- kasmėnesines ataskaitas apie suteiktas paslaugas už praeitą kalendorinį mėnesį, kurios turi būti pateikiamos iki einamojo mėnesio 15 dienos;
- ataskaita apie Informacijos saugos ir kibernetinio saugumo politikos gerinimo pasiūlymus ir rekomendacijas turi būti teikiama Organizacijai ne rečiau kaip kartą per 6 mėnesius;
- ataskaita apie Organizacijos kibernetinio saugumo brandą (angl. – Cybersecurity Maturity) teikiama Organizacijai ne rečiau kaip kartą per metus.

Pastaba. Visi šioje techninėje specifikacijoje nurodyti terminai skaičiuojami nuo sutarties įsigaliojimo dienos, jeigu konkrečiame reikalavime nenurodyta kitaip.

13. Kiti reikalavimai paslaugų teikimui:

13.1. Pradėdamas teikti paslaugas (ne vėliau kaip per 10 darbo dienų) nuo Sutarties įsigaliojimo datos, Paslaugų tiekėjas privalo pateikti ir suderinti su Užsakovu preliminarų metinį paslaugų teikimo planą. Preliminarus metinis paslaugų planas turi būti peržiūrimas ir tikslinimas ne rečiau kaip kas ketvirtį;

13.2. Atsižvelgiant į preliminarų metinį paslaugų teikimo planą ne vėliau kaip likus 5 d. d. iki sekančio mėnesio pradžios paslaugų teikėjas turi parengti ir suderinti su Užsakovu sekančio mėnesio paslaugų teikimo planą, nurodant planuojamas vykdyti konkrečias užduotis bei jų atlikimo apimtis darbo valandomis;

13.3. Informacijos saugumo bei kibernetinių incidentų atvejais Užsakovui informavus Paslaugų teikėją el. paštu arba telefonu Paslaugų teikėjas privalo nedelsiant (ne vėliau kaip per 3 valandas) suteikti paslaugas, numatytas šios techninės specifikacijos 6 p.

IV SKYRIUS
TAISYKLĖS IR STANDARTAI

14. Lietuvos Respublikos kibernetinio saugumo įstatymu.

15. Lietuvos Respublikos Vyriausybės 2024 m. lapkričio 6 d. nutarimu Nr. 945 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimo“.

16. Lietuvos standartu, LST ISO/IEC 27001. Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai.

17. Lietuvos standartu, LST ISO/IEC 27002. Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai.

18. Interneto saugumo centro (CIS) išleistomis kibernetinio saugumo priemonėmis.

19. Kitomis instrukcijomis ir aprašais pagal poreikį, reglamentuojančiais kibernetinio saugumo užtikrinimą Organizacijoje.

20. Tiekdamas paslaugą IAE, Tiekėjas privalo vadovautis IAE atliktų išorinių auditų rekomendacijomis, susijusiomis su informacine, kibernetine sauga, bei IT valdymu (išorinių auditų rekomendacijos bus pateiktos Paslaugų teikėjui).

V SKYRIUS
PASLAUGŲ VYKDYMO APIMTIS

21. Paslaugų teikimo apimtis. Paslaugos teikiamos nuotoliniu būdu, išskyrus šioje lentelėje numatytas valandas fiziniam atvykimui į Užsakovo patalpas:

Paslaugų teikimo forma	Paslaugų teikimo būdas	Paslaugų apimtis
Fizinis atvykimas	Elektrinės g. 4, K 47 Drūkšinių k. 31152 Visagino sav., skirta įmonės patalpa	Pagal poreikį, bet ne dažniau 2 kartus per metus (ne daugiau 10 val.).
Nuotolinė	Elektroniniu paštu, Microsoft Teams platforma, telefonu	Valandų skaičius per metus 480, 40 val. per mėnesį.

VI SKYRIUS
PASLAUGŲ SUTEIKIMO TERMINAS

22. Bendras Paslaugų suteikimo terminas – 24 mėnesiai nuo sutarties įsigaliojimo dienos.

VII SKYRIUS
PRIEIGA PRIE IAE KT RESURSŲ

23. Paslaugų teikimo laikotarpiui, esant poreikiui, Paslaugų teikėjui bus suteikta kompiuterinė darbo vieta ir nuotolinė prieiga prie IAE kompiuterių tinklo resursų.

VIII SKYRIUS
ĮRANGA

24. Paslaugų teikėjas užtikrina, kad turės pakankamai sutarties įgyvendinimui reikalingų priemonių ir įrangos.

25. Pagal šią paslaugų sutartį Užsakovo vardu negali būti perkama jokia techninė ar programinė įranga, reikalinga sutarties įgyvendinimui.

IX SKYRIUS
KITOS IŠLAIDOS

26. Visos kitos išlaidos, susijusios su sutarties įgyvendinimu, turi būti įskaičiuotos į bendrą sutarties kainą. Jokios papildomos išlaidos, neįskaičiuotos į sutarties kainą kompensuojamos nebus.

X SKYRIUS
DOKUMENTAI

27. Visi Paslaugų teikėjo rengiami dokumentai turi būti parengti lietuvių kalba.

28. Pateiktus derinimui dokumentus Užsakovas įvertina ne vėliau nei per 10 kalendorinių dienų nuo jų pateikimo. Įvertinimo terminai gali būti keičiami Paslaugų teikėjui ir Užsakovui susitarus.

29. Visos ataskaitos turi būti teikiamos skaitmeninėje išorinėje laikmenoje arba el. paštu PDF arba DOCX formatu.

XI SKYRIUS
KITI REIKALAVIMAI

30. Perkama nematerialaus pobūdžio (intelektinė) ar kitokia paslauga, nesusijusi su materialaus objekto sukūrimu, kurios teikimo metu nėra numatomas reikšmingas neigiamas poveikis aplinkai, nesukuriamas taršos šaltinis ir negeneruojamos atliekos (Aplinkos apsaugos kriterijų taikymo, vykdant žaliuosius pirkimus, tvarkos aprašo, patvirtinto Lietuvos Respublikos aplinkos ministro 2011-06-28 įsakymu Nr. D1-508, 4.4.3 punktas), todėl papildomi aplinkosauginiai reikalavimai perkamam objektui nėra nustatomi.

31. Visos Paslaugų teikėjo siūlomos paslaugos bei naudojama techninė ir programinė įranga neturi kelti grėsmės nacionaliniam saugumui Lietuvos Respublikos viešųjų pirkimų įstatymo 37 str. 8 d. prasme. Paslaugų teikėjas kartu su pasiūlymu privalo pateikti Lietuvos Respublikos viešųjų pirkimų įstatyme patvirtintos formos nacionalinio saugumo deklaracija (VPĮ 37 str. 9 d.).

32. Paslaugų teikėjas garantuoja visos iš Užsakovo gautos informacijos bei Užsakovui su paslaugų teikimu suteiktos informacijos konfidencialumą. Draudžiama perduoti bet kokią iš Užsakovo gautą ar jam su paslaugų suteikimu pateiktą informaciją tretiesiems asmenims be atsakingo Užsakovo atstovo raštiško leidimo, išskyrus teisės aktų įsakmiai numatytas išimtis.

Fizinės saugos skyriaus fizinės saugos kontrolės
grupės vadovas, pavaduojantis Fizinės saugos vadovą Algimantas Kazlauskas

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Fizinės saugos skyrius (150 / 14 / 16 / 132)
Dokumento pavadinimas (antraštė)	INFORMACIJOS SAUGUMO PAREIGŪNO KONSULTACINIŲ PASLAUGŲ PIRKIMO TECHNINĖ SPECIFIKACIJA
Dokumento registracijos data ir numeris	2025-09-22 Nr. Spc-95(13.67E)
Adresatas	Pirkimų ir sutarčių skyrius (446 / 945 / 944)
Dokumentą vizavo.	KSG vadovas Aleksandr Minič
Veiksmo atlikimo data ir laikas	2025-09-19 08:54:53
Dokumentą vizavo.	Pirkimų specialistė Gabrielė Valčiukaitė
Veiksmo atlikimo data ir laikas	2025-09-19 08:57:29
Dokumentą vizavo.	PSS vyresnysis pirkimų specialistas, pavaduojantis grupės vadovą Audrius Sipavičius
Veiksmo atlikimo data ir laikas	2025-09-19 09:19:39
Dokumentą vizavo.	Grupės vadovė Ieva Kazlauskienė
Veiksmo atlikimo data ir laikas	2025-09-19 11:48:51
Dokumentą pasirašė	FSK grupės vadovas, pavaduojantis Fizinės saugos vadovą Algimantas Kazlauskas
Veiksmo atlikimo data ir laikas	2025-09-19 12:43:11
Dokumentą tvirtino	Generalinis direktorius Linas Baužys
Veiksmo atlikimo data ir laikas	2025-09-20 11:34:14
Registratorius	Dokumentų valdymo specialistė Jolanta Grigorčenko
Veiksmo atlikimo data ir laikas	2025-09-22 09:18:40
Dokumento nuorašo atspausdinimo data ir jį atspausdinęs darbuotojas	2025-09-22 atspausdino Dokumentų valdymo specialistė Jolanta Grigorčenko

Nuorašas tikras
VĮ Ignalinos atominė elektrinė (102 / 103)
2025-09-22