UAB ŠILUTĖS ŠILUMOS TINKLAI
Verslo g.12, LT-99116 Šilutė
Tel. +370 441 62144, el. paštas: info@silutesst.lt

TECHNINĖ SPECIFIKACIJA Nr. 26-08

KIBERNETINIO SAUGUMO VADOVO PASLAUGA

IŠDUOTA:	**PATVIRTINTA** *UAB Šilutės šilumos tinklai direktoriaus 2026-03 -26 įsakymu Nr.1V-(1.6)-32*

1. BENDROSIOS NUOSTATOS

1.1. Pirkimo objektas – kibernetinio saugumo vadovo paslaugos UAB Šilutės šilumos tinklai.
1.2. Paslaugų tikslas – užtikrinti informacijos saugos ir kibernetinio saugumo valdymą, atitiktį teisės aktams bei didinti organizacijos atsparumą kibernetinėms grėsmėms.
1.3. Paslaugos turi būti teikiamos vadovaujantis galiojančiais Lietuvos Respublikos teisės aktais, Nacionalinio kibernetinio saugumo centro (NKSC) metodikomis bei TIS2 direktyvos reikalavimais.

2. PASLAUGŲ APIMTIS

Tiekėjas privalo teikti konsultacijas ir vykdyti veiklas šiose srityse:

2.1. Informacijos saugos ir kibernetinio saugumo politikos kūrimas ir tobulinimas.
2.2. IT turto saugumo ir suderinamumo vertinimas.
2.3. Žmogiškųjų išteklių saugumo užtikrinimas.
2.4. Informacijos saugumo incidentų valdymas.
2.5. Atsparumo kibernetiniams incidentams didinimas.
2.6. Informacinių sistemų ir informacinių išteklių svarbos vertinimas.
2.7. Kibernetinio saugumo rizikos vertinimas.
2.8. Techninės ir programinės įrangos tiekėjų vertinimas.
2.9. Veiklos tęstinumo valdymas (informacijos saugos aspektu).
2.10. Atitikties teisės aktams užtikrinimas.
2.11. Darbuotojų mokymų organizavimas ir efektyvumo gerinimas.
2.12. Konsultavimas IT sprendimų įsigijimo, kūrimo ir priežiūros klausimais.

3. PRIVALOMOS VEIKLOS IR REZULTATAI

3.1. Kibernetinio saugumo būklės auditas

- Atlikti auditą pagal NKSC metodiką.
- Parengti audito ataskaitą su:
  - saugumo įvertinimu,
  - nustatytais trūkumais,
  - rekomendacijomis.

3.2. Apsaugos priemonių vertinimas

- Įvertinti esamų saugumo priemonių pakankamumą.
- Pateikti ataskaitą ir rekomendacijas.

3.3. Incidentų valdymo pajėgumų vertinimas

- Įvertinti technines analizės priemones.
- Parengti gerinimo rekomendacijas.

3.4. Veiklos tęstinumo vertinimas

- Įvertinti pasirengimą incidentams.
- Parengti ataskaitą su veiksmų planu.

4. RIZIKOS VALDYMAS

4.1. Organizuoti kibernetinio saugumo rizikos vertinimą ne rečiau kaip kartą per metus.
4.2. Parengti:

- rizikos vertinimo ataskaitą,
- rizikos valdymo planą,
- rizikos mažinimo priemonių planą.

4.3. Užtikrinti:

- grėsmių analizę,
- spragų identifikavimą,
- rizikos lygio nustatymą.

4.4. Teikti duomenis į KSIS (pagal įgaliojimą).

5. INCIDENTŲ VALDYMAS

5.1. Dalyvauti incidentų tyrime ir analizėje.
5.2. Koordinuoti incidentų valdymą.
5.3. Registruoti incidentus KSIS.
5.4. Konsultuoti atsakingus darbuotojus incidentų metu.

6. KOMUNIKACIJA IR MOKYMAI

6.1. Organizuoti darbuotojų supažindinimą su saugos dokumentais.
6.2. Vykdyti nuolatinę komunikaciją apie grėsmes (ne rečiau kaip 1 kartą per mėnesį).
6.3. Teikti rekomendacijas dėl mokymų turinio ir efektyvumo.

7. POLITIKŲ IR PROCESŲ PERŽIŪRA

Ne rečiau kaip kartą per metus atlikti šių sričių peržiūrą:

7.1. Atsarginių kopijų valdymas.
7.2. IT turto gyvavimo ciklo valdymas.
7.3. Mobiliųjų įrenginių valdymas.
7.4. Jautrių duomenų apsauga.
7.5. Duomenų laikmenų valdymas.

8. TEIKĖJO ATSAKOMYBĖS

8.1. Teikti pasiūlymus dėl:

- saugumo politikų,
- organizacinių ir techninių priemonių.

8.2. Užtikrinti nuolatinį saugumo gerinimą.
8.3. Bendradarbiauti su NKSC.

9. KONTAKTINĖ INFORMACIJA

9.1. Techninę specifikaciją parengė IT specialistas – Laimondas Alminauskas, tel. Nr. (+370) 441 75534, el. paštas: it@silutesst.lt.