

KIBERNETINIO SAUGUMO REIKALAVIMAI TREČIOSIOMS ŠALIMS

(Sutarties priedas arba atskira dalis)

TIKSLAS IR TAIKymo SRITIS

Šie reikalavimai taikomi visoms trečiosioms šalims, teikiančioms IT, tinklų ir kibernetinio saugumo paslaugas arba produktus, kurie gali turėti įtakos Užsakovo tinklų ir informacinių sistemų saugumui.

Reikalavimų tikslas – užtikrinti, kad trečiųjų šalių veikla atitiktų **Lietuvos Respublikos kibernetinio saugumo įstatymo, Lietuvos Respublikos Vyriausybės nutarimo Nr. 818 bei ISO/IEC 27001:2022 ir ISO/IEC 27036-1/2 standartų reikalavimus.**

PAGRINDINIAI REIKALAVIMAI (SUTARTINIAI ĮSIPAREIGOJIMAI)

Kibernetinio saugumo derinimas.

Tiekėjas įsipareigoja derinti su Užsakovo kibernetinio saugumo vadovu visus sprendimus, galinčius turėti įtakos tinklų ir informacinių sistemų (TIS) saugumui.

Atitiktis KSĮ ir 818 nutarimui.

Tiekėjas užtikrina atitiktį Kibernetinio saugumo reikalavimų aprašo nuostatomis ir pateikia tai patvirtinančius dokumentus ar sertifikatus.

Personalo kvalifikacija.

Tiekėjo personalas turi būti apmokytas informacijos ir kibernetinio saugumo klausimais; Užsakovo prašymu pateikiami atitinkami įrodymai (sertifikatai, mokymų pažymėjimai).

Rizikų vertinimas.

Tiekėjas ne rečiau kaip kartą per metus atlieka kibernetinio saugumo rizikos vertinimą ir pateikia Užsakovui ataskaitą bei rizikų valdymo planą.

Incidentų pranešimas.

Tiekėjas nedelsdamas, bet ne vėliau kaip per 24 valandas, informuoja Užsakovą apie bet kokį incidentą, galintį paveikti Užsakovo TIS ar duomenis, ir pateikia tyrimo ataskaitą bei korekcinį veiksmų planą.

Audito teisė.

Užsakovas turi teisę atlikti tiekėjo atitikties auditą; tiekėjas privalo neatlygintinai sudaryti sąlygas auditui ir teikti visą prašomą informaciją.

Pažeidžiamumų (spragų) valdymas.

Tiekėjas turi įgyvendinti pažeidžiamumų valdymo procesą; kritinės spragos šalinamos ne vėliau kaip per 7 d., vidutinės – per 30 d.

Konfidencialumas.

Tiekėjo darbuotojai privalo pasirašyti konfidencialumo įsipareigojimus; duomenys naudojami tik sutartyje (jos prieduose) numatytiems tikslams.

Paslaugų lygio įsipareigojimai (SLA).

Paslaugų prieinamumas ne mažesnis kaip 99 %. Reagavimo į incidentus laikas – ne ilgesnis kaip 1 val. nuo aptikimo momento. Tiekėjas teikia mėnesines paslaugų kokybės ataskaitas.

Prieigos valdymas.

Prieiga prie Uždavikovo sistemų suteikiama tik pagal poreikį ir su terminuotu leidimu; visos loginės ir fizinės prieigos registruojamos.

Techninė ir fizinė aplinka.

Tiekėjas užtikrina savo patalpų, įrangos ir tinklų apsaugą, taiko duomenų šifravimą (TLS 1.3 ar naujesnį), atsargines kopijas ir fizinės apsaugos priemones.

Teisės ir pareigos.

Sutartyje (jos prieduose) apibrėžiamos abiejų šalių atsakomybės, duomenų nuosavybė ir žalos atlyginimo principai.

Ryšio ir duomenų perdavimo paslaugos.

Jeigu tiekėjas teikia interneto ar duomenų perdavimo paslaugas, sutartyje (jos prieduose) turi būti numatyta:

- reagavimas į incidentus darbo valandomis;
- nepertraukiamas paslaugų teikimas;
- sutrikimų registravimas;
- apsauga nuo DoS/DDoS atakų.

Atitikties įrodymai

Tiekėjas, Uždavikovo prašymu, pateikia:

- galiojančius sertifikatus (pvz., ISO 27001, SOC 2);
- rizikos vertinimo ar audito ataskaitas;
- incidentų registrus;
- personalo kvalifikacijos įrodymus.

Pranešimo ir kontaktų tvarka

Incidentų ir saugumo klausimais tiekėjas privalo nedelsdamas kreiptis el. paštu **el.info@vialietuva.lt** arba telefonu / el.paštu, nurodytu sutarties kontaktų dalyje.

Uždavikovas gali keisti kontaktinius asmenis atnaujindamas priedą be atskiros sutarties keitimo.

Bendros nuostatos

Šie reikalavimai yra neatskiriama sutarties dalis.

Jų nesilaikymas laikomas esminiu sutarties pažeidimu ir gali būti pagrindas sutarties nutraukimui. Visi reikalavimai taikomi sutarties galiojimo laikotarpiu ir ne trumpiau kaip iki paslaugų teikimo pabaigos.