SKAITMENINĖS SAUGOS OPERACIJŲ CENTRO PASLAUGOS (CERT)

1. Paslaugos paskirtis

1.1. Nuolat stebint AB „Ignitis grupė“ įmonių grupės (toliau – GRP) IT ir OT infrastruktūrą užkardyti kibernetinius incidentus taip užtikrinant nenutrūkstamą ir saugią GRP veiklą.
1.2. Nuolat tobulinant ir palaikant vieningą GRP Informacijos saugos vadybos sistemą (toliau – ISVS) užtikrinti Paslaugų teikėjo GRP teikiamų paslaugų skaitmeninės saugos, kibernetinių rizikų valdymą.
1.3. Mažinti grėsmes, kylančias GRP duomenų perdavimo tinkluose teikiamų paslaugų saugumo pažeidimų.
1.4. CERT paslauga yra skirta Paslaugų teikėjo teikiamų informacijos saugos paslaugų įgyvendinimui.

2. Paslaugos apimtis

Sritis	Apimties aprašymas
2.1. Kibernetinių incidentų valdymas	Kibernetinių incidentų aptikimas, valdymas ir reagavimas į kibernetinius incidentus.
2.2. Skaitmeninės saugos pažeidžiamumų valdymas	Pažeidžiamumų paieška, vertinimas ir valdymas vidinėse ir išorinėse informacinėse sistemose.
2.3. Informacijos saugos vadybos sistema	Skaitmeninės saugos srities vieningas formavimas, strateginių, valdymo ir koordinavimo vidaus teisės aktų, kitų dokumentų ir priemonių kūrimas, įgyvendinimas ir kontrolė. Skaitmeninės saugos programos vystymas ir valdymas. Paslaugų teikėjo teikiamų paslaugų sertifikavimas pagal tarptautinį informacijos saugos vadybos sistemos standartą ISO 27001. Informacijos saugos vadovo paslauga GRP įmonėms.
2.4. Skaitmeninės saugos mokymai ir konsultacijos	Skaitmeninės saugos mokymų ir konsultacijų teikimas. Socialinės inžinerijos simuliacijų, atmintinių, mokymų medžiagos rengimas ir mokymų vykdymas, konsultacijų teikimas skaitmeninės saugos klausimais, ataskaitų rengimas.
2.5. IT/OT sprendimų ir infrastruktūros saugos valdymas	Saugos reikalavimų formavimas ir jų taikymo kontrolė, rekomendacijų teikimas. IT/OT saugos rizikų vertinimas, periodiniai bei neplanuoti rizikų vertinimai, rizikų valdymo priemonių įgyvendinimo planavimas ir kontrolė.

3. Paslaugos teikimo terminai ir kokybės reikalavimai (SLA)

Sritis	Apimties aprašymas
3.1. Kibernetinių incidentų valdymas	Paslauga teikiama 24x7 darbo režimu (ne darbo valandomis organizuojant pasyvų budėjimą) Grupės informacijos saugos incidentų valdymo proceso apraše patvirtintais terminais ir apimtimi.
3.2. Skaitmeninės saugos pažeidžiamumų valdymas	Paslauga teikiama 8x5 darbo režimu. Tinklo pažeidžiamumų patikra vykdoma nerečiau kaip kartą per mėnesį. Žiniatinklio programų (angl. *WEB applications*) patikra vykdoma nerečiau kaip kartą per ketvirtį. Pažeidžiamumų patikros OT sistemose atliekamos tik iš anksto suderinus su Užsakovu, per 5 d.d. nuo užklausos. Patikrų rezultatai informacinių sistemų savininkams pateikiami per 10 d.d. po patikros. Kiti paslaugos terminai ir apimtis patvirtinti Grupės informacinio turto techninių pažeidžiamumų valdymo proceso apraše.
3.3. Informacijos saugos vadybos sistema	Paslauga teikiama 8x5 režimu be išankstinio Užsakovo užsakymo. Skaitmeninės saugos valdymo vidaus teisės aktai peržiūrimi, ir esant poreikiui atnaujinami, ne rečiau kaip kartą per metus arba pasikeitus LR/ES teisės aktams. Skaitmeninės saugos valdymo vidaus teisės aktų įgyvendinimo kontrolė atliekama ne rečiau kaip kartą per metus.

Sritis	Apimties aprašymas
	Skaitmeninės saugos strateginių, valdymo ir koordinavimo įgyvendinimas atliekamas vidaus ir išorės teisės aktuose nustatytais terminais.
3.4. Skaitmeninės saugos mokymai ir konsultacijos	Paslauga teikiama 8x5 režimu. Vykdoma ne mažiau kaip 4 socialinės inžinerijos simuliacijos per metus Grupėje (ne rečiau kaip kas ketvirtį) Kartą per metus organizuojami privalomi mokymai. Mokymų medžiaga atnaujinama ne rečiau kaip kartą per metus. Konsultacijos skaitmeninės saugos klausimais teikiamos pagal Užsakovo paklausimą. Konsultacija suteikiama per 5 d.d., jei su Užsakovu nesusitarta kitaip. Skaitmeninės saugos ataskaitos rengiamos pagal Užsakovo paklausimą, per 5 d.d. iš esamų duomenų rinkinių, ir per 30 d.d., jei ataskaitai parengti reikia naujo duomenų rinkinio. Išorės institucijoms ataskaitos ir pranešimai, numatyti teisės aktuose, rengiamos ir teikiamos be Užsakovo išankstinio paklausimo, teisės aktų nustatytais terminais ir apimtimi.
3.5. IT/OT sprendimų ir infrastruktūros saugos valdymas	Paslauga teikiama 8x5 režimu. Saugos reikalavimų formavimas atliekamas per 10 d.d. nuo Užsakovo užsakymo. Saugos reikalavimų taikymo periodinė kontrolė atliekama ne rečiau kaip kartą per metus, pagal ekspertiškai nustatytą imtį. Saugos reikalavimų taikymo kontrolė prieš įgyvendinant pokytį atliekama per 3 d.d. IT saugos rizikų vertinimas periodiškai atliekamas ne rečiau kaip kartą per metus. Neplanuoti rizikų vertinimai atliekami pagal Užsakovo poreikį, per 10 d.d. Vidaus ir išorės auditų, susijusių su skaitmenine sauga, vykdymas ir koordinavimas atliekamas teisės aktų nustatyti apimtimi. Informacijos saugumo valdymo sistemos ISO 27001 priežiūros auditai organizuojami kartą per metus, pakartotinio sertifikavimo – kas tris metus. Audito planas dalyviams pateikiamas ne vėliau kaip dvi savaitės iki audito datos.

4. Konsultacijos

4.1. Konsultacijų, susijusių su CERT teikimas Užsakovui.

5. Paslaugos teikimo ribos

5.1. Paslaugų teikėjas atsako, kad skaitmeninės saugos operacijų centro paslaugos būtų teikiamos pagal galiojančius vidaus ir išorės teisės aktus.