					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P35S					Dokumento pavadinimas: **IoT / OT saugumo politika**							
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:							
X	Politika		Standartas		Procedūra		Forma		Registras		Kita	

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

Suderinamumas su standartais ir reglamentais

Standartas / reglamentas	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	6.1, 6.2, 8 skyriai	
ISO/IEC 27002:2022	Kontrolės priemonės 5.23, 5.31	
NIST SP 800-53 Rev.5	SI-7, CM-7, AC-6, PE-20, SC-7	
ES BDAR	32 straipsnis	
ES NIS2 direktyva	21 straipsnio 2 dalies a, d, f punktai	
ES DORA reglamentas	9 straipsnio 2 dalis, 10 straipsnio 1 dalis	

1. Tikslas

1.1. Ši politika nustato privalomas saugaus daiktų interneto (IoT) ir operacinių technologijų (OT) įrenginių naudojimo ir valdymo taisykles organizacijoje. Tokie įrenginiai gali apimti išmaniuosius jutiklius, apsaugos kameras, gamybos įrenginius, ŠVOK valdiklius ar bet kurias prie tinklo prijungtas pramonines sistemas.

1.2. Šios politikos tikslas yra:

1.2.1. apsaugoti fizines ir skaitmenines operacijas nuo sutrikdymo ar manipuliavimo per nepakankamai apsaugotus prijungtus įrenginius

1.2.2. užtikrinti saugų IoT ir OT sistemų diegimą, stebėseną ir priežiūrą

1.2.3. užtikrinti atitiktį ISO/IEC 27001:2022, NIS2 direktyvai ir susijusiems reguliavimo reikalavimams

1.2.4. nustatyti praktiškas ir įgyvendinamas kontrolės priemones MVĮ, veikiančioms biuro, sandėlio ar gamybos aplinkose

2. Taikymo sritis

2.1. Ši politika taikoma visiems asmenims, dalyvaujantiems planuojant, diegiant, konfigūruojant, naudojant, prižiūrint ar šalinant IoT ar OT įrenginius. Tai apima:

2.1.1. darbuotojus, rangovus ar praktikantus, turinčius fizinę arba nuotolinę prieigą prie įrenginių

2.1.2. trečiųjų šalių tiekėjus ar paslaugų technikus, diegiančius arba prižiūrinčius prijungtas sistemas

2.1.3. generalinį direktorių ar darbuotojus, atsakingus už saugumo politikų priežiūrą

2.2. Politika apima:

2.2.1. IoT įrenginius, tokius kaip išmaniosios spynos, stebėjimo sistemos, išmanieji skaitikliai ar spausdintuvai

2.2.2. OT sistemas, įskaitant programuojamuosius loginius valdiklius (PLC), SCADA skydus ar pramoninius šliuzus

2.2.3. šių sistemų naudojamą pagalbinę aparatinę įrangą, valdymo programinę įrangą ir ryšių tinklus

2.3. Ši politika taikoma visose darbo vietose: biuro aplinkose, nuotolinėse vietose, gamybos zonose ir debesijos platformose, susietose su šiais įrenginiais.

3. Tikslai

3.1. Saugus diegimas: užtikrinti, kad visos IoT / OT sistemos prieš įtraukiant jas į eksploatacinę aplinką būtų saugiai sukonfigūruotos.

3.2. Ekspozicijos ribojimas: užkirsti kelią neteisėtai prieigai, netinkamam naudojimui ar prijungtų įrenginių perėmimui, taikant griežtą prieigos kontrolę ir tinklo segmentavimą.

3.3. Nuolatinė stebėsena: užtikrinti IoT / OT operacijų matomumą, registruojant veiklą žurnaluose ir stebint neįprastą elgseną.

3.4. Tiekėjų atskaitomybė: užtikrinti, kad trečiųjų šalių paslaugų teikėjai laikytųsi saugaus diegimo, konfigūravimo ir priežiūros praktikos.

3.5. Atitiktis reguliavimo reikalavimams: pagrįsti visišką atitiktį taikomiems standartams, tokiems kaip ISO 27001, ES BDAR (jei renkami asmens duomenys) ir NIS2 direktyva, siekiant užtikrinti kritinės infrastruktūros atsparumą.

4. Vaidmenys ir atsakomybės

4.1. Generalinis direktorius (GD)

4.1.1. atsako už bendrą IoT ir OT sistemų saugumą

4.1.2. tvirtina šią politiką ir užtikrina jos taikymą visose veiklos srityse

4.1.3. tikrina, ar tiekėjai ir rangovai laikosi saugaus diegimo ir priežiūros praktikos

4.1.4. autorizuoja tinklo prieigą bet kuriai IoT / OT sistemai

4.2. Paskirtas darbuotojas arba veiklos vadovas (jei paskirtas)

4.2.1. prižiūri IoT / OT įrenginių apskaitą, išdėstymą ir konfigūraciją

4.2.2. registruoja kiekvieno įrenginio vietą, tinklo priskyrimą ir priežiūros dokumentaciją

4.2.3. užtikrina, kad visi pakeitimai (pvz., programinės aparatinės įrangos atnaujinimai ar įrenginių pakeitimai) būtų dokumentuojami

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Peržiūros ir atnaujinimo reikalavimai

9.1. Metinė peržiūra

9.1.1. Ši politika turi būti peržiūrima bent kartą per metus GD

9.1.2. Peržiūros metu turi būti įvertinta, ar politika išlieka veiksminga, apima esamus įrenginių tipus ir atitinka naujas rizikas ar technologijas

9.2. Atnaujinimai pagal įvykius

9.2.1. Politikos atnaujinimai taip pat turi būti inicijuojami, kai:

9.2.2. įdiegiami nauji IoT ar OT sistemų tipai

9.2.3. tiekėjai paskelbia saugumo pranešimus arba eksploatavimo pabaigos pranešimus

9.2.4. incidentas arba auditas nustato IoT / OT kontrolės priemonių spragas

9.2.5. nauji teisės aktai arba standartai nustato papildomus reikalavimus

9.3. Dokumentavimas ir versijų kontrolė

9.3.1. Visi atnaujinimai turi būti dokumentuojami, įskaitant datą, versijos numerį ir pakeitimų santrauką

9.3.2. GD turi saugoti istorines politikos versijas audito tikslais

9.4. Pakeitimų komunikavimas

9.4.1. Bet kokie politikos atnaujinimai turi būti pateikti visiems susijusiems darbuotojams ir tiekėjams

9.4.2. Atnaujintos versijos turi būti prieinamos bendruose aplankuose arba spausdintoje medžiagoje diegimo vietose ar valdymo centruose

10. Susijusios politikos ir sąsajos

10.1. Ši politika turi būti įgyvendinama suderintai su šiomis susijusiomis MVĮ politikomis:

10.1.1. P4S – Prieigos kontrolės politika: nustato įrenginių lygmens prisijungimo kontrolės priemones, stiprių slaptažodžių naudojimą ir autorizuotos prieigos procedūras IoT ir OT platformoms

10.1.2. P9S – Nuotolinio darbo politika: draudžia naudoti nuotolinę prieigą prie IoT / OT valdymo skydų nesaugiais ar nepatvirtintais kanalais

10.1.3. P17S – Duomenų apsaugos ir privatumo politika: taikoma, jei IoT įrenginiai (pvz., apsaugos kameros) tvarko arba įrašo asmens duomenis, užtikrinant atitiktį ES BDAR

10.1.4. P30S – Reagavimo į incidentus politika: nustato IoT ar OT incidentų, įskaitant įtariamą manipuliavimą ar veiklos sutrikimą, aptikimo, pranešimo ir sprendimo procedūras

10.1.5. P36S – Socialinių tinklų ir išorinės komunikacijos politika: užtikrina, kad informacija apie įrenginius ar tinklo išdėstymą nebūtų atskleidžiama išorėje be patvirtinimo

10.2. Kiekviena susijusi politika sustiprina šios politikos taikymą ir praktinį naudojimą, nustatydama tikslines procedūrines gaires.

11. Pamatiniai standartai ir sistemos

11.1. ISO/IEC 27001

11.1.1. 6.1 punktas – rizikų identifikavimas ir rizikos tvarkymas: reikalauja, kad rizikos, susijusios su IoT ir OT sistemomis, būtų sistemingai vertinamos ir mažinamos

11.1.2. 8.1 punktas – operacijų planavimas ir kontrolė: užtikrina saugią prijungtų įrenginių operacinę kontrolę

11.2. ISO/IEC 27002

11.2.1. Kontrolės priemonė 5.23 – informacijos saugumas naudojant operacinių technologijų (OT) sistemas: apibrėžia saugų OT naudojimą fizinėse ir skaitmeninėse aplinkose

11.2.2. Kontrolės priemonė 5.31 – saugi informacinių sistemų konfigūracija: reikalauja sustiprintos IoT / OT įrenginių konfigūracijos ir nesaugių numatytųjų nustatymų vengimo

11.3. NIST SP 800-53 Rev.5

11.3.1. SI-7 – programinės įrangos, programinės aparatinės įrangos ir informacijos vientisumas: reikalauja programinės aparatinės įrangos ir atnaujinimų vientisumo patvirtinimo

11.3.2. CM-7 – mažiausio funkcionalumo principas: įrenginiuose negali būti įjungtų nenaudojamų ar nesaugių funkcijų

11.3.3. AC-6 – mažiausių privilegijų principas: prieiga prie įrenginių turi būti ribojama tik autorizuotiems naudotojams

11.3.4. PE-20 – turto stebėsena: fizinė ir operacinė IoT ir OT turto stebėsena

11.3.5. SC-7 – ribų apsauga: tinklo ryšių segmentavimas ir kontrolė prijungtoms sistemoms

11.4. ES BDAR (2016/679)

11.4.1. 32 straipsnis – tvarkymo saugumas: jei renkami asmens duomenys (pvz., per stebėjimo kameras), organizacija turi įgyvendinti tinkamas technines ir organizacines priemones tokiam tvarkymui apsaugoti

11.5. ES NIS2 direktyva (2022/2555)

11.5.1. 21 straipsnio 2 dalies a punktas – rizikos valdymo priemonės

11.5.2. 21 straipsnio 2 dalies d punktas – saugi įrenginių konfigūracija ir naudojimas

11.5.3. 21 straipsnio 2 dalies f punktas – tiekimo grandinės ir sistemų saugumas

11.6. ES DORA reglamentas (2022/2554)

11.6.1. 9 straipsnio 2 dalis – IRT rizikos valdymo taikymo sritis: apima pramoninius ir integruotus įrenginius, naudojamus operacinėse aplinkose

11.6.2. 10 straipsnio 1 dalis – IRT veiklos tęstinumas: reikalauja, kad įrenginių konfigūracijos palaikytų atsparumą ir atkūrimo operacijas

11.7. COBIT 2019

11.7.1. DSS01 – operacijų valdymas: taikoma technologinių operacijų priežiūrai, įskaitant fizinius įrenginius

11.7.2. DSS05 – saugumo paslaugų valdymas: užtikrina, kad prijungtos sistemos būtų tinkamai stebimos ir apsaugotos

11.7.3. APO13 – saugumo valdymas: stiprina politikas, skirtas operacinių išteklių apsaugai MVĮ aplinkoje