					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P35					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**

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	8 skyrius	
ISO/IEC 27002:2022	Kontrolės priemonės 5.7, 5.23, 5.27, 5.31, 5.36	
NIST SP 800-53 Rev.5	SC-7, SI-4, CM-2, AC-6, PL-8	
ES BDAR	5, 25, 32 straipsniai	
ES NIS2 direktyva	21, 23 straipsniai	
ES DORA reglamentas	9, 10 straipsniai	
COBIT 2019	DSS05.01, BAI09.01, APO13.02	

1. Tikslas

1.1 Ši politika nustato privalomuosius informacijos saugumo reikalavimus daiktų interneto (IoT) ir operacinių technologijų (OT) sistemų diegimui, eksploatavimui, stebėsenai ir eksploatacijos nutraukimui organizacijoje.

1.2 Ji užtikrina, kad tokios sistemos būtų integruotos į bendrą organizacijos kibernetinio saugumo valdymo sistemą ir apsaugotos nuo kompromitavimo, netinkamo naudojimo ar veiklos sabotažo.

1.3 Šios politikos tikslas – užtikrinti, kad būtų taikomos stiprios techninės, organizacinės ir procedūrinės kontrolės priemonės, siekiant apsaugoti IoT / OT sistemas, sąveikaujančias su fizine infrastruktūra, gamybos procesais ir saugai kritinėmis aplinkomis.

1.4 Ji padeda vykdyti reguliacinius ir sutartinius įsipareigojimus kibernetinio saugumo, saugos, aplinkos kontrolės ir veiklos tęstinumo srityse.

2. Taikymo sritis

2.1 Ši politika taikoma visoms IoT ir OT sistemoms, naudojamoms organizacijos veiklos, administracinėje ar gamybinėje aplinkoje, nepriklausomai nuo to, ar jos priklauso organizacijai, yra nuomojamos, ar teikiamos trečiųjų šalių.

2.2 Į taikymo sritį įtraukiamos, be kita ko, šios sistemos:

2.2.1 IoT įrenginiai, tokie kaip aplinkos jutikliai, patekimo kontrolės priemonės, išmanusis apšvietimas, stebėjimo įranga ir dėvimieji įrenginiai

2.2.2 OT platformos, tokios kaip PLC, SCADA, DCS, HMI pultai, MES sąsajos ir lauko valdikliai

2.2.3 Pramoniniai valdymo tinklai arba su debesijos paslaugomis sujungtas turtas, skirtas fizinių operacijų stebėsenai

2.3 Politika apima:

2.3.1 Visas aplinkas (vietines, kraštines, valdomas debesijos paslaugų)

2.3.2 Visas suinteresuotąsias šalis (vidaus naudotojus, integratorius, trečiųjų šalių tiekėjus, rangovus)

2.3.3 Visus gyvavimo ciklo etapus (projektavimą, įsigijimą, diegimą, eksploatavimą, eksploatacijos nutraukimą)

3. Tikslai

3.1 Apsaugoti IoT ir OT infrastruktūrą nuo vidinių ir išorinių kibernetinio saugumo grėsmių, įskaitant paslaugos trikdymą, neleistiną prieigą, išpirkos reikalaujančių programų plitimą ir programinės aparatinės įrangos klastojimą.

3.2 Užtikrinti, kad IoT / OT platformos netaptų IT ir OT sąsajos atakų vektoriais ir nesukeltų saugai kritinių sistemų kompromitavimo.

3.3 Taikyti saugumą pagal projektavimą ir daugiasluoksnės gynybos principus per visą šių technologijų gyvavimo ciklą.

3.4 Sudaryti sąlygas patikimai, saugiai ir audituojamai IoT ir OT platformų integracijai į organizacijos saugumo operacijų centrą (SOC) ir reagavimo į incidentus planus.

3.5 Užtikrinti, kad visi diegimai atitiktų ISO/IEC 27001 kontrolės priemones ir taikytinas sektorines gaires, pvz., IEC 62443, ISO 27019 ir NIST SP 800-82.

4. Vaidmenys ir atsakomybės

4.1 Informacijos saugumo vadovas (CISO) / saugumo funkcijos vadovas

4.1.1 Nustato IoT / OT kibernetinio saugumo politiką ir techninius standartus

4.1.2 Prižiūri rizikos vertinimus, kontrolės priemonių validavimą ir koordinavimą tarp padalinių

4.2 OT inžinieriai / objektų ir gamyklų vadovai

4.2.1 Validuoja OT sistemų konfigūracijas ir užtikrina politikos laikymąsi gamybinėse zonose

4.2.2 Palaiko fizines ir logines apsaugos priemones OT vientisumui ir saugai užtikrinti

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Ši politika turi būti peržiūrima ne rečiau kaip kartą per metus ir atnaujinama atsižvelgiant į:

9.1.1 OT ar IoT sistemų architektūros, tiekėjų ar platformų pokyčius

9.1.2 Reikšmingus reguliacinius pakeitimus, pvz., DORA reglamento, NIS2 direktyvos ar sektorinių direktyvų pakeitimus

9.1.3 Naujų pažeidžiamumų ar grėsmių modelių atsiradimą valdymo sistemose

9.1.4 Vidaus ar išorės auditų, įsiskverbimo testų ar red team pratybų išvadas

9.2 CISO, OT saugumo vadovas ir atitinkamų padalinių vadovai atsako už bendrą peržiūros proceso inicijavimą.

9.3 Tarpinės peržiūros turi būti inicijuojamos po:

9.3.1 Bet kurio su IoT / OT susijusio incidento, dėl kurio įvyko sistemos sutrikimas arba duomenų praradimas

9.3.2 Reikšmingo naujos įrangos, stebėsenos programinės įrangos ar programinės aparatinės įrangos platformų įdiegimo

9.3.3 Išmaniojo kraštinio skaičiavimo arba DI papildyto automatizavimo integravimo lauko lygmenyje

9.4 Visi politikos pakeitimai turi būti:

9.4.1 Dokumentuojami versijų istorijoje ir Politikos pakeitimų registre

9.4.2 Komunikuojami visiems paveiktiems naudotojams, tiekėjams ir IT / OT operatoriams

9.4.3 Pakartotinai tvirtinami vykdomosios vadovybės

10. Susijusios politikos ir sąsajos

10.1 Ši politika taikoma kartu su toliau nurodytomis informacijos saugumo politikomis ir yra jų palaikoma:

10.1.1 P1 – Informacijos saugumo politika: nustato pagrindinius saugumo principus, taikomus ir IoT bei OT sistemų saugumui.

10.1.2 P3 – Priimtino naudojimo politika: nustato asmeninių ir neautorizuotų įrenginių naudojimo apribojimus, įskaitant eksploatacines aplinkas.

10.1.3 P6 – Rizikos valdymo politika: nustato su įterptosiomis ir valdymo sistemomis susijusios rizikos vertinimo, priėmimo ir mažinimo gaires.

10.1.4 P12 – Turto valdymo politika: užtikrina, kad visos IoT ir OT sistemos būtų formaliai įtrauktos į apskaitą ir joms būtų priskirti atsakingi savininkai.

10.1.5 P20 – Galinių įrenginių apsaugos / kenkėjiškos programinės įrangos politika: taikoma prijungtiems valdikliams, išmaniesiems šliuzams ir kraštinėms sistemoms gamyboje.

10.1.6 P22 – Žurnalų tvarkymo ir stebėsenos politika: taikoma ir žurnalų surinkimo bei peržiūros procedūroms OT aplinkose.

10.1.7 P30 – Reagavimo į incidentus politika: tiesiogiai nustato, kaip turi būti eskaluojami ir valdomi IoT / OT pažeidimai, anomalijos ar sistemų sutrikimai.

10.1.8 P33 – Audito ir atitikties stebėsenos politika: nustato užtikrinimo mechanizmus, skirtus patvirtinti nuolatinę atitiktį šiai politikai.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika suderinta su tarptautiniu mastu pripažintais standartais ir reguliavimo sistemomis, kurios užtikrina daiktų interneto (IoT) ir operacinių technologijų (OT) sistemų saugumą, atsparumą ir atitiktį pramonės, gamybos ir organizacijos aplinkose.

11.2 ISO/IEC 27002:2022 – kontrolės priemonės 5.7, 5.23, 5.27, 5.31, 5.36

11.2.1 Kontrolės priemonė 5.7 – Grėsmių žvalgyba: padeda užtikrinti OT aplinkų stebėseną ir IoT būdingų pažeidžiamumų nustatymą.

11.2.2 Kontrolės priemonė 5.23 – Informacijos saugumas naudojantis debesijos paslaugomis: taikoma, kai IoT įrenginiai sąveikauja su debesijos platformomis telemetrijos, valdymo ar analitikos tikslais.

11.2.3 Kontrolės priemonė 5.27 – Saugi sistemų architektūra ir inžineriniai principai: reglamentuoja saugumo pagal projektavimą principų taikymą įterptosioms sistemoms ir valdymo tinklams.

11.2.4 Kontrolės priemonė 5.31 – Saugumas kūrimo ir palaikymo procesuose: nustato programinės įrangos ir programinės aparatinės įrangos validavimo, pataisų kontrolės ir tiekėjų reikalavimus OT diegimuose.

11.2.5 Kontrolės priemonė 5.36 – Atitiktis teisiniams ir sutartiniams reikalavimams: užtikrina OT turto atitiktį saugos, aplinkosaugos ir reguliaciniams reikalavimams.

11.2.6 Šios kontrolės priemonės kartu nustato gerąją praktiką, skirtą IoT / OT sistemų apsaugai viso jų gyvavimo ciklo metu, įskaitant architektūros projektavimą, saugų diegimą, pataisų valdymą, anomalijų aptikimą ir atitiktį sektoriniams reikalavimams.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-7 – Ribų apsauga: užtikrina, kad OT tinklai būtų segmentuoti ir apsaugoti nuo neautorizuotos prieigos.

11.3.2 SI-4 – Sistemų stebėsena: reikalauja įgyvendinti nuolatinės stebėsenos ir anomalijų aptikimo mechanizmus ICS aplinkose.

11.3.3 CM-2 – Bazinė konfigūracija: nustato konfigūracijos valdymo ir IoT / OT platformų stiprinimo reikalavimus.

11.3.4 AC-6 – Mažiausių privilegijų principas: taikomas naudotojų prieigai ir nuotolinei tiekėjų priežiūrai įterptosiose valdymo sistemose.

11.3.5 PL-8 – Saugumo ir privatumo architektūros: reglamentuoja saugaus sistemų integravimo planavimą, ypač OT modernizavimo projektuose.

11.4 ES BDAR (2016/679)

11.4.1 5 straipsnis – Su asmens duomenų tvarkymu susiję principai: taikomas IoT platformoms, tvarkančioms jutiklių ar elgsenos duomenis, susietus su fiziniais asmenimis.

11.4.2 25 straipsnis – Duomenų apsauga pagal projektavimą ir pagal numatytuosius nustatymus: reikalauja privatumo apsaugos priemones integruoti į IoT produktų projektavimą ir programinę aparatinę įrangą.

11.4.3 32 straipsnis – Tvarkymo saugumas: nustato šifravimo, prieigos kontrolės ir saugių ryšių reikalavimus išmaniųjų įrenginių duomenų perdavimui.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 ir 23 straipsniai: nustato saugumo pareigas esminiams ir svarbiems subjektams, naudojantiems OT sistemas. Tai apima rizikos vertinimą, pranešimą apie incidentus ir IoT / OT tiekėjų bei programinės aparatinės įrangos vientisumo tikrinimą tiekimo grandinėje.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 9 straipsnis – IRT rizikos valdymas: reikalauja saugios įterptųjų sistemų ir OT technologijų integracijos į IRT rizikos valdysenos programą.

11.6.2 10 straipsnis – IRT saugumo reikalavimai: nustato apsaugos priemones tarpusavyje susietoms OT platformoms, naudojamoms finansinių ir kritinių paslaugų aplinkose.

11.7 COBIT 2019

11.7.1 DSS05.01 – Apsauga nuo kenkėjiškos programinės įrangos: apima ICS būdingų grėsmių ir IoT kenkėjiškos programinės įrangos kampanijų aptikimą bei reagavimą į jas.

11.7.2 BAI09.01 – Saugumo reikalavimų nustatymas ir palaikymas: susiejama su saugiu išmaniosios ar įterptosios infrastruktūros parengimu ir eksploatavimu.

11.7.3 APO13.02 – Informacijos saugumo plano nustatymas ir palaikymas: reikalauja įtraukti OT sistemas ir jų pažeidžiamumus į visos organizacijos kibernetinio saugumo strategiją.