					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P21S					Dokumento pavadinimas: **Tinklo 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	8 kontrolė	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
ES BDAR	32 straipsnis	-
ES NIS2 direktyva	21 straipsnio 2 dalies d, e punktai	-
ES DORA reglamentas	9, 10 straipsniai	-
COBIT 2019	DSS05.02, APO13	-

1. Tikslas

1.1. Šios politikos tikslas – užtikrinti, kad visas vidinis ir išorinis tinklo ryšys būtų apsaugotas nuo neteisėtos prieigos, klastojimo, pasiklausymo ir netinkamo naudojimo, taikant aiškiai apibrėžtas saugumo kontrolės priemones.

1.2. Ši politika nustato saugaus tinklo infrastruktūros projektavimo, naudojimo ir valdymo taisykles, įskaitant maršrutizatorius, belaidės prieigos taškus, nuotolinės prieigos jungtis ir segmentuotus tinklus.

1.3. Šia politika siekiama sumažinti interneto grėsmių poveikį, užtikrinti vidiniais ir išoriniais tinklais perduodamų duomenų konfidencialumą ir palaikyti kritinių paslaugų prieinamumą.

1.4. Ši politika padeda siekti ISO/IEC 27001:2022 sertifikavimo ir tiesiogiai prisideda prie teisinių bei reguliavimo reikalavimų pagal ES BDAR, NIS2 direktyvą ir DORA reglamentą įgyvendinimo, kartu suteikdama techninį užtikrinimą klientams ir auditoriams.

2. Taikymo sritis

2.1. Ši politika taikoma visiems organizacijos IT tinklo komponentams, įskaitant:

2.1.1. Laidinę ir belaidę infrastruktūrą biuro vietose

2.1.2. Maršrutizatorius, komutatorius, prieigos taškus, ugniasienes ir šliuzus

2.1.3. Nuotolinės prieigos jungtis, įskaitant VPN, RDP ir debesijos tunelius

2.1.4. Debesijos aplinkoje veikiančias taikomąsias programas, pasiekiamas iš vidinių arba išorinių tinklų

2.1.5. Įrenginius, prijungtus prie tinklo darbuotojų, rangovų ar svečių

2.2. Ši politika reglamentuoja tiek fizinius, tiek loginius tinklo segmentus, įskaitant svečių zonas, IoT įrenginius ir vidinių administracinių funkcijų sistemas.

2.3. Politika taikoma visam personalui, turinčiam prieigą prie organizacijos tinklo, įskaitant:

2.3.1. Vidaus darbuotojus

2.3.2. Nuotoliniu ir hibridiniu būdu dirbančius darbuotojus

2.3.3. Išorės tiekėjus, konsultantus ir paslaugų teikėjus

2.3.4. Svečius, besinaudojančius laikina Wi-Fi prieiga

3. Tikslai

3.1. Užtikrinti, kad organizacijos tinklas būtų apsaugotas nuo neteisėtos prieigos ir išorinių kibernetinių grėsmių

3.2. Užtikrinti tinkamą segmentavimą tarp patikimų ir nepatikimų tinklų (pvz., svečių Wi-Fi, tiekėjų prieigos)

3.3. Sudaryti sąlygas saugiam nuotoliniam prisijungimui nepažeidžiant vidinių sistemų saugumo

3.4. Užkirsti kelią kenkėjiškos programinės įrangos plitimui ir duomenų iškėlimui per tinklo kanalus

3.5. Užtikrinti tinklo veiklos stebėseną, įspėjimus ir auditą, kad būtų palaikomas incidentų aptikimas ir atitiktis

3.6. Užtikrinti, kad prie vidinių tinklų galėtų jungtis tik patvirtinti ir apsaugoti įrenginiai

3.7. Įvykdyti įpareigojimus pagal ISO 27001, ES BDAR ir susijusius kibernetinio saugumo reikalavimus

4. Vaidmenys ir atsakomybės

4.1. Generalinis vadovas (GM)

4.1.1. Yra šios politikos savininkas ir užtikrina, kad būtų skirti tinkami ištekliai saugiam tinklo projektavimui ir valdymui

4.1.2. Peržiūri išimtis iš tinklo saugumo kontrolės priemonių ir tvirtina tiekėjų tinklo prieigos susitarimus

4.1.3. Peržiūri incidentus ar audito išvadas, susijusias su tinklo saugumo trūkumais

4.2. IT paslaugų teikėjas / vidaus IT funkcija

4.2.1. Įgyvendina, konfigūruoja ir prižiūri visas ugniasienes, maršrutizatorius, komutatorius ir belaidžio ryšio valdiklius

4.2.2. Valdo segmentavimą tarp vidinių, svečių ir išorinių tinklų

4.2.3. Stebi žurnalus ir įspėjimus dėl neteisėtos prieigos bandymų ar tinklo anomalijų

4.2.4. Užtikrina, kad programinės aparatinės įrangos ir konfigūracijų atnaujinimai būtų taikomi saugiai ir laiku

[... 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 ne rečiau kaip kartą per metus Generalinio vadovo kartu su IT paslaugų teikėju ir privatumo koordinatoriumi.

9.2. Tarpinės peržiūros inicijavimo sąlygos

9.2.1. Politikos peržiūra taip pat turi būti inicijuojama šiais atvejais:

9.2.1.1. Esminiai tinklo architektūros pokyčiai (pvz., naujos VPN ar ugniasienių sistemos)

9.2.1.2. Su tinklu susijęs incidentas (pvz., įsilaužimas, išpirkos reikalaujančios programinės įrangos plitimas ar duomenų iškėlimas)

9.2.1.3. Teisiniai, reguliavimo ar sistemų atnaujinimai, turintys įtakos tinklo apsaugai

9.2.1.4. Naujos tiekėjų platformos, kurioms reikalingi alternatyvūs prieigos metodai ar protokolai

9.3. Versijų valdymas ir dokumentavimas

9.3.1. Politikos pakeitimai turi būti registruojami nurodant versijos numerį, datą ir pakeitimų santrauką

9.3.2. Ankstesnės versijos turi būti archyvuojamos ne trumpiau kaip 3 metus

9.3.3. Apie atnaujinimus turi būti pranešta susijusiems darbuotojams, o kai įvedami reikšmingi elgsenos pokyčiai, turi būti gautas privalomas patvirtinimas

10. Susijusios politikos ir sąsajos

10.1. Ši politika turi būti įgyvendinama kartu su šiomis MVĮ saugumo politikomis:

10.1.1. P9S – Nuotolinio darbo politika: nustato saugius nuotolinės prieigos metodus, VPN reikalavimus ir galinių įrenginių apsaugą ne biure dirbantiems naudotojams.

10.1.2. P12S – Turto valdymo politika: užtikrina, kad visos prie tinklo prijungtos sistemos būtų identifikuotos, suskirstytos į kategorijas ir stebimos pagal aktualią saugumo būklę.

10.1.3. P17S – Duomenų apsaugos ir privatumo politika: užtikrina, kad tinklo segmentavimas, prieigos kontrolės priemonės ir žurnalavimas palaikytų privatumo ir duomenų apsaugos principus pagal ES BDAR.

10.1.4. P22S – Žurnalų tvarkymo ir stebėsenos politika: nustato reikalavimus tinklo įrenginių, nuotolinių jungčių ir belaidžio ryšio valdiklių žurnalų rinkimui ir peržiūrai.

10.1.5. P30S – Reagavimo į incidentus politika: apibrėžia privalomus veiksmus reaguojant į tinklo pažeidimus, neteisėtos prieigos bandymus ar kenkėjiškos programinės įrangos plitimą per vidinius tinklus.

11. Pamatiniai standartai ir sistemos

11.1. ISO/IEC 27001

11.1.1. 8.1 skyrius – reikalauja įgyvendinti kontrolės priemones, užtikrinančias saugias ir atsparias operacijas, įskaitant tinklus.

11.2. ISO/IEC 27002

11.2.1. 8.20 kontrolė – pateikia technines ir procedūrines gaires dėl tinklo prieigos, segmentavimo ir stebėsenos saugumo.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – reikalauja valdyti informacijos srautus tinkluose ir tarp sistemų.

11.3.2. SC-7 – reikalauja ribų apsaugos, saugaus maršrutizavimo ir tinklo segmentavimo, siekiant sumažinti neteisėtos prieigos riziką.

11.4. ES BDAR

11.4.1. 32 straipsnis – reikalauja tinkamų techninių ir organizacinių priemonių, kad būtų užtikrintas asmens duomenis tvarkančių tinklinių sistemų ir paslaugų konfidencialumas, vientisumas ir prieinamumas.

11.5. ES NIS2 direktyva

11.5.1. 21 straipsnio 2 dalies d punktas – reikalauja rizika grindžiamų techninių priemonių, įskaitant tinklo saugumą ir prieigos kontrolę.

11.5.2. 21 straipsnio 2 dalies e punktas – reikalauja sistemų segmentavimo ir izoliavimo, kad būtų užkirstas kelias kibernetinių incidentų plitimui.

11.6. ES DORA reglamentas

11.6.1. 9 straipsnis – reikalauja, kad įmonės įgyvendintų IRT rizikos valdymo kontrolės priemones, įskaitant saugiems tinklams ir komunikacijai skirtas priemones.

11.6.2. 10 straipsnis – reikalauja, kad skaitmeninio atsparumo strategijos apimtų tinklo infrastruktūros ir nuotolinio prisijungimo apsaugą.

11.7. COBIT 2019

11.7.1. DSS05.02 – reikalauja veiksmingos IT infrastruktūros ir tinklo aplinkų apsaugos nuo vidinių ir išorinių grėsmių.

11.7.2. APO13.01 – reikalauja rizikos valdymo strategijų, kurios kaip grėsmių mažinimo dalį apimtų tinklo segmentavimą ir stebėseną.