					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P21					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	Komentaras
ISO/IEC 27001:2022	8 skyrius	Netaikoma
ISO/IEC 27002:2022	8.20-8.22 kontrolės priemonės	Netaikoma
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	Netaikoma
ES BDAR	32 straipsnis	Netaikoma
ES NIS2 direktyva	21 straipsnio 2 dalies d punktas	Netaikoma
ES DORA reglamentas	9 straipsnis	Netaikoma
COBIT 2019	DSS01.03, DSS05.01, MEA03	Netaikoma

1. Tikslas

1.1 Šios politikos tikslas – nustatyti organizacijos reikalavimus, skirtus apsaugoti jos vidinius ir išorinius tinklus nuo neteisėtos prieigos, paslaugų sutrikdymo, duomenų perėmimo ir netinkamo naudojimo.

1.2 Ji užtikrina, kad visa tinklo infrastruktūra, įskaitant fizinę, virtualiąją, debesijos ir hibridinę infrastruktūrą, būtų apsaugota taikant sluoksniuotos gynybos modeliu grindžiamas kontrolės priemones, tokias kaip segmentavimas, ugniasienių taisyklių taikymas, saugus maršruto parinkimas ir centralizuota stebėsena.

1.3 Ši politika įgyvendina ISO/IEC 27001 8 skyriaus ir ISO/IEC 27002:2022 8.20-8.22 kontrolės priemonių reikalavimus bei užtikrina atitiktį taikomiems teisiniams ir reglamentavimo įpareigojimams pagal ES BDAR 32 straipsnį, NIS2 direktyvos 21 straipsnį ir DORA reglamento 9 straipsnį.

2. Taikymo sritis

2.1 Ši politika taikoma visiems tinklams ir susijusiems infrastruktūros komponentams, įskaitant:

2.1.1 maršrutizatorius, komutatorius, belaidžius prieigos taškus ir ugniasienes;

2.1.2 debesijos virtualiuosius tinklus (pvz., AWS VPC, Azure VNET), VPN koncentratorius ir SD-WAN sistemas;

2.1.3 vidinius LAN, demilitarizuotąsias zonas (DMZ), nuotolinės prieigos kanalus ir tarpobjektinius arba trečiųjų šalių ryšius;

2.1.4 pagalbines sistemas, tokias kaip DNS, DHCP, tarpiniai serveriai ir stebėsenos įrenginiai.

2.2 Politika yra privaloma visam personalui ir trečiųjų šalių paslaugų teikėjams, kurie valdo, konfigūruoja, stebi organizacijos tinklus ar turi su jais sąsają, nepriklausomai nuo to, ar jie yra vietiniai, ar debesijoje.

2.3 Visos sistemos ir taikomosios programos, prijungtos prie organizacijos tinklų, nepriklausomai nuo jų buvimo vietos ar nuosavybės, privalo atitikti šiuos tinklo saugumo reikalavimus.

3. Tikslai

3.1 Užtikrinti per tinklus perduodamų duomenų konfidencialumą, vientisumą ir prieinamumą taikant stiprią prieigos kontrolę, saugų maršruto parinkimą ir stebėseną.

3.2 Užkirsti kelią neteisėtai prieigai, šoniniam judėjimui tinkle ir tinklo išteklių išnaudojimui, taikant segmentavimą, zonavimą ir perimetro apsaugą.

3.3 Palaikyti nuoseklias tinklo konfigūracijas, pagrįstas pramonės gerąja praktika ir grėsmių žvalgyba, siekiant apsisaugoti nuo kintančių kibernetinių grėsmių.

3.4 Apsaugoti išorinę komunikaciją, debesijos tarpusavio jungtis ir nuotolinę prieigą, naudojant šifruotus kanalus, griežtą autentifikavimą ir galinių įrenginių atitikties tikrinimą.

3.5 Užtikrinti tinklo veiklos matomumą taikant centralizuotą žurnalų tvarkymą, realiojo laiko srauto analizę ir automatizuotą įspėjimų generavimą.

3.6 Užtikrinti atitiktį reglamentavimo reikalavimams, suderinant visas tinklo operacijas su ISO/IEC 27001:2022, ES BDAR, NIS2 direktyvos, DORA reglamento ir COBIT 2019 reikalavimais.

4. Vaidmenys ir atsakomybės

4.1 Vyriausiasis informacijos saugumo pareigūnas

4.1.1 Atsako už šią politiką ir užtikrina jos peržiūrą bei suderinimą su platesne organizacijos kibernetinio saugumo strategija.

4.1.2 Tvirtina tinklo segmentavimo modelius, jautrioms sistemoms taikomus ugniasienių taisyklių rinkinius ir išimčių prašymus.

4.2 Tinklo saugumo vadovas / infrastruktūros saugumo vadovas

4.2.1 Valdo tinklo apsaugos architektūrą, įskaitant ugniasienes, įsilaužimų aptikimo ir prevencijos sistemas (IDS/IPS), VPN ir saugų maršruto parinkimą.

4.2.2 Prižiūri tinklo segmentavimą, VLAN priskyrimą, srauto zonavimą ir išorinį junglumą.

4.2.3 Užtikrina nuolatinę įeinančio ir išeinančio srauto filtravimo peržiūrą bei nulinio pasitikėjimo modelio taikymą skirtinguose tinklo sluoksniuose.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Šią politiką kasmet turi peržiūrėti tinklo saugumo vadovas kartu su Vyriausiuoju informacijos saugumo pareigūnu ir atnaujinti atsižvelgiant į:

9.1.1 naujai kylančias grėsmes (pvz., naujus atakų būdus, protokolų pažeidžiamumus);

9.1.2 infrastruktūros pokyčius (pvz., migraciją į debesiją, SD-WAN diegimą);

9.1.3 reglamentavimo arba standartų pakeitimus, darančius poveikį tinklo apsaugai;

9.1.4 audito išvadas, incidentų tendencijas arba kontrolės priemonių sukeltą veikimo pablogėjimą.

9.2 Peržiūros taip pat turi būti inicijuojamos dėl:

9.2.1 esminių tinklo architektūros pakeitimų;

9.2.2 naujų ugniasienių, VPN ar debesijos tinklo platformų įdiegimo;

9.2.3 pagrindinių išteklių ar patikimų zonų eksploatacijos nutraukimo.

9.3 Atnaujinimai turi būti registruojami ISVS dokumentų kontrolės registre ir perduodami:

9.3.1 infrastruktūros ir tinklo operacijų komandoms;

9.3.2 SOC ir saugumo inžinerijos komandoms;

9.3.3 taikomųjų programų komandoms, kurių sistemos priklauso nuo tinklo srautų;

9.3.4 visiems trečiųjų šalių tiekėjams, turintiems aktyvų tarpusavio junglumą.

9.4 Visos ankstesnės politikos versijos turi būti saugiai archyvuojamos su pakeitimų istorijos žymomis, siekiant išlaikyti auditabilumą ir pakeitimų atsekamumą.

10. Susijusios politikos ir sąsajos

10.1 P1 - Informacijos saugumo politika. Nustato pagrindinius saugumo principus ir numato sluoksniuotas apsaugos priemones, įskaitant tinklu grindžiamą prieigos valdymą ir apsaugą nuo grėsmių.

10.2 P4 - Prieigos kontrolės politika. Užtikrina, kad tinklo segmentavimas būtų taikomas pagal naudotojų vaidmenis, mažiausių privilegijų principą ir naudotojų prieigos suteikimo taisykles.

10.3 P5 - Pakeitimų valdymo politika. Reguliuoja ugniasienių pakeitimus, VPN taisyklių koregavimą ir maršruto parinkimo pakeitimus per dokumentuotą ir audituojamą procesą.

10.4 P12 - Turto valdymo politika. Padeda identifikuoti ir klasifikuoti tinkluose veikiančias sistemas bei užtikrina, kad visi prijungti ištekliai būtų valdomi pagal politikoje apibrėžtą taikymo sritį.

10.5 P22 - Žurnalų tvarkymo ir stebėsenos politika. Nustato tinklo žurnalų, įskaitant ugniasienių įvykius, prieigos bandymus ir anomalijų aptikimą, rinkimo, koreliavimo ir saugojimo tvarką.

10.6 P30 - Reagavimo į incidentus politika. Nustato eskalavimo, lokalizavimo ir pašalinimo procedūras reaguojant į per tinklą plintančias grėsmes ar įsibrovimus, tokius kaip DDoS, šoninis judėjimas tinkle ar neteisėta prieiga.

11. Pamatiniai standartai ir sistemos

11.1 Ši politika suderinta su tarptautiniais standartais ir reglamentavimo reikalavimais, apibrėžiančiais saugias tinklo operacijas, segmentavimą, perimetro apsaugą ir saugią nuotolinę prieigą.

11.2 ISO/IEC 27001

11.2.1 8 skyrius - operacinis planavimas ir kontrolė: reikalauja, kad techninės kontrolės priemonės, įskaitant tinklo apsaugos priemones, būtų integruotos į operacinius procesus.

11.3 ISO/IEC 27002:2022

11.3.1 8.20-8.22 kontrolės priemonės. Pateikia gaires dėl tinklų apsaugos, paslaugų segmentavimo ir tinklo paslaugų apsaugos taikant prieigos kontrolę ir stebėseną.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - perimetro apsauga: reikalauja perimetro kontrolės priemonių, segmentavimo ir saugių tarpusavio sujungimų.

11.4.2 AC-4 - informacijos srautų valdymas: palaiko zonavimą ir taisyklėmis grindžiamus srauto apribojimus.

11.4.3 SC-32 - informacinių sistemų skaidymas: skatina loginį informacinių sistemų atskyrimą.

11.5 ES BDAR (2016/679)

11.5.1 32 straipsnis - tvarkymo saugumas: reikalauja techninių priemonių, tokių kaip ugniasienės ir segmentavimas, asmens duomenims apsaugoti.

11.6 ES NIS2 direktyva (2022/2555)

11.6.1 21 straipsnio 2 dalies d punktas: reikalauja veiksmingos tinklų ir informacinių sistemų saugos, perimetro apsaugos, saugios konfigūracijos ir atskyrimo kontrolės priemonių.

11.7 ES DORA reglamentas (2022/2554)

11.7.1 9 straipsnis - IRT rizikos valdymas: įpareigoja finansų subjektus apsaugoti tinklus ir tarpusavio jungtis nuo neteisėtos prieigos, duomenų nutekėjimo ir veiklos sutrikdymo.

11.8 COBIT 2019

11.8.1 DSS01.03 - infrastruktūros stebėsena: reikalauja aktyvios tinklo būklės ir junglumo kontrolės.

11.8.2 DSS05.01 - apsauga nuo kenkėjiškos programinės įrangos: apima segmentavimą ir perimetro kontrolę, siekiant sumažinti plitimą.

11.8.3 MEA03 - atitikties stebėsena, vertinimas ir įvertinimas: sustiprina tinklo politikos taikymą ir atitikties vertinimus.