					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P21					Dokumenta nosaukums: **Tīkla drošības politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņošana ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	N/A
ISO/IEC 27002:2022	Kontroles pasākumi 8.20-8.22	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
ES VDAR	32. pants	N/A
ES NIS2	21. panta 2. punkta d) apakšpunkts	N/A
ES DORA	9. pants	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Mērķis

1.1 Šīs politikas mērķis ir noteikt organizācijas prasības tās iekšējo un ārējo tīklu aizsardzībai pret nesankcionētu piekļuvi, pakalpojumu darbības traucējumiem, datu pārtveršanu un neatbilstošu izmantošanu.

1.2 Tā nodrošina, ka visa tīkla infrastruktūra, tostarp fiziskā, virtuālā, mākoņvides un hibrīdā infrastruktūra, ir aizsargāta ar slāņveida kontroles pasākumiem, piemēram, segmentēšanu, ugunsmūra noteikumu piemērošanu, drošu maršrutēšanu un centralizētu uzraudzību.

1.3 Šī politika nosaka ISO/IEC 27001 8. punkta un ISO/IEC 27002:2022 kontroles pasākumu 8.20 līdz 8.22 ieviešanu, nodrošinot atbilstību piemērojamajām tiesiskajām un regulatīvajām prasībām saskaņā ar VDAR 32. pantu, NIS2 21. pantu un DORA 9. pantu.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem tīkliem un saistītajiem infrastruktūras komponentiem, tostarp:

2.1.1 maršrutētājiem, komutatoriem, bezvadu piekļuves punktiem un ugunsmūriem;

2.1.2 mākoņvides virtuālajiem tīkliem (piemēram, AWS VPC, Azure VNet), VPN koncentratoriem un SD-WAN sistēmām;

2.1.3 iekšējiem LAN, demilitarizētajām zonām (DMZ), attālinātās piekļuves ceļiem un starpvietņu vai trešo pušu savienojumiem;

2.1.4 atbalsta sistēmām, piemēram, DNS, DHCP, starpniekserveriem un uzraudzības risinājumiem.

2.2 Politika ir saistoša visiem darbiniekiem un trešo pušu pakalpojumu sniedzējiem, kuri pārvalda, konfigurē, uzrauga organizācijas tīklus vai mijiedarbojas ar tiem neatkarīgi no tā, vai tie atrodas lokāli vai mākoņvidē.

2.3 Visām sistēmām un lietojumprogrammām, kas ir pieslēgtas organizācijas tīkliem, neatkarīgi no to atrašanās vietas vai īpašumtiesībām, jāatbilst šīm tīkla drošības prasībām.

3. Mērķi

3.1 Nodrošināt tīklos pārsūtīto datu konfidencialitāti, integritāti un pieejamību (CIA), izmantojot stingru piekļuves kontroli, drošu maršrutēšanu un uzraudzību.

3.2 Novērst nesankcionētu piekļuvi, sānu pārvietošanos un tīklā pieejamo resursu neatļautu izmantošanu, ieviešot segmentēšanu, zonējumu un perimetra aizsardzību.

3.3 Uzturēt konsekventas tīkla konfigurācijas, kas balstītas nozares standartos un draudu izlūkošanas datos, lai aizsargātos pret mainīgiem kiberdraudiem.

3.4 Aizsargāt ārējo saziņu, mākoņsavienojamību un attālināto piekļuvi, izmantojot šifrētus kanālus, stingru autentifikāciju un galiekārtu validāciju.

3.5 Nodrošināt pārskatāmību par tīkla darbību, izmantojot centralizētu žurnālfiksēšanu, datplūsmas pārbaudi reāllaikā un automātiskus brīdinājumus.

3.6 Nodrošināt regulatīvo atbilstību, saskaņojot visas tīkla darbības ar ISO/IEC 27001:2022, VDAR, NIS2, DORA un COBIT 2019 prasībām.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO)

4.1.1 Ir šīs politikas īpašnieks un nodrošina tās pārskatīšanu un saskaņotību ar organizācijas kopējo kiberdrošības stratēģiju.

4.1.2 Apstiprina tīkla segmentēšanas modeļus, ugunsmūra noteikumu kopas sensitīvām sistēmām un izņēmumu pieprasījumus.

4.2 Tīkla drošības vadītājs / infrastruktūras drošības vadītājs

4.2.1 Pārvalda tīkla aizsardzības arhitektūru, tostarp ugunsmūrus, ielaušanās atklāšanas un novēršanas sistēmas (IDS/IPS), VPN un drošu maršrutēšanu.

4.2.2 Pārrauga tīkla segmentēšanu, VLAN piešķīrumus, datplūsmas zonējumu un ārējo savienojamību.

4.2.3 Nodrošina nepārtrauktu ienākošās un izejošās datplūsmas filtrēšanas pārskatīšanu un nulles uzticēšanās principa piemērošanu visos tīkla līmeņos.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika tīkla drošības vadītājam sadarbībā ar CISO jāpārskata reizi gadā un jāatjaunina, pamatojoties uz:

9.1.1 jauniem riskiem (piemēram, jaunām uzbrukumu metodēm, protokolu ievainojamībām);

9.1.2 infrastruktūras izmaiņām (piemēram, migrāciju uz mākoņvidi, SD-WAN ieviešanu);

9.1.3 regulatīvajiem vai standartu atjauninājumiem, kas ietekmē tīkla aizsardzību;

9.1.4 audita konstatējumiem, incidentu tendencēm vai kontroles pasākumu izraisītu veiktspējas pasliktināšanos.

9.2 Pārskatīšana jāierosina arī šādos gadījumos:

9.2.1 būtiskas izmaiņas tīkla arhitektūrā;

9.2.2 jaunu ugunsmūra, VPN vai mākoņtīkla platformu ieviešana;

9.2.3 galveno aktīvu vai uzticamo zonu izņemšana no ekspluatācijas.

9.3 Atjauninājumi jāreģistrē ISMS dokumentu kontroles reģistrā un jāizplata:

9.3.1 infrastruktūras un tīkla operāciju funkcijai;

9.3.2 SOC un drošības inženierijas komandām;

9.3.3 lietojumprogrammu komandām, kuru sistēmas ir atkarīgas no tīkla plūsmām;

9.3.4 visiem trešo pušu piegādātājiem ar aktīvu savienojamību.

9.4 Visas iepriekšējās politikas versijas droši jāarhivē ar izmaiņu vēstures piezīmēm, lai saglabātu auditējamību un izmaiņu izsekojamību.

10. Saistītās politikas un sasaiste

10.1 P1 - Informācijas drošības politika. Nosaka drošības pamatprincipus un paredz slāņveida aizsardzību, tostarp uz tīklu balstītus piekļuves un apdraudējumu kontroles pasākumus.

10.2 P4 - Piekļuves kontroles politika. Nodrošina, ka tīkla segmentēšana tiek piemērota atbilstoši lietotāju lomām, minimālo privilēģiju principam un piekļuves tiesību piešķiršanas noteikumiem.

10.3 P5 - Izmaiņu pārvaldības politika. Regulē ugunsmūra izmaiņas, VPN noteikumu pielāgojumus un maršrutēšanas izmaiņas, izmantojot dokumentētu un auditējamu procesu.

10.4 P12 - Aktīvu pārvaldības politika. Atbalsta tīklam pieslēgto sistēmu identificēšanu un klasificēšanu un nodrošina, ka visi pieslēgtie aktīvi tiek pārvaldīti atbilstoši politikā noteiktajai piemērošanas jomai.

10.5 P22 - Žurnālfiksēšanas un uzraudzības politika. Regulē tīkla žurnālu, tostarp ugunsmūra notikumu, piekļuves mēģinājumu un anomāliju noteikšanas notikumu, vākšanu, korelāciju un glabāšanu.

10.6 P30 - Incidentu reaģēšanas politika. Nosaka eskalācijas, ierobežošanas un izskaušanas procedūras, reaģējot uz tīklā izplatītiem apdraudējumiem vai ielaušanos, piemēram, DDoS, sānu pārvietošanos vai nesankcionētu piekļuvi.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiskajiem standartiem un regulatīvajām prasībām, kas nosaka drošas tīkla operācijas, segmentēšanu, perimetra aizsardzību un drošu attālināto piekļuvi.

11.2 ISO/IEC 27001

11.2.1 8. punkts - darbības plānošana un kontrole: paredz, ka tehniskie kontroles pasākumi, tostarp tīkla aizsardzības pasākumi, jāintegrē darbības procesos.

11.3 ISO/IEC 27002:2022

11.3.1 Kontroles pasākumi 8.20-8.22. Sniedz norādes par tīklu aizsardzību, pakalpojumu segmentēšanu un tīkla pakalpojumu aizsardzību, izmantojot piekļuves kontroles pasākumus un uzraudzību.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - perimetra aizsardzība: paredz perimetra kontroles pasākumus, segmentēšanu un drošus starpsavienojumus.

11.4.2 AC-4 - informācijas plūsmas kontrole: atbalsta zonējumu un uz noteikumiem balstītus datplūsmas ierobežojumus.

11.4.3 SC-32 - informācijas sistēmu nodalīšana: veicina informācijas sistēmu loģisku nodalīšanu.

11.5 ES VDAR (2016/679)

11.5.1 32. pants - apstrādes drošība: nosaka tehniskos pasākumus, piemēram, ugunsmūrus un segmentēšanu, personas datu aizsardzībai.

11.6 ES NIS2 direktīva (2022/2555)

11.6.1 21. panta 2. punkta d) apakšpunkts: nosaka prasību nodrošināt efektīvu tīklu un informācijas sistēmu drošību, perimetra aizsardzību, drošu konfigurāciju un nodalīšanas kontroles pasākumus.

11.7 ES DORA (2022/2554)

11.7.1 9. pants - IKT risku pārvaldība: uzliek pienākumu finanšu struktūrām aizsargāt tīklus un starpsavienojumus pret nesankcionētu piekļuvi, datu noplūdēm un darbības traucējumiem.

11.8 COBIT 2019

11.8.1 DSS01.03 - infrastruktūras uzraudzība: nosaka proaktīvu kontroli pār tīkla darbspēju un savienojamību.

11.8.2 DSS05.01 - aizsardzība pret ļaunatūru: ietver segmentēšanu un perimetra kontroli, lai mazinātu izplatīšanos.

11.8.3 MEA03 - atbilstības uzraudzība, izvērtēšana un novērtēšana: stiprina tīkla politikas ievērošanu un atbilstības izvērtēšanu.