					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P21S					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**

Saskaņotība ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	-
ISO/IEC 27002:2022	8. kontrole	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
ES GDPR	32. pants	-
ES NIS2	21(2)(d), (e) pants	-
ES DORA	9., 10. pants	-
COBIT 2019	DSS05.02, APO13	-

1. Mērķis

1.1. Šīs politikas mērķis ir nodrošināt, ka visa iekšējā un ārējā tīkla komunikācija ir aizsargāta pret nesankcionētu piekļuvi, manipulācijām, noklausīšanos un neatbilstošu izmantošanu, ieviešot skaidri noteiktus drošības kontroles pasākumus.

1.2. Tā nosaka prasības tīkla infrastruktūras drošai projektēšanai, izmantošanai un pārvaldībai, tostarp attiecībā uz maršrutētājiem, bezvadu piekļuves punktiem, attālās piekļuves savienojumiem un segmentētiem tīkliem.

1.3. Tās mērķis ir mazināt pakļautību internetā balstītiem apdraudējumiem, nodrošināt pa iekšējiem un ārējiem tīkliem pārsūtīto datu konfidencialitāti un uzturēt kritiskos pakalpojumus pieejamus.

1.4. Šī politika atbalsta ISO/IEC 27001:2022 sertifikāciju un tieši veicina GDPR, NIS2 un DORA noteikto tiesisko un regulatīvo pienākumu izpildi, vienlaikus nodrošinot tehnisku apliecinājumu klientiem un auditoriem.

2. Piemērošanas joma

2.1. Šī politika attiecas uz visām organizācijas IT tīkla komponentēm, tostarp:

2.1.1. vadu un bezvadu infrastruktūru biroja lokācijās;

2.1.2. maršrutētājiem, komutatoriem, piekļuves punktiem, ugunsmūriem un vārtejām;

2.1.3. attālās piekļuves savienojumiem, tostarp VPN, RDP un mākoņtuneļiem;

2.1.4. mākoņpakalpojumos balstītām lietotnēm, kurām piekļūst no iekšējiem vai ārējiem tīkliem;

2.1.5. ierīcēm, ko tīklam pieslēdz darbinieki, līgumslēdzēji vai viesi.

2.2. Šī politika reglamentē gan fiziskos, gan loģiskos tīkla segmentus, tostarp viesu zonas, IoT ierīces un biroja iekšējās sistēmas.

2.3. Politika attiecas uz visu personālu, kam ir piekļuve organizācijas tīklam, tostarp:

2.3.1. iekšējiem darbiniekiem;

2.3.2. attālinātā darba veicējiem un hibrīddarba personālam;

2.3.3. ārējiem piegādātājiem, konsultantiem un pakalpojumu sniedzējiem;

2.3.4. viesiem ar pagaidu Wi-Fi piekļuvi.

3. Mērķi

3.1. Nodrošināt, ka organizācijas tīkls ir aizsargāts pret nesankcionētu piekļuvi un ārējiem kiberdraudiem.

3.2. Nodrošināt pienācīgu segmentēšanu starp uzticamiem un neuzticamiem tīkliem, piemēram, viesu Wi-Fi un piegādātāju piekļuvi.

3.3. Nodrošināt drošu attālināto savienojamību, neapdraudot iekšējās sistēmas.

3.4. Novērst ļaunprogrammatūras izplatīšanos un datu neatļautu iznesi tīkla kanālos.

3.5. Nodrošināt tīkla darbības uzraudzību, brīdināšanu un auditējamību, lai atbalstītu incidentu atklāšanu un atbilstību.

3.6. Nodrošināt, ka iekšējiem tīkliem drīkst pieslēgties tikai apstiprinātas un aizsargātas ierīces.

3.7. Izpildīt ISO 27001, GDPR un saistīto kiberdrošības ietvaru prasības.

4. Lomas un atbildība

4.1. Ģenerāldirektors

4.1.1. Ir šīs politikas īpašnieks un nodrošina, ka drošai tīkla projektēšanai un pārvaldībai tiek piešķirti atbilstoši resursi.

4.1.2. Izvērtē izņēmumus no tīkla drošības kontroles pasākumiem un apstiprina piegādātāju tīkla piekļuves vienošanās.

4.1.3. Izskata incidentus vai audita konstatējumus, kas saistīti ar tīkla drošības ievainojamībām.

4.2. IT atbalsta pakalpojumu sniedzējs / iekšējā IT funkcija

4.2.1. Ievieš, konfigurē un uztur visus ugunsmūrus, maršrutētājus, komutatorus un bezvadu kontrolierus.

4.2.2. Pārvalda segmentēšanu starp iekšējiem, viesu un ārējiem tīkliem.

4.2.3. Uzrauga žurnālus un brīdinājumus par nesankcionētas piekļuves mēģinājumiem vai tīkla anomālijām.

4.2.4. Nodrošina, ka aparātprogrammatūras un konfigurācijas atjauninājumi tiek ieviesti droši un savlaicīgi.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Ikgadējā pārskatīšana

9.1.1. Šī politika jāpārskata vismaz reizi gadā ģenerāldirektoram kopā ar IT atbalsta pakalpojumu sniedzēju un privātuma koordinatoru.

9.2. Starpposma pārskatīšanas ierosinātāji

9.2.1. Politikas pārskatīšana jāierosina arī šādos gadījumos:

9.2.1.1. būtiskas izmaiņas tīkla arhitektūrā, piemēram, jaunas VPN vai ugunsmūra sistēmas;

9.2.1.2. ar tīklu saistīts incidents, piemēram, ielaušanās, izspiedējprogrammatūras izplatīšanās vai datu neatļauta iznese;

9.2.1.3. tiesiskā, regulatīvā vai ietvaru atjaunināšana, kas ietekmē tīkla aizsardzību;

9.2.1.4. jaunas piegādātāju platformas, kurām nepieciešamas alternatīvas piekļuves metodes vai protokoli.

9.3. Versiju pārvaldība un dokumentēšana

9.3.1. Politikas pārskatījumi jāreģistrē ar versijas numuru, datumu un izmaiņu kopsavilkumu.

9.3.2. Iepriekšējās versijas jāarhivē vismaz 3 gadus.

9.3.3. Par atjauninājumiem jāpaziņo ietekmētajiem darbiniekiem, un, ja tiek ieviestas būtiskas uzvedības izmaiņas, jāsaņem obligāts apliecinājums.

10. Saistītās politikas un sasaiste

10.1. Šī politika jāievieš kopā ar šādām MVU drošības politikām:

10.1.1. P9S – Attālinātā darba politika: nosaka drošas attālās piekļuves metodes, VPN prasības un galiekārtu aizsardzību lietotājiem ārpus organizācijas telpām.

10.1.2. P12S – Aktīvu pārvaldības politika: nodrošina, ka visas tīklam pieslēgtās sistēmas ir identificētas, klasificētas un uzskaitītas ar aktuālu drošības statusu.

10.1.3. P17S – Datu aizsardzības un privātuma politika: nodrošina, ka tīkla segmentēšana, piekļuves kontroles pasākumi un žurnālfiksēšana atbalsta GDPR noteiktos privātuma un datu aizsardzības principus.

10.1.4. P22S – Žurnālfiksēšanas un uzraudzības politika: nosaka prasības žurnālu iegūšanai un pārskatīšanai no tīkla ierīcēm, attālajiem savienojumiem un bezvadu kontrolieriem.

10.1.5. P30S – Incidentu reaģēšanas politika: nosaka nepieciešamās darbības, reaģējot uz tīkla pārkāpumiem, nesankcionētas piekļuves mēģinājumiem vai ļaunprogrammatūras izplatīšanos iekšējos tīklos.

11. Atsauces standarti un ietvari

11.1. ISO/IEC 27001

11.1.1. 8. punkts – nosaka prasību ieviest kontroles pasākumus drošas un noturīgas darbības nodrošināšanai, tostarp attiecībā uz tīkliem.

11.2. ISO/IEC 27002

11.2.1. Kontrole 8.20 – sniedz tehniskas un procesuālas vadlīnijas tīkla piekļuves, segmentēšanas un uzraudzības aizsardzībai.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – nosaka prasību kontrolēt informācijas plūsmu tīklos un starp sistēmām.

11.3.2. SC-7 – nosaka prasību īstenot robežapsardzību, drošu maršrutēšanu un tīkla segmentēšanu, lai mazinātu nesankcionētas piekļuves risku.

11.4. ES GDPR

11.4.1. 32. pants – nosaka pienākumu īstenot atbilstošus tehniskos un organizatoriskos pasākumus, lai nodrošinātu personas datus apstrādājošu tīklotu sistēmu un pakalpojumu konfidencialitāti, integritāti un pieejamību.

11.5. ES NIS2 direktīva

11.5.1. 21(2)(d) pants – nosaka uz risku balstītus tehniskos pasākumus, tostarp tīkla drošību un piekļuves kontroli.

11.5.2. 21(2)(e) pants – nosaka sistēmu segmentēšanu un izolāciju, lai novērstu kiberdrošības incidentu izplatīšanos.

11.6. ES DORA

11.6.1. 9. pants – nosaka prasību organizācijām ieviest IKT risku pārvaldības kontroles pasākumus, tostarp drošiem tīkliem un sakariem.

11.6.2. 10. pants – nosaka, ka digitālās noturības stratēģijām jāaptver tīkla infrastruktūras un attālās savienojamības aizsardzība.

11.7. COBIT 2019

11.7.1. DSS05.02 – nosaka prasību efektīvi aizsargāt IT infrastruktūru un tīkla vidi pret iekšējiem un ārējiem apdraudējumiem.

11.7.2. APO13.01 – nosaka prasību risku pārvaldības stratēģijās iekļaut tīkla segmentēšanu un uzraudzību kā daļu no apdraudējumu mazināšanas.