					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P21					Naslov dokumenta: **Politika varnosti omrežij**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
ISO/IEC 27001:2022	Klavzula 8	N/A
ISO/IEC 27002:2022	Kontrole 8.20–8.22	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
Uredba EU GDPR	Člen 32	N/A
Direktiva EU NIS2	Člen 21(2)(d)	N/A
Uredba EU DORA	Člen 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Namen

1.1 Namen te politike je opredeliti zahteve organizacije za zaščito njenih notranjih in zunanjih omrežij pred nepooblaščenim dostopom, motnjami v delovanju storitev, prestrezanjem podatkov in neustrezno uporabo.

1.2 Ta politika zagotavlja, da je celotna omrežna infrastruktura, vključno s fizično, virtualno, oblačno in hibridno infrastrukturo, zaščitena z večplastnimi kontrolami, kot so segmentacija, uveljavljanje pravil požarnih zidov, varno usmerjanje in centralizirano spremljanje.

1.3 Ta politika uveljavlja zahteve standarda ISO/IEC 27001, klavzule 8.1, in kontrol iz Priloge A od 8.20 do 8.22 ter zagotavlja skladnost z veljavnimi pravnimi in regulativnimi obveznostmi iz člena 32 GDPR, člena 21 Direktive EU NIS2 in člena 9 Uredbe EU DORA.

2. Področje uporabe

2.1 Ta politika velja za vsa omrežja in povezane infrastrukturne komponente, vključno z:

2.1.1 usmerjevalniki, stikali, brezžičnimi dostopovnimi točkami in požarnimi zidovi,

2.1.2 virtualnimi omrežji v oblaku (npr. AWS VPC, Azure VNet), koncentratorji VPN in sistemi SD-WAN,

2.1.3 internimi lokalnimi omrežji, demilitariziranimi conami (DMZ), potmi za oddaljeni dostop ter povezavami med lokacijami ali s tretjimi osebami,

2.1.4 podpornimi sistemi, kot so DNS, DHCP, posredniški strežniki in naprave za spremljanje.

2.2 Ta politika je zavezujoča za vse zaposlene ter ponudnike storitev tretjih oseb, ki upravljajo, konfigurirajo, spremljajo omrežja organizacije ali se povezujejo z njimi, ne glede na to, ali gre za infrastrukturo v lastnih prostorih ali v oblaku.

2.3 Vsi sistemi in aplikacije, povezani v omrežja organizacije, ne glede na lokacijo ali lastništvo, morajo biti skladni s temi zahtevami za varnost omrežij.

3. Cilji

3.1 Zagotoviti zaupnost, celovitost in razpoložljivost (CIA) podatkov, ki se prenašajo prek omrežij, z močnimi kontrolami dostopa, varnim usmerjanjem in spremljanjem.

3.2 Preprečiti nepooblaščen dostop, lateralno gibanje in zlorabo omrežnih virov z uveljavljanjem segmentacije, coniranja in zaščite omrežnih meja.

3.3 Vzdrževati dosledne omrežne konfiguracije na podlagi panožnih standardov in obveščevalnih podatkov o grožnjah za zaščito pred razvijajočimi se kibernetskimi grožnjami.

3.4 Zaščititi zunanje komunikacije, povezljivost z oblačnimi okolji in oddaljeni dostop z uporabo šifriranih kanalov, stroge avtentikacije in preverjanja končnih točk.

3.5 Zagotoviti vidnost omrežnih dejavnosti s centraliziranim beleženjem dnevniških zapisov, pregledovanjem omrežnega prometa v realnem času in samodejnim opozarjanjem.

3.6 Zagotoviti skladnost s predpisi z uskladitvijo vseh omrežnih operacij z zahtevami standarda ISO/IEC 27001:2022, GDPR, NIS2, DORA in COBIT 2019.

4. Vloge in odgovornosti

4.1 Vodja informacijske varnosti (CISO)

4.1.1 Je skrbnik te politike ter zagotavlja njen pregled in usklajenost s širšo strategijo kibernetske varnosti organizacije.

4.1.2 Odobri modele segmentacije omrežja, nabore pravil požarnih zidov za občutljive sisteme in zahteve za izjeme.

4.2 Vodja varnosti omrežij / vodja varnosti infrastrukture

4.2.1 Upravlja arhitekturo zaščite omrežja, vključno s požarnimi zidovi, sistemi za zaznavanje in preprečevanje vdorov (IDS/IPS), VPN in varnim usmerjanjem.

4.2.2 Nadzira segmentacijo omrežja, dodeljevanje omrežij VLAN, coniranje prometa in zunanjo povezljivost.

4.2.3 Zagotavlja neprekinjen nadzor filtriranja vhodnega in izhodnega prometa ter uveljavljanje načela ničelnega zaupanja med omrežnimi ravnmi.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Zahteve za pregled in posodobitev

9.1 To politiko mora vodja varnosti omrežij letno pregledati v sodelovanju z vodjo informacijske varnosti (CISO) ter jo posodobiti na podlagi:

9.1.1 nastajajočih groženj (npr. novih tehnik napadov, ranljivosti protokolov),

9.1.2 sprememb infrastrukture (npr. migracije sistemov v oblak, uvedbe SD-WAN),

9.1.3 regulativnih ali standardizacijskih posodobitev, ki vplivajo na zaščito omrežij,

9.1.4 ugotovitev presoje, trendov incidentov ali zmanjšanja učinkovitosti zaradi uvedenih kontrol.

9.2 Pregled se mora sprožiti tudi ob:

9.2.1 večjih spremembah arhitekture omrežja,

9.2.2 uvedbi novih platform za požarne zidove, VPN ali oblačna omrežja,

9.2.3 izločitvi ključnih sredstev ali zaupanja vrednih con iz uporabe.

9.3 Posodobitve morajo biti zabeležene v registru dokumentacije ISMS in posredovane:

9.3.1 ekipam za infrastrukturo in omrežne operacije,

9.3.2 ekipam SOC in varnostnega inženiringa,

9.3.3 aplikacijskim ekipam z odvisnostmi od omrežnih tokov,

9.3.4 vsem dobaviteljem tretjih oseb z aktivno medsebojno povezljivostjo.

9.4 Vse predhodne različice politike morajo biti varno arhivirane z opombami o zgodovini sprememb, da se ohranita revizijska preverljivost in sledljivost sprememb.

10. Povezane politike in povezave

10.1 P1 - Politika informacijske varnosti. Določa temeljna varnostna načela in zahteva večplastno zaščito, vključno z omrežnimi kontrolami dostopa in zaščite pred grožnjami.

10.2 P4 - Politika nadzora dostopa. Zagotavlja, da se segmentacija omrežja uveljavlja skladno z vlogami uporabnikov, načelom najmanjših privilegijev in pravili za dodelitev dostopa.

10.3 P5 - Politika upravljanja sprememb. Ureja spremembe požarnih zidov, prilagoditve pravil VPN in spremembe usmerjanja prek dokumentiranega procesa, primernega za revizijo.

10.4 P12 - Politika upravljanja sredstev. Podpira identifikacijo in razvrstitev omrežno povezanih sistemov ter zagotavlja, da so vsa povezana sredstva upravljana v okviru področij uporabe, opredeljenih s politikami.

10.5 P22 - Politika beleženja in spremljanja. Ureja zbiranje, korelacijo in hrambo omrežnih dnevniških zapisov, vključno z dogodki požarnih zidov, poskusi dostopa in zaznanimi anomalijami.

10.6 P30 - Politika odzivanja na incidente. Opredeljuje postopke eskalacije, zajezitve in odstranjevanja groženj kot odziv na omrežno prenosljive grožnje ali vdore, kot so DDoS, lateralno gibanje ali nepooblaščen dostop.

11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z mednarodnimi standardi in regulativnimi zahtevami, ki opredeljujejo varne omrežne operacije, segmentacijo, zaščito omrežnih meja in varen oddaljeni dostop.

11.2 ISO/IEC 27001

11.2.1 Klavzula 8.1 - Operativno načrtovanje in nadzor: zahteva, da so tehnične kontrole, vključno z zaščitnimi ukrepi za omrežja, vključene v operativne procese.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrole 8.20-8.22: podajajo usmeritve za zaščito omrežij, segmentacijo storitev in varovanje omrežnih storitev s kontrolami dostopa in spremljanjem.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - zaščita omrežnih meja: zahteva perimetrske kontrole, segmentacijo in varne medsebojne povezave.

11.4.2 AC-4 - uveljavljanje pravil pretoka informacij: podpira coniranje in omejitve prometa na podlagi pravil.

11.4.3 SC-32 - razdelitev informacijskih sistemov: spodbuja logično ločevanje informacijskih sistemov.

11.5 Uredba EU GDPR (2016/679)

11.5.1 Člen 32 - varnost obdelave: zahteva tehnične ukrepe, kot so požarni zidovi in segmentacija, za zaščito osebnih podatkov.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Člen 21(2)(d): zahteva učinkovito varnost omrežnih in informacijskih sistemov, zaščito omrežnih meja, varno konfiguracijo in kontrole ločevanja.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Člen 9 - upravljanje tveganj IKT: finančnim subjektom nalaga zaščito omrežij in medsebojnih povezav pred nepooblaščenim dostopom, uhajanjem podatkov in operativnimi motnjami.

11.8 COBIT 2019

11.8.1 DSS01.03 - spremljanje infrastrukture: zahteva proaktiven nadzor nad stanjem omrežja in povezljivostjo.

11.8.2 DSS05.01 - zaščita pred zlonamerno programsko opremo: vključuje segmentacijo in nadzor omrežnih meja za zmanjšanje širjenja.

11.8.3 MEA03 - spremljanje, vrednotenje in presoja skladnosti: krepi izvajanje omrežne politike in presoje skladnosti.