					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P21					Naziv dokumenta: **Politika mrežne sigurnosti**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	Nije primjenjivo
ISO/IEC 27002:2022	Kontrole 8.20-8.22	Nije primjenjivo
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	Nije primjenjivo
GDPR EU	Članak 32	Nije primjenjivo
Direktiva EU NIS2	Članak 21(2)(d)	Nije primjenjivo
Uredba EU DORA	Članak 9	Nije primjenjivo
COBIT 2019	DSS01.03, DSS05.01, MEA03	Nije primjenjivo

1. Svrha

1.1 Svrha ove politike jest utvrditi zahtjeve organizacije za zaštitu internih i vanjskih mreža od neovlaštenog pristupa, prekida usluga, presretanja podataka i zlouporabe.

1.2 Ova politika osigurava da je cjelokupna mrežna infrastruktura, uključujući fizička, virtualna, oblačna i hibridna okruženja, zaštićena slojevitim kontrolama kao što su segmentacija, provedba pravila vatrozida, sigurno usmjeravanje i centralizirano praćenje.

1.3 Ova politika provodi zahtjeve norme ISO/IEC 27001 iz točke 8.1 i kontrola iz Dodatka A 8.20 do 8.22 te osigurava usklađenost s primjenjivim zakonskim i regulatornim obvezama iz članka 32 GDPR-a, članka 21 Direktive NIS2 i članka 9 Uredbe DORA.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve mreže i povezane infrastrukturne komponente, uključujući:

2.1.1 usmjernike, preklopnike, bežične pristupne točke i vatrozide

2.1.2 virtualne mreže u oblaku (npr. AWS VPC, Azure VNet), VPN koncentratore i SD-WAN sustave

2.1.3 interne LAN mreže, demilitarizirane zone (DMZ), putove za udaljeni pristup te međulokacijske veze i veze s trećim stranama

2.1.4 potporne sustave kao što su DNS, DHCP, proxy poslužitelji i uređaji za praćenje

2.2 Ova politika obvezujuća je za svo osoblje i pružatelje usluga trećih strana koji upravljaju mrežama organizacije, konfiguriraju ih, nadziru ili se na njih povezuju, bilo u vlastitim prostorijama ili u oblaku.

2.3 Svi sustavi i aplikacije povezani s mrežama organizacije, neovisno o lokaciji ili vlasništvu, moraju biti usklađeni s ovim zahtjevima mrežne sigurnosti.

3. Ciljevi

3.1 Osigurati povjerljivost, cjelovitost i dostupnost podataka koji se prenose mrežama primjenom snažnih kontrola pristupa, sigurnog usmjeravanja i praćenja.

3.2 Spriječiti neovlašteni pristup, lateralno kretanje i iskorištavanje mrežno povezanih resursa provedbom segmentacije, zoniranja i zaštite granica sustava.

3.3 Održavati dosljedne mrežne konfiguracije temeljene na industrijskim standardima i obavještajnim podacima o prijetnjama radi obrane od kibernetičkih prijetnji koje se razvijaju.

3.4 Zaštititi vanjsku komunikaciju, povezivost s oblakom i udaljeni pristup uporabom šifriranih kanala, stroge autentifikacije i provjere krajnjih uređaja.

3.5 Osigurati vidljivost mrežnih aktivnosti putem centraliziranog zapisivanja i praćenja, pregleda mrežnog prometa u stvarnom vremenu i automatiziranog upozoravanja.

3.6 Osigurati usklađenost s regulatornim zahtjevima usklađivanjem svih mrežnih operacija sa zahtjevima normi ISO/IEC 27001:2022, GDPR-a, Direktive NIS2, Uredbe DORA i okvira COBIT 2019.

4. Uloge i odgovornosti

4.1 glavni direktor informacijske sigurnosti (CISO)

4.1.1 Vlasnik je ove politike te osigurava njezino preispitivanje i usklađenost sa širom strategijom kibernetičke sigurnosti organizacije.

4.1.2 Odobrava modele mrežne segmentacije, skupove pravila vatrozida za osjetljive sustave i zahtjeve za iznimkama.

4.2 voditelj mrežne sigurnosti / voditelj sigurnosti infrastrukture

4.2.1 Upravlja arhitekturom mrežne obrane, uključujući vatrozide, sustave za otkrivanje i sprječavanje upada (IDS/IPS), VPN i sigurno usmjeravanje.

4.2.2 Nadzire mrežnu segmentaciju, dodjelu VLAN-ova, zoniranje prometa i vanjsku povezivost.

4.2.3 Osigurava kontinuirano preispitivanje filtriranja ulaznog i izlaznog prometa te provedbu modela nultog povjerenja na svim mrežnim razinama.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Pregled i zahtjevi za ažuriranje

9.1 Ovu politiku mora najmanje jednom godišnje preispitati voditelj mrežne sigurnosti u suradnji s glavnim direktorom informacijske sigurnosti (CISO), a mora se ažurirati na temelju:

9.1.1 novih prijetnji (npr. novih tehnika napada, ranjivosti protokola)

9.1.2 promjena infrastrukture (npr. migracije sustava u oblak, uvođenje SD-WAN-a)

9.1.3 regulatornih ili normativnih ažuriranja koja utječu na mrežne zaštite

9.1.4 nalaza revizije, trendova incidenata ili smanjenja učinkovitosti kontrola

9.2 Preispitivanje se mora pokrenuti i u slučaju:

9.2.1 značajnih promjena mrežne arhitekture

9.2.2 uvođenja novih platformi vatrozida, VPN-a ili mrežnih platformi u oblaku

9.2.3 stavljanja izvan uporabe ključne imovine ili pouzdanih zona

9.3 Ažuriranja se moraju evidentirati u registru dokumenata ISMS-a i dostaviti:

9.3.1 timovima za infrastrukturu i mrežne operacije

9.3.2 timu centra sigurnosnih operacija i timovima za sigurnosni inženjering

9.3.3 aplikacijskim timovima čiji sustavi ovise o mrežnim tokovima

9.3.4 svim dobavljačima trećih strana s aktivnom međupovezanošću

9.4 Sve prethodne verzije politike moraju se sigurno arhivirati uz bilješke o povijesti promjena radi očuvanja mogućnosti revizije i sljedivosti promjena.

10. Povezane politike i poveznice

10.1 P1 - Politika informacijske sigurnosti. Uspostavlja temeljna sigurnosna načela i zahtijeva slojevitu zaštitu, uključujući kontrole pristupa i kontrole prijetnji na mrežnoj razini.

10.2 P4 - Politika kontrole pristupa. Osigurava da se mrežna segmentacija provodi u skladu s korisničkim ulogama, načelom najmanjih ovlasti i pravilima dodjele pristupnih prava.

10.3 P5 - Politika upravljanja promjenama. Uređuje izmjene vatrozida, prilagodbe VPN pravila i promjene usmjeravanja kroz dokumentiran i revizijski dokaziv postupak.

10.4 P12 - Politika upravljanja imovinom. Podupire identifikaciju i klasifikaciju sustava povezanih na mrežu te osigurava da se svom povezanom imovinom upravlja u okviru opsega definiranog politikom.

10.5 P22 - Politika bilježenja i praćenja. Uređuje prikupljanje, korelaciju i zadržavanje mrežnih dnevničkih zapisa, uključujući događaje vatrozida, pokušaje pristupa i otkrivanje anomalija.

10.6 P30 - Politika odgovora na incidente. Definira postupke eskalacije, ograničavanja i uklanjanja prijetnji ili upada koji se prenose mrežom, kao što su DDoS, lateralno kretanje ili neovlašteni pristup.

11. Referentni standardi i okviri

11.1 Ova politika usklađena je s međunarodnim standardima i regulatornim zahtjevima koji uređuju sigurno upravljanje mrežama, segmentaciju, perimetarsku zaštitu i siguran udaljeni pristup.

11.2 ISO/IEC 27001

11.2.1 Točka 8.1 - Operativno planiranje i kontrola: zahtijeva da tehničke kontrole, uključujući mrežne zaštitne mjere, budu ugrađene u operativne procese.

11.3 ISO/IEC 27002:2022

11.3.1 Kontrole 8.20-8.22. Daju smjernice za zaštitu mreža, segmentaciju usluga i zaštitu mrežnih usluga putem kontrola pristupa i praćenja.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Zaštita granica sustava: zahtijeva perimetarske kontrole, segmentaciju i sigurna međupovezivanja.

11.4.2 AC-4 - Provedba tokova informacija: podupire zoniranje i ograničenja prometa temeljena na pravilima.

11.4.3 SC-32 - Particioniranje informacijskih sustava: promiče logičko odvajanje informacijskih sustava.

11.5 GDPR EU (2016/679)

11.5.1 Članak 32 - Sigurnost obrade: zahtijeva tehničke mjere, kao što su vatrozidi i segmentacija, radi zaštite osobnih podataka.

11.6 Direktiva EU NIS2 (2022/2555)

11.6.1 Članak 21(2)(d): zahtijeva djelotvornu sigurnost mrežnih i informacijskih sustava, perimetarsku zaštitu, sigurnu konfiguraciju i kontrole razdvajanja.

11.7 Uredba EU DORA (2022/2554)

11.7.1 Članak 9 - upravljanje IKT rizicima: obvezuje financijske subjekte na zaštitu mreža i međupovezivanja od neovlaštenog pristupa, curenja podataka i operativnih prekida.

11.8 COBIT 2019

11.8.1 DSS01.03 - Praćenje infrastrukture: zahtijeva proaktivnu kontrolu nad stanjem mreže i povezivošću.

11.8.2 DSS05.01 - Zaštita od zlonamjernog softvera: uključuje segmentaciju i zaštitu granica sustava radi smanjenja širenja.

11.8.3 MEA03 - Praćenje, vrednovanje i procjena usklađenosti: jača provedbu mrežne politike i procjene usklađenosti.