					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P21S					Naziv dokumenta: **Politika sigurnosti mreže**							
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**

Pravna napomena (autorska prava i ograničenja uporabe)

(C) 2025 Clarysec LLC. All rights reserved.

Ovaj dokument intelektualno je vlasništvo društva Clarysec LLC. Nijedan dio ovog dokumenta ne smije se kopirati, ponovno upotrebljavati, distribuirati niti mijenjati u komercijalne svrhe ili svrhe implementacije bez izričitog prethodnog pisanog odobrenja.

Neovlaštena uporaba strogo je zabranjena i može rezultirati pravnim postupkom.

Za licenciranje kontaktirajte: info@clarysec.com

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točka 8	-
ISO/IEC 27002:2022	Kontrola 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
GDPR EU	Članak 32	-
Direktiva EU NIS2	Članci 21(2)(d), (e)	-
Uredba EU DORA	Članci 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Svrha

1.1. Svrha ove politike jest osigurati da su sve interne i vanjske mrežne komunikacije zaštićene od neovlaštenog pristupa, neovlaštenih izmjena, presretanja ili zlouporabe primjenom jasno definiranih sigurnosnih kontrola.

1.2. Ova politika utvrđuje pravila za sigurno projektiranje, korištenje i upravljanje mrežnom infrastrukturom, uključujući usmjerivače, bežične pristupne točke, veze za udaljeni pristup i segmentirane mreže.

1.3. Cilj politike jest smanjiti izloženost prijetnjama koje dolaze s interneta, osigurati povjerljivost podataka koji se prenose internim i vanjskim mrežama te održati dostupnost ključnih usluga.

1.4. Ova politika podupire certifikaciju prema ISO/IEC 27001:2022 i izravno doprinosi ispunjavanju zakonskih i regulatornih obveza prema GDPR-u, NIS2 i DORA-i, uz pružanje tehničkog jamstva klijentima i revizorima.

2. Područje primjene

2.1. Ova politika primjenjuje se na sve sastavnice IT mreže organizacije, uključujući:

2.1.1. žičanu i bežičnu infrastrukturu na uredskim lokacijama

2.1.2. usmjerivače, preklopnike, pristupne točke, vatrozide i pristupnike

2.1.3. veze za udaljeni pristup, uključujući VPN, RDP i tunele prema oblaku

2.1.4. aplikacije u oblaku kojima se pristupa iz internih ili vanjskih mreža

2.1.5. uređaje koje na mrežu povezuju zaposlenici, ugovorni izvođači ili gosti

2.2. Ova politika uređuje fizičke i logičke mrežne segmente, uključujući mreže za goste, uređaje Interneta stvari (IoT) i pozadinske poslovne sustave.

2.3. Politika obuhvaća sve osobe koje imaju pristup mreži organizacije, uključujući:

2.3.1. interne zaposlenike

2.3.2. radnike na daljinu i osoblje koje radi u hibridnom modelu

2.3.3. vanjske dobavljače, konzultante i pružatelje usluga

2.3.4. goste koji koriste privremeni Wi-Fi pristup

3. Ciljevi

3.1. Osigurati zaštitu mreže organizacije od neovlaštenog pristupa i vanjskih kibernetičkih prijetnji.

3.2. Osigurati odgovarajuću segmentaciju između pouzdanih i nepouzdanih mreža (npr. gostujući Wi-Fi, pristup dobavljača).

3.3. Omogućiti sigurno udaljeno povezivanje bez ugrožavanja internih sustava.

3.4. Spriječiti širenje zlonamjernog softvera i iznošenje podataka putem mrežnih kanala.

3.5. Osigurati praćenje, upozoravanje i revizijski trag mrežnih aktivnosti radi podrške otkrivanju incidenata i usklađenosti.

3.6. Osigurati da je povezivanje na interne mreže dopušteno samo odobrenim i zaštićenim uređajima.

3.7. Ispuniti obveze prema normi ISO 27001, GDPR-u i povezanim okvirima kibernetičke sigurnosti.

4. Uloge i odgovornosti

4.1. Glavni rukovoditelj (GM)

4.1.1. Vlasnik je ove politike i osigurava dodjelu odgovarajućih resursa za sigurno projektiranje i upravljanje mrežom.

4.1.2. Pregledava iznimke od kontrola sigurnosti mreže i odobrava sporazume o mrežnom pristupu dobavljača.

4.1.3. Pregledava incidente ili revizijske nalaze povezane sa slabostima sigurnosti mreže.

4.2. Pružatelj IT podrške / interna IT funkcija

4.2.1. Provodi, konfigurira i održava sve vatrozide, usmjerivače, preklopnike i kontrolere bežične mreže.

4.2.2. Upravlja segmentacijom između internih, gostujućih i vanjskih mreža.

4.2.3. Prati dnevničke zapise i upozorenja radi otkrivanja pokušaja neovlaštenog pristupa ili mrežnih anomalija.

4.2.4. Osigurava da se ažuriranja firmvera i konfiguracije primjenjuju sigurno i pravodobno.

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

9. Zahtjevi za pregled i ažuriranje

9.1. Godišnji pregled

9.1.1. Ovu politiku mora najmanje jednom godišnje pregledati glavni rukovoditelj zajedno s pružateljem IT podrške i koordinatorom za privatnost.

9.2. Okidači za izvanredni pregled

9.2.1. Pregled politike mora se pokrenuti i u slučaju:

9.2.1.1. značajnih promjena mrežne arhitekture (npr. novi VPN ili sustavi vatrozida)

9.2.1.2. mrežnog incidenta (npr. upad, širenje ucjenjivačkog softvera ili iznošenje podataka)

9.2.1.3. zakonskih, regulatornih ili okvirnih izmjena koje utječu na zaštitu mreže

9.2.1.4. novih platformi dobavljača koje zahtijevaju alternativne metode pristupa ili protokole

9.3. Upravljanje verzijama i dokumentacijom

9.3.1. Revizije politike moraju biti evidentirane s brojem verzije, datumom i sažetkom promjena.

9.3.2. Prethodne verzije moraju se arhivirati najmanje 3 godine.

9.3.3. Ažuriranja se moraju priopćiti pogođenim zaposlenicima, uz obveznu potvrdu upoznatosti s politikom kada se uvode značajne promjene u postupanju.

10. Povezane politike i poveznice

10.1. Ova politika mora se provoditi zajedno sa sljedećim SME sigurnosnim politikama:

10.1.1. P9S – Politika rada na daljinu: uređuje sigurne metode udaljenog pristupa, zahtjeve za VPN i zaštitu krajnjih uređaja za korisnike izvan lokacije.

10.1.2. P12S – Politika upravljanja imovinom: osigurava da su svi sustavi povezani na mrežu identificirani, kategorizirani i praćeni uz ažurne sigurnosne statuse.

10.1.3. P17S – Politika zaštite podataka i privatnosti: osigurava da segmentacija mreže, kontrole pristupa i zapisivanje podupiru načela privatnosti i zaštite podataka prema GDPR-u.

10.1.4. P22S – Politika bilježenja i praćenja: utvrđuje zahtjeve za prikupljanje i pregled dnevničkih zapisa s mrežnih uređaja, udaljenih veza i kontrolera bežične mreže.

10.1.5. P30S – Politika odgovora na incidente: definira potrebne radnje kao odgovor na mrežne povrede, pokušaje neovlaštenog pristupa ili širenje zlonamjernog softvera putem internih mreža.

11. Referentni standardi i okviri

11.1. ISO/IEC 27001

11.1.1. Točka 8.1 – Zahtijeva provedbu kontrola radi osiguravanja sigurnih i otpornih operacija, uključujući mreže.

11.2. ISO/IEC 27002

11.2.1. Kontrola 8.20 – Pruža tehničke i proceduralne smjernice za zaštitu mrežnog pristupa, segmentacije i praćenja.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Zahtijeva kontrolu toka informacija unutar mreža i između sustava.

11.3.2. SC-7 – Zahtijeva zaštitu granica sustava, sigurno usmjeravanje i segmentaciju mreže radi smanjenja rizika od neovlaštenog pristupa.

11.4. GDPR EU

11.4.1. Članak 32 – Zahtijeva odgovarajuće tehničke i organizacijske mjere za osiguravanje povjerljivosti, cjelovitosti i dostupnosti umreženih sustava i usluga koji obrađuju osobne podatke.

11.5. Direktiva EU NIS2

11.5.1. Članak 21(2)(d) – Zahtijeva tehničke mjere temeljene na riziku, uključujući sigurnost mreže i kontrolu pristupa.

11.5.2. Članak 21(2)(e) – Zahtijeva segmentaciju i izolaciju sustava radi sprječavanja širenja kibernetičkih incidenata.

11.6. Uredba EU DORA

11.6.1. Članak 9 – Zahtijeva da organizacije uspostave kontrole za upravljanje IKT rizicima, uključujući kontrole za sigurne mreže i komunikacije.

11.6.2. Članak 10 – Zahtijeva da strategije digitalne otpornosti obuhvate zaštitu mrežne infrastrukture i udaljenog povezivanja.

11.7. COBIT 2019

11.7.1. DSS05.02 – Zahtijeva djelotvornu zaštitu IT infrastrukture i mrežnih okruženja od internih i vanjskih prijetnji.

11.7.2. APO13.01 – Zahtijeva strategije upravljanja rizicima koje uključuju segmentaciju mreže i praćenje kao dio ublažavanja prijetnji.