					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P21S					Naslov dokumenta: **Politika varnosti omrežja**							
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	-
ISO/IEC 27002:2022	Kontrola 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
Uredba EU GDPR	Člen 32	-
Direktiva EU NIS2	Člena 21(2)(d), 21(2)(e)	-
Uredba EU DORA	Člena 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Namen

1.1. Namen te politike je zagotoviti, da so vse notranje in zunanje omrežne komunikacije zaščitene pred nepooblaščenim dostopom, posegi, prisluškovanjem ali neustrezno uporabo z jasno opredeljenimi varnostnimi kontrolami.

1.2. Določa pravila za varno načrtovanje, uporabo in upravljanje omrežne infrastrukture, vključno z usmerjevalniki, brezžičnimi dostopovnimi točkami, povezavami za oddaljeni dostop in segmentiranimi omrežji.

1.3. Njen cilj je zmanjšati izpostavljenost grožnjam z interneta, zagotoviti zaupnost podatkov, ki se prenašajo po notranjih in zunanjih omrežjih, ter ohraniti razpoložljivost ključnih storitev.

1.4. Ta politika podpira certificiranje po standardu ISO/IEC 27001:2022 in neposredno prispeva k izpolnjevanju zakonskih in regulativnih obveznosti v skladu z GDPR, NIS2 in DORA, hkrati pa zagotavlja tehnična zagotovila strankam in presojevalcem.

2. Področje uporabe

2.1. Ta politika velja za vse komponente organizacijskega IT-omrežja, vključno z:

2.1.1. žično in brezžično infrastrukturo na lokacijah organizacije

2.1.2. usmerjevalniki, stikali, dostopovnimi točkami, požarnimi zidovi in prehodi

2.1.3. povezavami za oddaljeni dostop, vključno z VPN, RDP in tuneli v oblaku

2.1.4. aplikacijami v oblaku, do katerih se dostopa iz notranjih ali zunanjih omrežij

2.1.5. napravami, ki jih v omrežje povezujejo zaposleni, pogodbeni izvajalci ali gostje

2.2. Ta politika ureja fizične in logične segmente omrežja, vključno z gostujočimi conami, napravami interneta stvari in zalednimi sistemi.

2.3. Politika velja za vse osebe z dostopom do omrežja organizacije, vključno z:

2.3.1. zaposlenimi

2.3.2. delavci na daljavo in zaposlenimi v hibridnih oblikah dela

2.3.3. zunanjimi dobavitelji, svetovalci in ponudniki storitev

2.3.4. gosti, ki uporabljajo začasni dostop do omrežja Wi-Fi

3. Cilji

3.1. Zagotoviti, da je omrežje organizacije zaščiteno pred nepooblaščenim dostopom in zunanjimi kibernetskimi grožnjami.

3.2. Uvesti ustrezno segmentacijo med zaupanja vrednimi in nezaupanja vrednimi omrežji (npr. gostujoči Wi-Fi, dostop dobaviteljev).

3.3. Omogočiti varno povezljivost na daljavo brez ogrožanja notranjih sistemov.

3.4. Preprečiti širjenje zlonamerne programske opreme in odtekanje podatkov prek omrežnih kanalov.

3.5. Zagotoviti spremljanje, opozarjanje in revizijsko beleženje omrežne dejavnosti za podporo odkrivanju incidentov in skladnosti.

3.6. Zagotoviti, da je povezovanje v notranja omrežja dovoljeno le odobrenim in ustrezno zaščitenim napravam.

3.7. Izpolniti obveznosti v skladu z ISO/IEC 27001, GDPR in povezanimi okviri kibernetske varnosti.

4. Vloge in odgovornosti

4.1. Generalni direktor

4.1.1. Je lastnik te politike in zagotavlja, da so za varno načrtovanje in upravljanje omrežja dodeljeni ustrezni viri.

4.1.2. Pregleduje izjeme od kontrol varnosti omrežja in odobrava dogovore o dostopu dobaviteljev do omrežja.

4.1.3. Pregleduje incidente ali ugotovitve presoje, povezane s pomanjkljivostmi na področju varnosti omrežja.

4.2. Ponudnik IT-podpore / notranja IT-funkcija

4.2.1. Uvede, konfigurira in vzdržuje vse požarne zidove, usmerjevalnike, stikala in krmilnike brezžičnih omrežij.

4.2.2. Upravlja segmentacijo med notranjimi, gostujočimi in zunanjimi omrežji.

4.2.3. Spremlja dnevnike in opozorila glede poskusov nepooblaščenega dostopa ali omrežnih anomalij.

4.2.4. Zagotavlja, da se posodobitve vdelane programske opreme in konfiguracij uvajajo varno in pravočasno.

[... 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. Letni pregled

9.1.1. To politiko mora najmanj enkrat letno pregledati generalni direktor skupaj s ponudnikom IT-podpore in koordinatorjem za zasebnost.

9.2. Sprožilci za vmesni pregled

9.2.1. Pregled politike se mora sprožiti tudi ob:

9.2.1.1. večjih spremembah omrežne arhitekture (npr. novi sistemi VPN ali požarnega zidu)

9.2.1.2. z omrežjem povezanem incidentu (npr. vdor, širjenje izsiljevalske programske opreme ali odtekanje podatkov)

9.2.1.3. zakonskih, regulativnih ali okvirnih posodobitvah, ki vplivajo na zaščito omrežja

9.2.1.4. novih platformah dobaviteljev, ki zahtevajo alternativne metode dostopa ali protokole

9.3. Upravljanje različic in dokumentacija

9.3.1. Revizije politike morajo biti zabeležene s številko različice, datumom in povzetkom sprememb.

9.3.2. Prejšnje različice morajo biti arhivirane najmanj 3 leta.

9.3.3. Posodobitve morajo biti sporočene zadevnim zaposlenim, ob pomembnih spremembah vedenjskih zahtev pa je treba pridobiti tudi zahtevano potrditev.

10. Povezane politike in povezave

10.1. Ta politika se mora izvajati skupaj z naslednjimi varnostnimi politikami SME:

10.1.1. P9S – Politika dela na daljavo: določa varne metode oddaljenega dostopa, zahteve glede VPN in zaščito končnih točk za uporabnike zunaj lokacije.

10.1.2. P12S – Politika upravljanja sredstev: zagotavlja, da so vsi sistemi, povezani v omrežje, identificirani, kategorizirani in sledeni z ažurnim varnostnim stanjem.

10.1.3. P17S – Politika varstva podatkov in zasebnosti: zagotavlja, da segmentacija omrežja, kontrole dostopa in beleženje podpirajo načela zasebnosti in varstva podatkov v skladu z GDPR.

10.1.4. P22S – Politika beleženja in spremljanja: določa zahteve za zajem in pregled dnevnikov iz omrežnih naprav, oddaljenih povezav in brezžičnih krmilnikov.

10.1.5. P30S – Politika odzivanja na incidente: določa zahtevane ukrepe ob omrežnih kršitvah, poskusih nepooblaščenega dostopa ali širjenju zlonamerne programske opreme prek notranjih omrežij.

11. Referenčni standardi in okviri

11.1. ISO/IEC 27001

11.1.1. Klavzula 8.1 – zahteva uvedbo kontrol za zagotavljanje varnega in odpornega delovanja, vključno z omrežji.

11.2. ISO/IEC 27002

11.2.1. Kontrola 8.20 – podaja tehnične in postopkovne usmeritve za varovanje omrežnega dostopa, segmentacije in spremljanja.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – zahteva nadzor pretoka informacij znotraj omrežij in med sistemi.

11.3.2. SC-7 – zahteva zaščito omrežnega roba, varno usmerjanje in segmentacijo omrežja za zmanjšanje tveganja nepooblaščenega dostopa.

11.4. Uredba EU GDPR

11.4.1. Člen 32 – zahteva ustrezne tehnične in organizacijske ukrepe za zagotavljanje zaupnosti, celovitosti in razpoložljivosti omrežno povezanih sistemov in storitev, ki obdelujejo osebne podatke.

11.5. Direktiva EU NIS2

11.5.1. Člen 21(2)(d) – zahteva tehnične ukrepe na podlagi tveganj, vključno z varnostjo omrežja in nadzorom dostopa.

11.5.2. Člen 21(2)(e) – zahteva segmentacijo in izolacijo sistemov za preprečevanje širjenja kibernetskih incidentov.

11.6. Uredba EU DORA

11.6.1. Člen 9 – zahteva, da organizacije uvedejo kontrole za upravljanje tveganj IKT, vključno s kontrolami za varna omrežja in komunikacije.

11.6.2. Člen 10 – zahteva, da strategije digitalne operativne odpornosti zajemajo zaščito omrežne infrastrukture in povezljivosti na daljavo.

11.7. COBIT 2019

11.7.1. DSS05.02 – zahteva učinkovito zaščito IT-infrastrukture in omrežnih okolij pred notranjimi in zunanjimi grožnjami.

11.7.2. APO13.01 – zahteva strategije upravljanja tveganj, ki vključujejo segmentacijo omrežja in spremljanje kot del zmanjševanja groženj.