					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P19S					Naslov dokumenta: **Politika upravljanja ranljivosti in popravkov**							
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	Kontroli 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
EU NIS2	Člena 21(2)(d), 21(2)(e)	
EU DORA	Člena 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
EU GDPR	Člen 32(1)(b)	

1. Namen

1.1 Ta politika določa, kako organizacija prepoznava, ocenjuje in zmanjšuje ranljivosti v sistemih, aplikacijah in infrastrukturi.

1.2 Njen namen je zmanjšati kibernetska tveganja z zagotavljanjem pravočasnega nameščanja popravkov in izvajanja ukrepov za odpravo pomanjkljivosti na podlagi tveganj, primernih za mala in srednje velika podjetja (MSP).

1.3 Ta politika podpira skladnost z zahtevami standarda ISO/IEC 27001:2022 in pomaga izpolnjevati regulativne obveznosti v skladu z GDPR, NIS2 in DORA, saj zahteva proaktivno upravljanje tehničnih ranljivosti.

1.4 Organizacija priznava, da nepopravljeni sistemi predstavljajo pomembno tveganje za informacijsko varnost in jih je treba obravnavati sistematično in brez odlašanja.

2. Področje uporabe

2.1 Ta politika se uporablja za:

2.1.1 vse strežnike, namizne računalnike, prenosne računalnike, mobilne naprave, omrežno opremo in platforme v oblaku, ki jih uporablja organizacija,

2.1.2 vse operacijske sisteme, programsko opremo tretjih oseb, vtičnike in aplikacije, ki se uporabljajo pri poslovanju,

2.1.3 notranje osebje IT ali zunanje izvajalce storitev, odgovorne za vzdrževanje sistemov, posodobitve ali spremljanje,

2.1.4 vso namensko razvito izvorno kodo ali vdelano programsko opremo, ki jo vzdržuje organizacija ali se vzdržuje v njenem imenu.

2.2 Politika zajema tako infrastrukturo, ki jo organizacija upravlja neposredno, kot tudi sisteme, ki jih upravljajo pogodbeni dobavitelji ali ponudniki gostovanja.

3. Cilji

3.1 pravočasno in dosledno prepoznavati ter ocenjevati znane ranljivosti v vseh IT-sredstvih,

3.2 nameščati popravke in posodobitve programske opreme glede na resnost ter tveganje za delovanje organizacije ali osebne podatke,

3.3 preprečevati izkoriščanje tehničnih slabosti, ki bi lahko povzročile prekinitev storitev, kršitev varnosti osebnih podatkov ali neskladnost s predpisi,

3.4 voditi točne evidence o nameščenih popravkih, odprtih vprašanjih in izjemah, da se zagotovi pripravljenost na revizijo,

3.5 uporabljati orodja in procese, primerne velikosti organizacije in njeni operativni kompleksnosti, brez zmanjšanja učinkovitosti,

3.6 podpirati pravno in regulativno skladnost, vključno s členom 32 GDPR in kontrolo 8 Priloge A standarda ISO.

4. Vloge in odgovornosti

4.1 Generalni direktor (GD)

4.1.1 nosi splošno odgovornost za zagotavljanje izvajanja dejavnosti nameščanja popravkov in upravljanja ranljivosti,

4.1.2 odobri izjeme glede tveganj, kadar popravkov ni mogoče namestiti, ter pregleda povezane ukrepe za ublažitev,

4.1.3 pregleduje poročila o stanju nameščanja popravkov in zagotavlja razpoložljivost virov za izpolnjevanje obveznosti na tem področju.

4.2 Izvajalec IT-podpore / notranji skrbnik IT

4.2.1 spremlja sisteme glede ranljivosti in razpoložljivih popravkov z uporabo opozoril dobaviteljev, obvestil o grožnjah in obvestil na ravni operacijskega sistema,

4.2.2 namešča posodobitve operacijskih sistemov, vdelane programske opreme in aplikacij v določenih rokih,

4.2.3 vodi formalno evidenco popravkov in dokumentira nerešene ali odložene posodobitve,

4.2.4 izvaja testiranje in uvajanje kritičnih posodobitev za zmanjšanje operativnih motenj.

[... 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 ob prispevku izvajalca IT-podpore in koordinatorja za zasebnost.

9.2 Sprožilci pregleda

9.2.1 Vmesni pregledi se morajo izvesti, če:

9.2.1.1 pomembna ranljivost ali izkoriščanje prizadene sisteme v področju uporabe,

9.2.1.2 pride do pomembnih sprememb sistemov ali programske opreme,

9.2.1.3 revizija ugotovi vrzeli v postopkih nameščanja popravkov,

9.2.1.4 je zabeležen incident ali kršitev, povezana z nameščanjem popravkov.

9.3 Nadzor različic politike

9.3.1 Vse posodobitve morajo biti zabeležene v evidenci različic s povzetkom sprememb.

9.3.2 Spremembe morajo biti sporočene prizadetemu osebju.

9.3.3 Zastarele različice morajo biti arhivirane z omejenim dostopom.

10. Povezane politike in povezave

10.1 Ta politika podpira več drugih politik SME in je z njimi povezana:

10.1.1 P12S – Politika upravljanja sredstev: določa lastništvo sistemov in razvrstitev, s čimer zagotavlja, da so vsa sredstva, za katera je potrebno nameščanje popravkov, upoštevana in evidentirana v popisu,

10.1.2 P14S – Politika hrambe in odstranjevanja podatkov: zagotavlja, da so sistemi, predvideni za izločitev iz uporabe, varno posodobljeni ali izbrisani, s čimer se zmanjša izpostavljenost ranljivostim,

10.1.3 P17S – Politika varstva podatkov in zasebnosti: daje prednost odpravi ranljivosti v sistemih, ki obdelujejo osebne podatke, zaradi skladnosti s predpisi o zasebnosti,

10.1.4 P22S – Politika beleženja in spremljanja: podpira zaznavanje nepopravljenih sistemov ali sumljivega vedenja, ki lahko kaže na izkoriščanje ranljivosti,

10.1.5 P30S – Politika odzivanja na incidente: določa postopke za odzivanje na ranljivosti, ki povzročijo varnostne incidente, vključno z eskalacijo in poročanjem.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001

11.1.1 Klavzula 8.1 – zahteva izvajanje kontrol za obravnavo operativnih tveganj, vključno z upravljanjem ranljivosti.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.8 – določa procese za pregledovanje in odpravljanje znanih slabosti v sistemih.

11.2.2 Kontrola 8.9 – poudarja varno konfiguracijo, preverjanje popravkov in nadzor sprememb, da se med posodobitvami prepreči nova izpostavljenost.

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – zahteva prepoznavanje ranljivosti in odpravo pomanjkljivosti v določenih rokih.

11.3.2 SI-2 – zahteva hitro uporabo popravkov in posodobitev glede na resnost.

11.3.3 CM-2 – ureja izhodiščne konfiguracije sistemov in dokumentiranje posodobitev za zagotavljanje dosledne zaščite.

11.4 Uredba EU GDPR

11.4.1 Člen 32(1)(b) – zahteva, da organizacije uvedejo ustrezne tehnične ukrepe, vključno z nameščanjem popravkov, za zagotavljanje varnosti obdelave.

11.5 Direktiva EU NIS2

11.5.1 Člen 21(2)(d) – zahteva obravnavo ranljivosti s sistematičnim pregledovanjem in odpravljanjem pomanjkljivosti.

11.5.2 Člen 21(2)(e) – nalaga varno konfiguracijo in upravljanje popravkov za zagotavljanje odpornosti sistemov IKT.

11.6 Uredba EU DORA

11.6.1 Člen 8(1) – zahteva zaznavanje in zmanjševanje tveganj IKT, vključno s tehničnimi ranljivostmi.

11.6.2 Člen 10(2) – finančnim subjektom nalaga odpravo slabosti, ki vplivajo na sisteme IKT in operacije.

11.7 COBIT 2019

11.7.1 DSS05.02 – zahteva obravnavo znanih tehničnih ranljivosti za ohranjanje varnega delovanja.

11.7.2 APO12.01 – usklajuje upravljanje tveganj s proaktivnim spremljanjem in odpravljanjem sistemskih slabosti.