					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P19					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	Sistematična obravnava tehničnih ranljivosti in trajna učinkovitost varnostnih kontrol.
ISO/IEC 27002:2022	Kontrole 8.8, 8.9, 5	Smernice za nameščanje popravkov, skeniranje ranljivosti, celovitost programske opreme, varno konfiguracijo in popis sredstev.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Zahteva pogosto skeniranje, odpravo pomanjkljivosti in upravljanje konfiguracij.
EU GDPR	Člen 32, uvodna izjava 49	Tehnični ukrepi za pravočasno nameščanje popravkov, obravnavo ranljivosti in neprekinjeno varnost.
EU NIS2	Člen 21(2)(d)	Zaznavanje, odzivanje in zmanjševanje ranljivosti za zagotavljanje visoke ravni kibernetske higiene.
EU DORA	Člena 8, 10(2)(f)	Pravočasna odprava ranljivosti IKT ter stalne presoje, vodene z grožnjami.
COBIT 2019	DSS05.02, DSS01.03, MEA	Skeniranje, sledenje in zmanjševanje tehničnih slabosti, spremljanje znakov izkoriščanja ter presoja učinkovitosti, vključno s stanjem popravkov.

1. Namen

1.1 Ta politika določa obvezne zahteve organizacije za prepoznavanje, razvrščanje, odpravo in spremljanje tehničnih ranljivosti ter pomanjkljivosti programske opreme v vseh informacijskih sistemih in sredstvih, ki so v obsegu sistema upravljanja informacijske varnosti (ISMS).

1.2 Zagotavlja, da se vse znane ranljivosti ocenijo in obravnavajo pravočasno ter na podlagi tveganj z usklajenim nameščanjem popravkov, prilagoditvami konfiguracije ali nadomestnimi kontrolami, skladno s poslovnimi potrebami in obveznostmi glede skladnosti.

1.3 Ta politika podpira skladnost s kontrolo 8.8 Priloge A standarda ISO/IEC 27001 in smernicami ISO/IEC 27002 ter obravnava regulativne zahteve v skladu s členom 8 Uredbe EU DORA, členom 21 Direktive EU NIS2, členom 32 Uredbe EU GDPR ter domenama DSS in APO okvira COBIT 2019.

2. Področje uporabe

2.1 Ta politika se uporablja za vse informacijske sisteme, sredstva in okolja, ki hranijo, obdelujejo ali prenašajo podatke, ki so predmet upravljanja v okviru ISMS, vključno z:

2.1.1 operacijskimi sistemi, aplikacijami, omrežnimi napravami, vdelano programsko opremo, oblačnimi platformami, programskimi vmesniki (API) in programsko opremo tretjih oseb.

2.1.2 sistemi v razvojnih, pripravljalnih in produkcijskih okoljih, okoljih za varnostno kopiranje ter okoljih za obnovitev po nesreči.

2.1.3 končnimi točkami, strežniki, napravami interneta stvari, infrastrukturo za virtualizacijo in vsebniki.

2.2 Zavezujoča je za:

2.2.1 notranje osebje: skrbnike IT, sistemske inženirje, razvijalce aplikacij, varnostne analitike in infrastrukturne ekipe.

2.2.2 zunanje strani: pogodbene izvajalce, ponudnike upravljanih storitev (MSP), dobavitelje programske opreme in sistemske integratorje s tehničnimi odgovornostmi za sredstva v obsegu.

2.3 Politika zajema celoten življenjski cikel upravljanja ranljivosti in popravkov, vključno z:

2.3.1 skeniranjem in zaznavanjem

2.3.2 razvrščanjem tveganj in določanjem prioritet

2.3.3 pridobivanjem popravkov, testiranjem, uvajanjem in povrnitvijo

2.3.4 obravnavo izjem in načrtovanjem nadomestnih kontrol

2.3.5 beleženjem, poročanjem in revizijsko sledljivostjo

3. Cilji

3.1 Zagotoviti, da so vse znane ranljivosti prepoznane, ocenjene in odpravljene na način, ki zmanjšuje izpostavljenost tveganju ter je usklajen z operativnimi prioritetami.

3.2 Vzpostaviti dosledne procese na ravni celotne organizacije za skeniranje ranljivosti, razvrščanje resnosti (npr. CVSS) in upravljanje popravkov, vključno z nujno obravnavo in načrtovanjem povrnitve.

3.3 Omogočiti upravljanje varnih konfiguracij z uskladitvijo z izhodiščnimi konfiguracijami za utrjevanje, praksami upravljanja sprememb in sprotnimi obveščevalnimi podatki o grožnjah.

3.4 Zagotoviti merljivo skladnost z regulatornimi zahtevami in standardnimi kontrolami, povezanimi s celovitostjo sistemov, higieno popravkov in pravočasno odpravo pomanjkljivosti.

3.5 Določiti odgovornost in pristojnosti po vlogah za celoten življenjski cikel upravljanja ranljivosti ter zagotoviti, da vse zainteresirane strani ravnajo v skladu z opredeljenimi sporazumi o ravni storitev in poročanimi kazalniki kontrol.

3.6 Zagotoviti pripravljenost na revizijo in izboljšati odpornost proti nastajajočim grožnjam, vključno z ranljivostmi ničtega dne, aktivnimi verigami izkoriščanja in odmevnimi obvestili dobaviteljev.

4. Vloge in odgovornosti

4.1 Vodja informacijske varnosti (CISO)

4.1.1 Je lastnik politike in zagotavlja njeno vključitev v ISMS.

4.1.2 Določa profil tveganja organizacije ter zagotavlja usklajenost z regulativnimi zahtevami in pričakovanji glede kontrol.

4.2 Vodja upravljanja ranljivosti / vodja varnostnih operacij

4.2.1 Nadzira celovito izvajanje upravljanja ranljivosti in popravkov.

4.2.2 Usklajuje urnike skeniranja, modele določanja prioritet in časovnice odprave.

4.2.3 Vzdržuje register ranljivosti in sodeluje pri ocenjevanju nadomestnih kontrol.

[... 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 Ta politika se pregleda najmanj enkrat letno ali ob:

9.1.1 pomembnih regulativnih posodobitvah (npr. spremembe DORA, NIS2)

9.1.2 spremembah okvirov za določanje prioritet ranljivosti (npr. posodobitve CVSS)

9.1.3 večjih spremembah IT-okolja (npr. migracija v oblak, prenova EDR)

9.1.4 odmevnih kršitvah ali zunanjih opozorilih, ki zahtevajo okrepitev politike

9.2 Preglede izvaja vodja informacijske varnosti v sodelovanju z varnostnimi operacijami, upravljanjem tveganj in vodstvom infrastrukture.

9.3 Posodobitve politike morajo biti:

9.3.1 dokumentirane v registru nadzora dokumentacije ISMS

9.3.2 pregledane in odobrene s strani najvišjega vodstva

9.3.3 sporočene vsem zadevnim zainteresiranim stranem, vključno z obdelovalci tretjih oseb

9.4 Zgodovinske različice se morajo varno hraniti za potrebe revizije in odgovornosti.

10. Povezane politike in povezave

10.1 P1 - Politika informacijske varnosti. Določa krovno zavezanost varovanju sistemov in podatkov, kar vključuje proaktivno upravljanje ranljivosti in zagotavljanje celovitosti programske opreme.

10.2 P5 - Politika upravljanja sprememb. Ureja vsa uvajanja popravkov in prilagoditve konfiguracije ter zahteva dokumentiranje, testiranje, odobritev in postopke povrnitve, ki dopolnjujejo procese odprave ranljivosti.

10.3 P6 - Politika upravljanja tveganj. Podpira razvrščanje in obravnavo neodpravljenih ranljivosti s strukturiranimi ocenami tveganja, analizo vpliva in postopki sprejemanja preostalega tveganja.

10.4 P12 - Politika upravljanja sredstev. Zagotavlja, da so sistemi ustrezno popisani in razvrščeni, kar omogoča dosledno skeniranje ranljivosti, dodelitev lastništva in pokritost s popravki skozi celoten življenjski cikel.

10.5 P22 - Politika beleženja in spremljanja. Določa zahteve za zaznavanje dogodkov in vzpostavitev revizijske sledi. Ta politika podpira vidljivost nad dejavnostmi nameščanja popravkov, nepooblaščenimi spremembami in poskusi izkoriščanja znanih ranljivosti.

10.6 P30 - Politika odzivanja na incidente. Določa protokole eskalacije in strategije zajezitve za izkoriščene ranljivosti, preiskave kršitev in korektivne ukrepe, usklajene s kontrolami te politike.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001: Klavzula 8.1 - Operativno načrtovanje in nadzor: zahteva sistematično obravnavo tehničnih ranljivosti za zagotovitev trajne učinkovitosti varnostnih kontrol.

11.2 ISO/IEC 27002:2022 - Kontrole 8.8, 8.9, 5: podaja smernice za nameščanje popravkov, skeniranje ranljivosti, celovitost programske opreme in povezavo z varno konfiguracijo ter popisom sredstev.

11.3 NIST SP 800-53 Rev.5: RA-5 - Spremljanje in skeniranje ranljivosti: zahteva pogosto skeniranje in sledenje odpravi. SI-2 - Odprava pomanjkljivosti: zahteva takojšnjo oceno in ublažitev pomanjkljivosti z razpoložljivimi popravki ali drugimi ukrepi. CM-2 / CM-6 - Izhodiščne konfiguracije in kontrole upravljanja konfiguracije: vzpostavlja temelje za varne konfiguracije sistemov, povezane z uveljavljanjem popravkov.

11.4 EU GDPR (2016/679): Člen 32 - Varnost obdelave: zahteva uvedbo ustreznih tehničnih ukrepov, kot sta pravočasno nameščanje popravkov in obravnava ranljivosti, za zagotavljanje zaupnosti in odpornosti sistemov. Uvodna izjava 49: spodbuja subjekte k uvedbi preventivnih kontrolnih ukrepov proti znanim grožnjam za podporo varnosti in neprekinjenemu delovanju.

11.5 Direktiva EU NIS2 (2022/2555): Člen 21(2)(d): bistvenim in pomembnim subjektom nalaga zaznavanje ranljivosti sistemov, odzivanje nanje in njihovo zmanjševanje ter vzdrževanje visoke ravni kibernetske higiene.

11.6 Uredba EU DORA (2022/2554): Člen 8 - Upravljanje tveganj IKT: zahteva prepoznavanje in pravočasno odpravo ranljivosti v informacijskih in komunikacijskih tehnologijah, ki se uporabljajo v

finančnih sistemih. Člen 10(2)(f): poudarja stalne presoje ranljivosti in nameščanje popravkov, vodene z grožnjami, kot del operativne odpornosti.

11.7 COBIT 2019: DSS05.02 - Upravljanje varnostnih ranljivosti: organizacijam nalaga skeniranje, sledenje in zmanjševanje znanih tehničnih slabosti. DSS01.03 - Spremljanje infrastrukture: zagotavlja, da se sistemi spremljajo glede znakov izkoriščanja ali slabosti. MEA03 - Spremljanje, vrednotenje in presoja skladnosti: zahteva redno presojo učinkovitosti kontrol, vključno s stanjem popravkov in obravnavo izjem.