					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P19S					Naziv dokumenta: **Politika upravljanja ranjivostima i zakrpama**							
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	
ISO/IEC 27002:2022	Kontrole 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
Direktiva EU NIS2	Članci 21(2)(d), 21(2)(e)	
Uredba EU DORA	Članci 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
GDPR	Članak 32(1)(b)	

1. Svrha

1.1 Ova politika definira način na koji organizacija pravodobno i dosljedno identificira, procjenjuje i ublažava ranjivosti u sustavima, aplikacijama i infrastrukturi.

1.2 Svrha ove politike jest smanjiti kibernetički sigurnosni rizik pravodobnim zakrpavanjem i otklanjanjem nedostataka na temelju procjene rizika, primjereno malim i srednjim poduzećima (SME).

1.3 Ova politika podupire usklađenost sa zahtjevima za certifikaciju prema normi ISO/IEC 27001:2022 i pomaže u ispunjavanju regulatornih obveza prema GDPR-u, NIS2 i DORA-i zahtijevajući proaktivno upravljanje tehničkim ranjivostima.

1.4 Organizacija prepoznaje da nezakrpljeni sustavi predstavljaju značajnu prijetnju informacijskoj sigurnosti te se moraju rješavati sustavno i bez odgode.

2. Područje primjene

2.1 Ova politika primjenjuje se na:

2.1.1 sve poslužitelje, stolna i prijenosna računala, mobilne uređaje, mrežnu opremu i platforme u oblaku koje organizacija koristi

2.1.2 sve operacijske sustave, softver trećih strana, dodatke i aplikacije koji se koriste u poslovnim operacijama

2.1.3 interno IT osoblje ili vanjske pružatelje usluga odgovorne za održavanje sustava, ažuriranja ili praćenje

2.1.4 sav prilagođeno razvijeni kod ili ugrađeni kod koji organizacija održava sama ili se održava u njezino ime

2.2 Ova politika obuhvaća i infrastrukturu kojom organizacija upravlja izravno i sustave kojima upravljaju ugovoreni dobavljači ili pružatelji usluga hostinga.

3. Ciljevi

3.1 pravodobno i dosljedno identificirati i procjenjivati poznate ranjivosti na cjelokupnoj IT imovini

3.2 primjenjivati zakrpe i ažuriranja softvera na temelju ozbiljnosti i rizika za poslovanje organizacije ili osobne podatke

3.3 spriječiti iskorištavanje tehničkih slabosti koje mogu dovesti do prekida usluge, povrede podataka ili neusklađenosti sa zakonskim zahtjevima

3.4 voditi točne evidencije o primijenjenim zakrpama, otvorenim pitanjima i iznimkama radi revizijske spremnosti

3.5 koristiti alate i procese primjerene veličini organizacije i složenosti njezina poslovanja, bez ugrožavanja djelotvornosti

3.6 podupirati zakonsku i regulatornu usklađenost, uključujući članak 32. GDPR-a i Kontrolu 8 iz Priloga A norme ISO

4. Uloge i odgovornosti

4.1 glavni rukovoditelj (GM)

4.1.1 snosi ukupnu odgovornost za osiguravanje provedbe aktivnosti zakrpavanja i upravljanja ranjivostima

4.1.2 odobrava iznimke od rizika kada nije moguće primijeniti zakrpe i pregledava povezane mjere ublažavanja

4.1.3 pregledava izvješća o statusu zakrpavanja i osigurava dostupnost resursa za ispunjavanje obveza zakrpavanja

4.2 pružatelj IT podrške / interni IT administrator

4.2.1 prati sustave radi utvrđivanja ranjivosti i dostupnih zakrpa koristeći obavijesti dobavljača, sigurnosna upozorenja i obavijesti na razini operacijskog sustava

4.2.2 primjenjuje ažuriranja operacijskog sustava, firmvera i aplikacija unutar definiranih rokova

4.2.3 vodi formalnu evidenciju zakrpa i dokumentira neriješena ili odgođena ažuriranja

4.2.4 provodi testiranje i planiranje kritičnih ažuriranja radi smanjenja operativnih prekida na najmanju moguću mjeru

[... 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, uz doprinos pružatelja IT podrške i koordinatora za privatnost

9.2 okidači pregleda

9.2.1 izvanredni pregledi moraju se provesti ako:

9.2.1.1 velika ranjivost ili iskorištavanje utječe na sustave unutar područja primjene

9.2.1.2 dođe do značajnih promjena sustava ili softvera

9.2.1.3 revizija utvrdi nedostatke u procesima zakrpavanja

9.2.1.4 zabilježi se incident ili povreda povezana sa zakrpavanjem

9.3 upravljanje verzijama politike

9.3.1 sva ažuriranja moraju se evidentirati u zapisniku verzija sa sažetkom promjena

9.3.2 promjene se moraju priopćiti zahvaćenom osoblju

9.3.3 zastarjele verzije moraju se arhivirati uz ograničen pristup

10. Povezane politike i poveznice

10.1 Ova politika podupire i ovisi o više drugih SME politika:

10.1.1 P12S – Politika upravljanja imovinom: utvrđuje vlasništvo nad sustavima i klasifikaciju te osigurava da je sva imovina koja zahtijeva zakrpavanje obuhvaćena i evidentirana u popisu imovine

10.1.2 P14S – Politika zadržavanja i zbrinjavanja podataka: osigurava da se sustavi planirani za stavljanje izvan uporabe sigurno ažuriraju ili brišu, čime se smanjuje izloženost ranjivostima

10.1.3 P17S – Politika zaštite podataka i privatnosti: daje prioritet otklanjanju ranjivosti na sustavima koji obrađuju osobne podatke radi usklađenosti sa zakonima o privatnosti

10.1.4 P22S – Politika bilježenja i praćenja: podupire otkrivanje nezakrpljenih sustava ili sumnjivih ponašanja koja mogu upućivati na iskorištavanje ranjivosti

10.1.5 P30S – Politika odgovora na incidente: definira postupke za odgovor na ranjivosti koje rezultiraju sigurnosnim incidentima, uključujući korake eskalacije i prijavljivanja

11. Referentni standardi i okviri

11.1 ISO/IEC 27001

11.1.1 Točka 8.1 – zahtijeva provedbu kontrola za rješavanje operativnog rizika, uključujući upravljanje ranjivostima

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.8 – propisuje procese za skeniranje i otklanjanje poznatih slabosti u sustavima

11.2.2 Kontrola 8.9 – naglašava sigurnu konfiguraciju, provjeru zakrpa i upravljanje promjenama kako bi se izbjegla nova izloženost tijekom ažuriranja

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – zahtijeva identificiranje ranjivosti i njihovo otklanjanje unutar definiranih rokova

11.3.2 SI-2 – nalaže pravodobnu primjenu zakrpa i ažuriranja na temelju ozbiljnosti

11.3.3 CM-2 – uređuje referentne konfiguracije sustava i dokumentiranje ažuriranja radi osiguravanja dosljedne zaštite

11.4 GDPR

11.4.1 Članak 32(1)(b) – zahtijeva da organizacije primijene odgovarajuće tehničke mjere, uključujući zakrpavanje, radi održavanja sigurnosti obrade

11.5 Direktiva EU NIS2

11.5.1 Članak 21(2)(d) – zahtijeva postupanje s ranjivostima kroz sustavno skeniranje i otklanjanje nedostataka

11.5.2 Članak 21(2)(e) – obvezuje na sigurnu konfiguraciju i upravljanje zakrpama radi osiguravanja IKT otpornosti

11.6 Uredba EU DORA

11.6.1 Članak 8(1) – zahtijeva otkrivanje i ublažavanje IKT rizika, uključujući tehničke ranjivosti

11.6.2 Članak 10(2) – nalaže financijskim subjektima otklanjanje slabosti koje utječu na IKT sustave i operacije

11.7 COBIT 2019

11.7.1 DSS05.02 – zahtijeva obradu poznatih tehničkih ranjivosti radi održavanja sigurnog poslovanja

11.7.2 APO12.01 – usklađuje upravljanje rizicima s proaktivnim praćenjem i otklanjanjem slabosti sustava