					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P19					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	Sustavno upravljanje tehničkim ranjivostima; kontinuirana djelotvornost sigurnosnih kontrola.
ISO/IEC 27002:2022	Kontrole 8.8, 8.9, 5	Smjernice za provedbu zakrpavanja, skeniranja ranjivosti, cjelovitost softvera, sigurnu konfiguraciju i popis imovine.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Propisuje učestala skeniranja, otklanjanje nedostataka i upravljanje konfiguracijom.
EU GDPR	Članak 32, uvodna izjava 49	Tehničke mjere za pravodobno zakrpavanje, obradu ranjivosti i kontinuitet sigurnosti.
EU NIS2	Članak 21(2)(d)	Otkrivanje, odgovor i ublažavanje ranjivosti radi održavanja visoke razine kibernetičke higijene.
EU DORA	Članci 8, 10(2)(f)	Pravodobno otklanjanje IKT ranjivosti; kontinuirane procjene temeljene na prijetnjama.
COBIT 2019	DSS05.02, DSS01.03, MEA	Skeniranje, praćenje i ublažavanje tehničkih slabosti; praćenje znakova iskorištavanja; revizija djelotvornosti, uključujući status zakrpavanja.

1. Svrha

1.1 Ova politika definira obvezne zahtjeve organizacije za identifikaciju, klasifikaciju, otklanjanje i praćenje tehničkih ranjivosti i softverskih nedostataka u svim informacijskim sustavima i imovini unutar opsega ISMS-a.

1.2 Ova politika osigurava da se sve poznate ranjivosti procjenjuju i obrađuju pravodobno i na temelju rizika, putem koordiniranog zakrpavanja, prilagodbi konfiguracije ili kompenzacijskih kontrola, u skladu s poslovnim potrebama i obvezama usklađenosti.

1.3 Ova politika podupire usklađenost s kontrolom 8.8 Dodatka A norme ISO/IEC 27001 i smjernicama norme ISO/IEC 27002 te obuhvaća regulatorne zahtjeve iz članka 8 Uredbe EU DORA, članka 21 Direktive EU NIS2, članka 32 Uredbe EU GDPR i domena DSS i APO okvira COBIT 2019.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve informacijske sustave, imovinu i okruženja koja pohranjuju, obrađuju ili prenose podatke koji podliježu upravljanju u okviru ISMS-a, uključujući:

2.1.1 operativne sustave, aplikacije, mrežne uređaje, firmver, platforme u oblaku, aplikacijska programska sučelja i softver trećih strana.

2.1.2 sustave u razvoju, testna okruženja, produkcijska okruženja, okruženja sigurnosnih kopija i okruženje za oporavak od katastrofe.

2.1.3 krajnje uređaje, poslužitelje, uređaje Interneta stvari (IoT), virtualizacijsku infrastrukturu i kontejnere.

2.2 Ova politika obvezuje:

2.2.1 interno osoblje: IT administratore, sistemske inženjere, razvojne inženjere, sigurnosne analitičare i infrastrukturne timove.

2.2.2 vanjske strane: ugovorne izvođače, pružatelje upravljanih usluga (MSP), dobavljače softvera i sistem integratore s tehničkim odgovornostima nad imovinom unutar područja primjene.

2.3 Ova politika obuhvaća cjelokupan životni ciklus upravljanja ranjivostima i zakrpama, uključujući:

2.3.1 skeniranje i otkrivanje

2.3.2 klasifikaciju i određivanje prioriteta na temelju rizika

2.3.3 pribavljanje, testiranje, uvođenje i povrat zakrpa

2.3.4 postupanje s iznimkama i planiranje kompenzacijskih kontrola

2.3.5 evidentiranje, izvješćivanje i sljedivost za potrebe revizije

3. Ciljevi

3.1 Osigurati da se sve poznate ranjivosti identificiraju, procijene i otklone na način koji smanjuje izloženost riziku i usklađen je s operativnim prioritetima.

3.2 Uspostaviti dosljedne procese na razini cijele organizacije za skeniranje ranjivosti, klasifikaciju ozbiljnosti (npr. CVSS) i upravljanje zakrpama, uključujući hitno postupanje i planiranje povrata.

3.3 Omogućiti sigurno upravljanje konfiguracijom usklađivanjem s baznim konfiguracijama, praksama upravljanja promjenama i obavještajnim podacima o prijetnjama u stvarnom vremenu.

3.4 Osigurati mjerljivu usklađenost s regulatornim zahtjevima i kontrolama temeljenima na standardima koje se odnose na cjelovitost sustava, disciplinu zakrpavanja i pravodobno otklanjanje nedostataka.

3.5 Definirati ovlasti i odgovornosti po ulogama za cjelokupan životni ciklus upravljanja ranjivostima te osigurati da svi dionici postupaju u skladu s definiranim sporazumima o razini usluge (SLA) i prijavljivim metrikama kontrola.

3.6 Ojačati spremnost za reviziju i unaprijediti otpornost na nove prijetnje, uključujući zero-day ranjivosti, aktivne lance iskorištavanja i objave dobavljača s visokim utjecajem.

4. Uloge i odgovornosti

4.1 Glavni službenik za informacijsku sigurnost (CISO)

4.1.1 Vlasnik je ove politike i osigurava njezinu integraciju u sustav upravljanja informacijskom sigurnošću (ISMS).

4.1.2 Definira profil rizika organizacije i osigurava usklađenost s regulatornim zahtjevima i očekivanjima u pogledu kontrola.

4.2 Voditelj upravljanja ranjivostima / voditelj sigurnosnih operacija

4.2.1 Nadzire cjelokupne aktivnosti upravljanja ranjivostima i zakrpama.

4.2.2 Koordinira rasporede skeniranja, modele određivanja prioriteta i rokove otklanjanja.

4.2.3 Održava registar ranjivosti i surađuje u procjeni kompenzacijskih kontrola.

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

9. Zahtjevi za pregled i ažuriranje

9.1 Ova politika mora se pregledavati najmanje jednom godišnje ili nakon:

9.1.1 značajnih regulatornih izmjena (npr. izmjena DORA-e ili NIS2)

9.1.2 promjena u okvirima za određivanje prioriteta ranjivosti (npr. ažuriranja CVSS-a)

9.1.3 značajnih promjena IT okruženja (npr. migracija u oblak, opsežna promjena EDR-a)

9.1.4 povreda s visokim utjecajem ili vanjskih upozorenja koja zahtijevaju jačanje politike

9.2 Preglede provodi glavni službenik za informacijsku sigurnost (CISO) u suradnji sa sigurnosnim operacijama, upravljanjem rizicima i vodstvom infrastrukture.

9.3 Ažuriranja politike moraju biti:

9.3.1 dokumentirana u registru kontrole dokumenata ISMS-a

9.3.2 pregledana i odobrena od strane izvršnog rukovodstva

9.3.3 priopćena svim pogođenim dionicima, uključujući izvršitelje obrade trećih strana

9.4 Povijesne verzije moraju se sigurno čuvati za potrebe revizije i odgovornosti.

10. Povezane politike i poveznice

10.1 P1 - Politika informacijske sigurnosti. Utvrđuje krovnu obvezu zaštite sustava i podataka, što uključuje proaktivno upravljanje ranjivostima i osiguranje cjelovitosti softvera.

10.2 P5 - Politika upravljanja promjenama. Uređuje sva uvođenja zakrpa i prilagodbe konfiguracije te zahtijeva dokumentiranje, testiranje, odobravanje i postupke povrata koji nadopunjuju procese otklanjanja ranjivosti.

10.3 P6 - Politika upravljanja rizicima. Podupire klasifikaciju i obradu neotklonjenih ranjivosti putem strukturiranih procjena rizika, analize utjecaja i postupaka prihvaćanja preostalog rizika.

10.4 P12 - Politika upravljanja imovinom. Osigurava da su sustavi točno evidentirani i klasificirani, čime se omogućuju dosljedno skeniranje ranjivosti, dodjela vlasništva i pokrivenost zakrpavanja tijekom životnog ciklusa.

10.5 P22 - Politika bilježenja i praćenja. Definira zahtjeve za otkrivanje događaja i uspostavu revizijskog traga. Ova politika podupire vidljivost aktivnosti zakrpavanja, neovlaštenih promjena i pokušaja iskorištavanja poznatih ranjivosti.

10.6 P30 - Politika odgovora na incidente. Propisuje protokole eskalacije i strategije ograničavanja za iskorištene ranjivosti, istrage povreda i korektivne radnje usklađene s kontrolama iz ove politike.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001: Točka 8.1 - Operativno planiranje i kontrola: zahtijeva sustavno postupanje s tehničkim ranjivostima radi osiguravanja kontinuirane djelotvornosti sigurnosnih kontrola.

11.2 ISO/IEC 27002:2022 - Kontrole 8.8, 8.9, 5: pruža smjernice za provedbu zakrpavanja, skeniranja ranjivosti, cjelovitost softvera i integraciju sa sigurnom konfiguracijom i popisima imovine.

11.3 NIST SP 800-53 Rev.5: RA-5 - praćenje i skeniranje ranjivosti: propisuje učestala skeniranja i praćenje otklanjanja. SI-2 - otklanjanje nedostataka: zahtijeva pravodobnu procjenu i ublažavanje nedostataka dostupnim zakrpama ili drugim mjerama. CM-2 / CM-6 - bazne konfiguracije i kontrole upravljanja konfiguracijom: uspostavlja temelje za sigurne konfiguracije sustava povezane s provedbom zakrpavanja.

11.4 Uredba EU GDPR (2016/679): Članak 32 - sigurnost obrade: zahtijeva provedbu odgovarajućih tehničkih mjera, kao što su pravodobno zakrpavanje i obrada ranjivosti, radi osiguravanja povjerljivosti i otpornosti sustava. Uvodna izjava 49: potiče subjekte na provedbu preventivnih kontrola protiv poznatih prijetnji radi potpore sigurnosti i kontinuitetu.

11.5 Direktiva EU NIS2 (2022/2555): Članak 21(2)(d): obvezuje ključne i važne subjekte na otkrivanje, odgovor i ublažavanje ranjivosti sustava te održavanje visoke razine kibernetičke higijene.

11.6 Uredba EU DORA (2022/2554): Članak 8 - upravljanje IKT rizicima: zahtijeva identifikaciju i pravodobno otklanjanje ranjivosti u informacijskim i komunikacijskim tehnologijama koje se upotrebljavaju u financijskim sustavima. Članak 10(2)(f): naglašava kontinuirane procjene ranjivosti temeljene na prijetnjama i zakrpavanje kao dio operativne otpornosti.

11.7 COBIT 2019: DSS05.02 - upravljanje sigurnosnim ranjivostima: usmjerava organizacije na skeniranje, praćenje i ublažavanje poznatih tehničkih slabosti. DSS01.03 - praćenje infrastrukture: osigurava da se sustavi prate radi znakova iskorištavanja ili slabosti. MEA03 - praćenje, vrednovanje i procjena usklađenosti: zahtijeva redovitu reviziju djelotvornosti kontrola, uključujući status zakrpavanja i postupanje s iznimkama.