					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P39					Naziv dokumenta: **Politika koordinirane objave ranjivosti**							
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**

Usklađenost sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
GDPR EU	čl. 32(1)(d)	
Direktiva EU NIS2	čl. 21(2)(e)	
Uredba EU DORA	čl. 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Svrha

1.1 Uspostaviti formalan postupak za zaprimanje, obradu i objavu informacija o ranjivostima koje utječu na sustave ili usluge organizacije, u skladu sa zahtjevom iz članka 21. stavka 2. točke (e) Direktive NIS2 koji se odnosi na postupanje s ranjivostima i njihovu objavu.

1.2 Poticati vanjske sigurnosne istraživače, partnere i korisnike na odgovornu prijavu ranjivosti (Coordinated Vulnerability Disclosure - CVD) te definirati način na koji organizacija komunicira informacije o ranjivostima relevantnim dionicima.

2. Opseg

2.1 Ova politika primjenjuje se na sve mrežne i informacijske sustave u vlasništvu organizacije ili pod njezinim upravljanjem te na sve utvrđene ranjivosti u tim sustavima.

2.2 Obuhvaća interne timove (sigurnost, IT, razvoj) i sve vanjske strane koje prijavljuju ranjivosti (npr. istraživače, klijente, dobavljače). Također uređuje komunikaciju s dobavljačima proizvoda ili pružateljima usluga ako su njihove komponente uključene u ranjivost.

3. Ciljevi

3.1 Pravodobno otkrivati i otklanjati sigurnosne ranjivosti oslanjajući se na interne procjene i vanjske prijave.

3.2 Osigurati jasne smjernice vanjskim prijaviteljima za sigurno i zakonito dostavljanje informacija o ranjivostima te omogućiti organizaciji djelotvoran odgovor i sanaciju.

3.3 Osigurati usklađenost sa zahtjevima Direktive NIS2 i dobrom praksom u industriji (ISO/IEC 29147 i 30111) za koordiniranu objavu ranjivosti radi poboljšanja sigurnosti cjelokupnog ekosustava.

4. Uloge i odgovornosti

4.1 Tim za odgovor na ranjivosti (VRT): imenovani tim, pod vodstvom glavnog službenika za informacijsku sigurnost (CISO) ili voditelja upravljanja ranjivostima, koji zaprima i trijažira prijave ranjivosti, procjenjuje rizik i utjecaj te koordinira sanaciju i javnu objavu.

4.2 IT i razvojni timovi: surađuju s VRT-om radi provjere prijavljenih ranjivosti, razvoja i testiranja zakrpa ili mjera ublažavanja te uvođenja ispravaka. Po potrebi dostavljaju tehničke pojedinosti za sigurnosne obavijesti.

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

9. Praćenje i revizija

9.1 VRT mora voditi evidenciju objava ranjivosti u kojoj se prati svaka prijava od zaprimanja do zatvaranja. Ta se evidencija mora pregledavati mjesečno radi osiguravanja pravodobnog napretka po otvorenim stavkama. Stavke koje kasne moraju se eskalirati.

9.2 Unutarnja revizija ili neovisni procjenitelj sigurnosti jednom godišnje pregledava djelotvornost procesa postupanja s ranjivostima, primjerice provjerom jesu li uzorci slučajeva ranjivosti obrađeni u skladu s politikom (potvrđeni, ispravljeni i objavljeni pravodobno). Također provjeravaju je li javno dostupni kanal za objavu funkcionalan (npr. da se testne poruke e-pošte zaprime i da se po njima postupi).

9.3 Metrike o ranjivostima (broj prema ozbiljnosti, vrijeme sanacije i slično) sastavljaju se tromjesečno i predstavljaju odboru za upravljanje kibernetičkom sigurnošću radi ažuriranja procjene rizika.

10. Pregled i održavanje

10.1 Ova politika pregledava se najmanje jednom godišnje. Dodatno, svaka značajna promjena u našem IT okruženju (npr. pokretanje nove usluge izložene internetu) ili relevantan regulatorni razvoj (npr. novi propisi EU o objavi ranjivosti proizvoda) pokreće izvanredni pregled.

10.2 Ažuriranja politike uključuju povratne informacije vanjskih prijavitelja i naučene lekcije iz internih analiza nakon incidenata. Značajne promjene odobrava CISO te se one priopćavaju svim zaposlenicima i objavljuju u našem mrežnom repozitoriju sigurnosnih politika radi transparentnosti.

11. Povezane politike i poveznice

11.1 P01 – Politika informacijske sigurnosti. Upravljački mandat za postupanje s ranjivostima i njihovu objavu.

11.2 P19 – Politika upravljanja ranjivostima i zakrpama. Interni proces sanacije povezan sa zaprimanjem prijava kroz CVD.

11.3 P24 – Politika sigurnog razvoja. Osigurava ispravke i jačanje SDLC-a na temelju prijavljenih problema.

11.4 P25 – Politika zahtjeva sigurnosti aplikacija. Osigurava da proizvodi imaju sigurnosne zahtjeve spremne za objavu ranjivosti.

11.5 P30 – Politika odgovora na incidente. Obuhvaća aktivno iskorištavanje objavljenih ranjivosti.

11.6 P31 – Politika prikupljanja dokaza i forenzike. Čuva artefakte povezane s prijavljenim ili iskorištenim slabostima.

11.7 P26 – Politika sigurnosti trećih strana i dobavljača. Koordinira objave koje uključuju komponente dobavljača.

11.8 P37 – Politika pravne i regulatorne usklađenosti. Uređuje obavješćivanje, formulacije sigurne luke i objavu.

12. Reference

12.1 Direktiva NIS2 (EU 2022/2555), članak 21. stavak 2. točka (e) (sigurnost u razvoju te postupanje s ranjivostima i njihova objava)

12.2 Provedbena uredba Komisije (EU) 2024/2690, Prilog, odjeljak 6.10 (tehnički zahtjevi za postupke postupanja s ranjivostima i njihove objave)

12.3 ENISA tehničke smjernice o mjerama upravljanja kibernetičkim rizicima – odjeljak o postupanju s ranjivostima i njihovoj objavi

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (kontrola A.5.7 o obavještajnim podacima o prijetnjama i objavi ranjivosti; kontrola A.8.28 o sigurnom razvoju)

12.5 ISO/IEC 29147:2018 (smjernice za objavu ranjivosti) i ISO/IEC 30111:2019 (smjernice za postupke postupanja s ranjivostima)