					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P39					Naslov dokumenta: **Politika usklajenega razkrivanja ranljivosti**							
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	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	
Uredba (EU) GDPR	Člen 32(1)(d)	
Direktiva (EU) NIS2	Člen 21(2)(e)	
Uredba (EU) DORA	Člen 11(1)(d)	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Namen

1.1 Ta politika določa formalni postopek za prejem, obravnavo in razkrivanje informacij o ranljivostih, ki vplivajo na sisteme ali storitve organizacije, kot to zahteva člen 21(2)(e) Direktive (EU) NIS2 glede obravnave in razkrivanja ranljivosti.

1.2 Namen politike je spodbuditi zunanje varnostne raziskovalce, partnerje in uporabnike k odgovornemu prijavljanju ranljivosti (Coordinated Vulnerability Disclosure - CVD) ter določiti način, kako organizacija posreduje informacije o ranljivostih zainteresiranim stranem.

2. Področje uporabe

2.1 Ta politika se uporablja za vse omrežne in informacijske sisteme, ki so v lasti organizacije ali njenem upravljanju, ter za vse ugotovljene ranljivosti v teh sistemih.

2.2 Zajema notranje ekipe (informacijska varnost, IT, razvoj) in vse zunanje strani, ki prijavljajo ranljivosti (npr. raziskovalci, stranke, dobavitelji). Ureja tudi komunikacijo z dobavitelji produktov ali izvajalci storitev, kadar so njihove komponente vključene v ranljivost.

3. Cilji

3.1 Zagotoviti pravočasno zaznavanje in odpravo varnostnih ranljivosti z uporabo notranjih presoj in zunanjih razkritij.

3.2 Zagotoviti jasna navodila za zunanje prijavitelje za varno in zakonito predložitev informacij o ranljivostih ter za organizacijo za učinkovit odziv in odpravo pomanjkljivosti.

3.3 Zagotoviti usklajenost z zahtevami Direktive (EU) NIS2 in dobro prakso panoge (ISO/IEC 29147 in ISO/IEC 30111) za usklajeno razkrivanje ranljivosti ter s tem izboljšati splošno varnost ekosistema.

4. Vloge in odgovornosti

4.1 Skupina za odziv na ranljivosti (VRT): imenovana skupina, ki jo vodi vodja informacijske varnosti (CISO) ali vodja upravljanja ranljivosti, prejema prijave ranljivosti in izvaja njihovo triažo, ocenjuje tveganje in vpliv ter usklajuje odpravo in javno razkritje.

4.2 Ekipe IT in razvoja: sodelujejo z VRT pri preverjanju prijavljenih ranljivosti, razvoju in testiranju popravkov ali ukrepov za ublažitev ter uvajanju odpravkov. Po potrebi zagotovijo tehnične podrobnosti za varnostna obvestila.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Spremljanje in revizija

9.1 VRT mora voditi dnevnik razkritij ranljivosti, v katerem se spremlja vsaka prijava od prejema do zaključka. Ta dnevnik se pregleduje mesečno, da se zagotovi pravočasen napredek pri odprtih zadevah. Zapadle zadeve se eskalirajo.

9.2 Notranja revizija ali neodvisni presojevalec informacijske varnosti letno pregleda učinkovitost procesa obravnave ranljivosti, na primer s preverjanjem, ali so bili vzorčni primeri ranljivosti obravnavani skladno s politiko (potrjeni, odpravljeni, razkriti pravočasno). Preveri se tudi, ali javno dostopen kanal za razkritje deluje (npr. ali so testna e-sporočila prejeta in ustrezno obravnavana).

9.3 Kazalniki o ranljivostih (obseg po resnosti, časi odprave ipd.) se pripravljajo četrtletno in predstavijo odboru za upravljanje kibernetske varnosti za potrebe posodobitev ocene tveganj.

10. Pregled in vzdrževanje

10.1 Ta politika se pregleda najmanj enkrat letno. Dodatni pregled zunaj rednega cikla se sproži ob vsaki pomembni spremembi v našem IT-okolju (npr. uvedba nove storitve, izpostavljene internetu) ali pomembnem regulativnem razvoju (npr. nova zakonodaja EU glede razkrivanja ranljivosti produktov).

10.2 Posodobitve politike vključujejo povratne informacije zunanjih prijaviteljev in ugotovitve iz notranjih pregledov po incidentu. Večje spremembe odobri vodja informacijske varnosti (CISO), o njih pa se obvesti vse zaposlene; zaradi preglednosti se objavijo tudi v našem spletnem repozitoriju varnostnih politik.

11. Povezane politike in povezave

11.1 P01 – P01 Politika informacijske varnosti. Določa vodstveni mandat za obravnavo in razkrivanje ranljivosti.

11.2 P19 – Politika upravljanja ranljivosti in popravkov. Določa notranji postopek odprave, povezan s sprejemom prijav CVD.

11.3 P24 – Politika varnega razvoja. Zagotavlja odpravo pomanjkljivosti in utrjevanje SDLC na podlagi prijavljenih težav.

11.4 P25 – Politika zahtev informacijske varnosti za aplikacije. Zagotavlja, da imajo produkti varnostne zahteve, pripravljene za razkritje.

11.5 P30 – Politika odzivanja na incidente. Obravnava aktivno izkoriščanje razkritih ranljivosti.

11.6 P31 – Politika zbiranja dokazov in forenzike. Zagotavlja ohranjanje artefaktov prijavljenih ali izkoriščanih pomanjkljivosti.

11.7 P26 – Politika varnosti tretjih oseb in dobaviteljev. Usklajuje razkritja, ki vključujejo komponente dobaviteljev.

11.8 P37 – Politika pravne in regulativne skladnosti. Ureja obveščanje, besedilo varnega pristana in objavo.

12. Reference

12.1 Direktiva NIS2 ((EU) 2022/2555), člen 21(2), točka (e) (varnost pri razvoju ter obravnava in razkrivanje ranljivosti)

12.2 Izvedbena uredba Komisije (EU) 2024/2690, Priloga, oddelek 6.10 (tehnične zahteve glede procesov obravnave in razkrivanja ranljivosti)

12.3 Tehnične smernice ENISA o ukrepih za upravljanje tveganj kibernetske varnosti – oddelek o obravnavi in razkrivanju ranljivosti

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (kontrola A.5.7 o obveščevalnih podatkih o grožnjah in razkrivanju ranljivosti; kontrola A.8.28 o varnem razvoju)

12.5 ISO/IEC 29147:2018 (smernice za razkrivanje ranljivosti) in ISO/IEC 30111:2019 (smernice za procese obravnave ranljivosti)