					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P30					Naziv dokumenta: **Politika odgovora na incidente**							
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 8.1, točka 9	Strukturirani procesi za upravljanje rizicima i odgovor na incidente
ISO/IEC 27002:2022	Kontrole 5.25–5.27	Uloge, prijava, odgovor i poboljšanje povezani s incidentima
NIST SP 800-53 Rev.5	IR-1 do IR-9	Sveobuhvatan životni ciklus odgovora na incidente
GDPR EU	Članak 33. stavak 1., članak 33. stavak 3. točke (a)–(d), članak 34. stavak 1., članak 34. stavak 2. točke (a)–(c)	Rokovi za prijavu povreda, izvješćivanje i komunikacija s ispitanicima
Direktiva EU NIS2	Članak 23. stavci 1.–4.	Obavješćivanje nacionalnog nadležnog tijela i strukturirano izvješćivanje
Uredba EU DORA	Članak 17. stavci 1.–3.	Prijava velikih incidenata povezanih s IKT-om za financijske subjekte
COBIT 2019	DSS02, DSS04, MEA	Definira, prati i ocjenjuje upravljanje incidentima, kontinuitet i vrednovanje

1. Svrha

1.1 Ova politika uspostavlja formalni okvir za identifikaciju, prijavu, analizu, ograničavanje, odgovor, oporavak i vrednovanje nakon incidenta za incidente informacijske sigurnosti koji utječu na organizaciju.

1.2 Njome se osigurava pravodoban, koordiniran i učinkovit odgovor radi smanjenja operativnih poremećaja, financijskih gubitaka, reputacijske štete i neusklađenosti s regulatornim zahtjevima.

1.3 Politika također podupire kontinuirano poboljšavanje profila kibernetičke otpornosti organizacije kroz naučene lekcije i uključivanje nalaza nakon incidenta u upravljanje, alate i programe osposobljavanja.

2. Područje primjene

2.1 Ova politika primjenjuje se na:

2.1.1 svo osoblje, uključujući zaposlenike, ugovorne izvođače, konzultante i pružatelje usluga trećih strana

2.1.2 sve informacijske sustave, aplikacije, infrastrukturu, mreže i podatke, bilo u vlastitim prostorijama, u oblaku ili u hibridnim okruženjima

2.1.3 sve vrste sigurnosnih incidenata, uključujući, ali ne ograničavajući se na:

2.1.3.1 neovlašteni pristup ili eskalaciju privilegija

2.1.3.2 napade zlonamjernim softverom i ransomwareom

2.1.3.3 napade uskraćivanjem usluge (DoS/DDoS)

2.1.3.4 gubitak podataka, curenje podataka ili neovlašteno iznošenje podataka

2.1.3.5 zlouporabu od strane insajdera ili kršenja politike

2.1.3.6 povrede fizičke sigurnosti koje utječu na digitalnu imovinu

2.2 Ova politika obuhvaća otkrivanje, trijažu, istragu, eskalaciju, ograničavanje, postupanje s dokazima, obavješćivanje, oporavak i analizu osnovnog uzroka.

3. Ciljevi

3.1 Uspostaviti ponovljivu i skalabilnu sposobnost odgovora na incidente koja omogućuje brzo otkrivanje, klasifikaciju i ublažavanje sigurnosnih incidenata.

3.2 Smanjiti utjecaj sigurnosnih događaja na poslovanje kroz strukturirane postupke ograničavanja, uklanjanja prijetnje i oporavka sustava.

3.3 Osigurati da su prijava incidenata i odgovor na incidente usklađeni sa zakonskim, regulatornim i ugovornim zahtjevima, osobito onima koji se odnose na rokove za prijavu povreda i postupanje s dokazima.

3.4 Poduprijeti transparentnost i odgovornost kroz odgovarajuće evidentiranje, dokumentiranje i praćenje metrika za sve sigurnosne incidente.

3.5 Poticati kontinuirano poboljšavanje kroz preglede nakon incidenta, korektivne radnje i osposobljavanje dionika.

4. Uloge i odgovornosti

4.1 glavni direktor za informacijsku sigurnost (CISO)

4.1.1 Odgovoran je za okvir odgovora na incidente, osigurava provedbu politike i nadzire koordinaciju incidenata na razini cijele organizacije.

4.1.2 Djeluje kao glavna kontaktna točka prema regulatorima, vrhovnom vodstvu i vanjskom pravnom savjetniku tijekom incidenata visoke ozbiljnosti.

4.2 Koordinator odgovora na incidente

4.2.1 Koordinira međufunkcionalne timove za odgovor, upravlja tijekovima rada te prati status ograničavanja i oporavka.

4.2.2 Pokreće i vodi pregled nakon incidenta te osigurava da su korektivne radnje evidentirane i provedene.

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

9. Pregled i zahtjevi za ažuriranje

9.1 Ova politika mora se pregledavati najmanje jednom godišnje i prema potrebi revidirati radi uključivanja:

9.1.1 promjena u okruženju prijetnji, vrstama incidenata ili vektorima napada

9.1.2 naučenih lekcija iz većih incidenata, zamalo nastalih događaja ili regulatornih nalaza

9.1.3 ažuriranja primjenjivih zakona i propisa (npr. GDPR, DORA, NIS2)

9.1.4 povratnih informacija iz vježbi odgovora na incidente i pregleda nakon incidenta

9.2 CISO je odgovoran za pokretanje i koordinaciju postupka pregleda, uz savjetovanje s:

9.2.1.1 pravnim savjetnikom i DPO-om

9.2.1.2 SOC-om i IT operacijama

9.2.1.3 timovima za kontinuitet poslovanja i upravljanje rizicima

9.2.1.4 vrhovnim vodstvom

9.3 Promjene politike moraju biti:

9.3.1 dokumentirane u repozitoriju pod verzijskom kontrolom

9.3.2 priopćene svim zahvaćenim timovima i ažurirane u osposobljavanju za podizanje svijesti

9.3.3 provjerene kroz stolne ili praktične vježbe odgovora na incidente unutar tri mjeseca od odobrenja

9.4 Hitna ažuriranja potaknuta novim prijetnjama, nalazima revizije ili novim pravnim obvezama moraju se provesti bez odgode i evidentirati u povijesti izmjena politike.

10. Povezane politike i poveznice

10.1 Ovu politiku podupiru i s njom su povezane sljedeće organizacijske politike:

10.1.1 P1 – Politika informacijske sigurnosti: uspostavlja krovni zahtjev za poslovanje utemeljeno na riziku i spremnost za incidente.

10.1.2 P5 – Politika upravljanja promjenama: osigurava da aktivnosti ograničavanja i oporavka koje uključuju infrastrukturu ili usluge slijede formalne postupke.

10.1.3 P13 – Politika klasifikacije i označavanja podataka: podupire klasifikaciju ozbiljnosti incidenta na temelju osjetljivosti podataka.

10.1.4 P15 – Politika sigurnosnog kopiranja i vraćanja podataka: omogućuje oporavak od ransomwarea ili destruktivnih napada uz osiguranje cjelovitosti.

10.1.5 P18 – Politika kriptografskih kontrola: definira mjere šifriranja koje smanjuju učinak incidenta i rizike izloženosti podataka.

10.1.6 P22 – Politika evidentiranja događaja i praćenja: pruža temeljnu vidljivost događaja, upozoravanje i zadržavanje revizijskih zapisa potrebnih za učinkovito otkrivanje i forenziku.

10.1.7 P29 – Politika testnih podataka i testnog okruženja: osigurava da se i s incidentima koji utječu na neprodukcijske sustave postupa na strukturiran i siguran način.

10.1.8 P33 – Politika praćenja revizije i usklađenosti: potvrđuje spremnost za incidente i djelotvornost odgovora kroz strukturirane revizije i procjene usklađenosti.

11. Referentni standardi i okviri

11.1 ISO/IEC 27001: točka 8.1 – operativno planiranje i kontrola: strukturirani procesi za upravljanje rizicima i planiranje odgovora na incidente.

11.2 ISO/IEC 27002:2022 – kontrole 5.25–5.27: odgovornosti za upravljanje incidentima, prijavu, odgovor, komunikaciju i poboljšanje.

11.3 NIST SP 800-53 Rev.5: IR-1 do IR-9, AU-6, PL-2: sveobuhvatni zahtjevi za životni ciklus odgovora na incidente, reviziju i sigurnosno planiranje.

11.4 GDPR EU: članci 33. i 34.: obveze prijave nadzornim tijelima i zahtjevi za obavješćivanje ispitanika (uz definirane iznimke).

11.5 Direktiva EU NIS2 (2022/2555): članak 23.: obvezno nacionalno izvješćivanje, uz međuizvješća i završno izvješće.

11.6 Uredba EU DORA (2022/2554): članak 17.: zahtjevi za prijavu incidenata povezanih s IKT-om nadležnim tijelima za financijske institucije.

11.7 COBIT 2019: DSS02, DSS04, MEA01: upravljanje incidentima usluga i kontinuitetom, uz praćenje učinkovitosti i usklađenosti.