					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P31					Naziv dokumenta: **Politika prikupljanja dokaza i forenzike**							
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 5.25–5.27, 8	
ISO/IEC 27035:2016	Dijelovi 1 i 3	
NIST SP 800-53 Rev. 5	IR-1 do IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Forenzika mobilnih uređaja i medija	Forenzika mobilnih uređaja i medija
NIST SP 800-86	Integracija forenzičkih tehnika	Integracija forenzičkih tehnika u odgovor na incidente
GDPR EU	Članak 5, 33–34	
Direktiva EU NIS2	Članak 23(1)–(4)	
Uredba EU DORA	Članak 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Svrha

1.1 Ova politika uspostavlja strukturiran i pravno održiv okvir za identifikaciju, prikupljanje, očuvanje, analizu i zbrinjavanje digitalnih dokaza tijekom potvrđenih ili sumnjivih sigurnosnih incidenata.

1.2 Njome se osigurava da procesi forenzičke spremnosti i postupanja s dokazima:

1.2.1 održavaju cjelovitost dokaza i lanac nadzora

1.2.2 podupiru interne istrage, sudske postupke ili regulatorno izvješćivanje

1.2.3 budu usklađeni s međunarodno priznatim forenzičkim standardima i kriterijima pravne dopuštenosti

1.3 Ova politika podupire opredijeljenost organizacije za proaktivan odgovor na incidente, pravnu usklađenost i transparentno upravljanje, uz istodobno smanjenje operativnih poremećaja.

2. Opseg

2.1 Ova politika primjenjuje se na:

2.1.1 sve zaposlenike, ugovorne izvršitelje, dobavljače i pružatelje usluga koji sudjeluju u administraciji sustava, postupanju s incidentima ili istražnim aktivnostima

2.1.2 sve krajnje uređaje, poslužitelje, aplikacije, mreže i platforme u oblaku pod kontrolom organizacije ili u okviru ugovorene odgovornosti

2.1.3 svaki incident ili događaj koji zahtijeva postupanje s dokazima, uključujući:

2.1.3.1 insajderske prijetnje, povrede podataka ili istrage prijevare

2.1.3.2 zlouporabu sustava ili vjerodajnica

2.1.3.3 incidente povezane s operativnom tehnologijom (OT) ili industrijskim sustavima upravljanja

2.1.3.4 povrede fizičkog pristupa koje uključuju digitalnu imovinu

2.2 Ova politika uređuje i svaku interakciju s vanjskim forenzičkim uslugama ili tijelima kaznenog progona tijekom pravnih eskalacija ili regulatornih postupaka.

3. Ciljevi

3.1 Omogućiti brzo, sigurno i s politikom usklađeno prikupljanje dokaza tijekom sigurnosnih događaja ili istraga.

3.2 Očuvati cjelovitost, autentičnost i dopuštenost prikupljenih digitalnih dokaza primjenom stroge kontrole pristupa, zapisivanja događaja i postupaka provjere.

3.3 Osigurati da su sve forenzičke aktivnosti usklađene s pravnim i regulatornim obvezama, uključujući zaštitu podataka, radno pravo i ograničenja međunarodnog prijenosa.

3.4 Poduprijeti analizu nakon incidenta, utvrđivanje osnovnog uzroka i unaprjeđenje kontrola na temelju kvalitetnih forenzičkih nalaza.

3.5 Integrirati forenzičku spremnost u cjelokupni sustav upravljanja informacijskom sigurnošću (ISMS) radi potpore revizijama, obavješćivanju o povredama i donošenju odluka na razini rukovodstva.

4. Uloge i odgovornosti

4.1 glavni direktor informacijske sigurnosti (CISO)

4.1.1 Vlasnik je ove politike i osigurava da su sve forenzičke aktivnosti pravno održive, podložne reviziji i utemeljene na riziku.

4.1.2 Odobrava eskalaciju prema vanjskim pravnim subjektima i pružateljima forenzičkih usluga.

4.2 forenzički analitičari / osobe zadužene za odgovor na incidente

4.2.1 Vode prikupljanje, očuvanje i tehničku analizu dokaza.

4.2.2 Osiguravaju da se lanac nadzora ispravno evidentira i održava.

4.2.3 Dokumentiraju sve provedene radnje, nalaze i postavke alata korištene tijekom istraga.

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

9. Pregled i ažuriranje zahtjeva

9.1 Ova politika mora se pregledati najmanje jednom godišnje i ažurirati prema potrebi kako bi odražavala:

9.1.1 promjene zakona, propisa ili sudske prakse koje utječu na forenzičke postupke ili postupanje s podacima

9.1.2 ažuriranja industrijski priznatih forenzičkih standarda ili alata

9.1.3 naučene lekcije iz pregleda nakon incidenta, pravnih sporova ili nalaza revizije

9.1.4 tehnološke promjene platformi, uređaja ili sustava koji su predmet istrage

9.2 Za proces pregleda odgovoran je CISO i on mora uključivati savjetovanje sa sljedećim funkcijama:

9.2.1 pravna funkcija i funkcija usklađenosti

9.2.2 službenik za zaštitu podataka (DPO)

9.2.3 timovi sigurnosnih operacija i forenzike

9.2.4 unutarnja revizija

9.3 Sve izmjene moraju biti:

9.3.1 pod verzijskom kontrolom i pohranjene u repozitoriju politika

9.3.2 priopćene pogođenim dionicima, uključujući forenzičke timove i timove za odgovor

9.3.3 popraćene ažuriranjima relevantnih operativnih postupaka i materijala za osposobljavanje

9.4 Izvanredni pregledi moraju se pokrenuti nakon svakog kritičnog incidenta koji uključuje nepropisno postupanje s dokazima, prekid lanca nadzora ili probleme s pravnom dopuštenošću.

10. Povezane politike i poveznice

10.1 Ova politika usklađena je sa sljedećim organizacijskim politikama i njima je podržana:

10.1.1 P1 – Politika informacijske sigurnosti: uspostavlja temeljni mandat za istrage, kontrolu dokaza i usklađenost s primjenjivim propisima.

10.1.2 P5 – Politika upravljanja promjenama: osigurava da se sustavi koji su predmet istrage ne mijenjaju tijekom aktivnih forenzičkih postupaka.

10.1.3 P14 – Politika zadržavanja i zbrinjavanja podataka: uređuje sigurno zbrinjavanje i rokove zadržavanja dokaza i podataka povezanih s predmetom.

10.1.4 P18 – Politika kriptografskih kontrola: propisuje zahtjeve za šifriranje pri pohrani i prijenosu osjetljivih podataka ili podataka dokazne vrijednosti.

10.1.5 P22 – Politika zapisivanja događaja i praćenja: osigurava dostupnost dnevničkih zapisa događaja i telemetrije za prikupljanje dokaza i forenzičku korelaciju.

10.1.6 P30 – Politika odgovora na incidente: definira trijažu incidenata i putove eskalacije pri kojima se pokreću forenzički postupci.

10.1.7 P33 – Politika praćenja revizije i usklađenosti: provjerava pridržavanje forenzičkih protokola i zahtjeva lanca nadzora kroz redovite revizije.

11. Referentni standardi i okviri

11.1 Ova politika usklađena je s međunarodnim standardima forenzike i postupanja s incidentima te osigurava cjelovitost dokaza, pravnu održivost i usklađenost u različitim nadležnostima.

11.2 ISO/IEC 27001

11.2.1 Točka 8.1 – Podupire operativnu kontrolu forenzičke spremnosti i postupaka povezanih s dokazima

11.3 ISO/IEC 27002

11.3.1 Dodatak A, kontrola 5.25 – Odgovornosti za upravljanje incidentima: zahtijeva definirane uloge za postupanje s incidentima informacijske sigurnosti i istragama.

11.3.2 Dodatak A, kontrola 5.26 – Prijavljivanje događaja informacijske sigurnosti: podupire prikupljanje artefakata povezanih s događajima kao dokaza.

11.3.3 Dodatak A, kontrola 5.27 – Odgovor na incidente informacijske sigurnosti: propisuje strukturirano otklanjanje posljedica i istragu utemeljenu na dokazima.

11.3.4 Dodatak A, kontrola 8.27 – Siguran razvoj i forenzika (gdje je primjenjivo): obuhvaća zaštitu sustava i alata tijekom istraga.

11.4 ISO/IEC 27035:2016 (dijelovi 1 i 3)

11.4.1 Opisuje načela otkrivanja incidenata, odgovora i forenzičke spremnosti, uključujući planiranje, lanac nadzora i upravljanje dokazima incidenta.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 do IR-9, AU-6, PL-2: definira strukturirane zahtjeve za planiranje, otkrivanje, analizu, ograničavanje i odgovor na sigurnosne incidente. Podupire prikupljanje dokaza i mogućnost revizije dokaza (AU-6) te osigurava usklađenost s planovima sigurnosti i privatnosti sustava (PL-2) tijekom forenzičkih istraga.

11.6 NIST SP 800-86

11.6.1 Pruža smjernice za integraciju forenzičkih procesa u širi životni ciklus odgovora na incidente i osiguravanje forenzičke spremnosti.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Usmjeren je na najbolje prakse za prikupljanje, očuvanje i analizu digitalnih medija i dokaza s mobilnih uređaja na pravno održiv način.

11.8 GDPR EU (2016/679)

11.8.1 Članak 5 – Načela obrade osobnih podataka: primjenjuje se na dokaze koji sadržavaju osobne ili osjetljive podatke te osigurava minimizaciju i ograničenje svrhe.

11.8.2 Članci 33–34 – Obavješćivanje o povredi podataka: forenzički podaci podupiru usklađenost s obvezama prijave povrede i postupcima pravnog otkrivanja.

11.9 Direktiva EU NIS2 (2022/2555)

11.9.1 Članak 23 – Obveze prijavljivanja: forenzička dokumentacija i nalazi podupiru pravodobna i točna izvješća o incidentima nadležnim tijelima.

11.10 Uredba EU DORA (2022/2554)

11.10.1 Članak 17 – Prijavljivanje IKT incidenata: zahtijeva detaljnu analizu osnovnog uzroka i dokazne zapise o većim incidentima povezanima s IKT-om, osobito u financijskom sektoru.

11.11 COBIT 2019

11.11.1 DSS01.07 – Upravljanje sigurnosnim incidentima: nalaže dokumentiranje incidenata i temeljitost istrage.

11.11.2 DSS05.04 – Upravljanje sigurnosnim istragama: naglašava očuvanje digitalnih dokaza i potporu stegovnim i pravnim radnjama.