					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P31S					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 propisima

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 6.1, 6.3, 8	Planiranje temeljeno na riziku, aktivnosti poboljšavanja i operativne kontrole za očuvanje cjelovitosti dokaza
ISO/IEC 27002:2022	Kontrole 5.24–5.27	Smjernice za sigurno postupanje, preispitivanje nakon incidenta i poboljšavanja temeljena na dokazima
ISO/IEC 27035-3:2016	Točke 6.3, 6.4, 7	Osigurava pravilno planiranje, zakonito prikupljanje i sigurno postupanje s digitalnim dokazima uz dokumentiranje lanca nadzora
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Forenzička spremnost, zaštita revizijskih zapisa i učinkovita integracija u odgovor na incidente
GDPR EU	Članci 33, 34	Dokumentiranje i sljedivost povreda osobnih podataka
Direktiva EU NIS2	Članak 23	Sljedivo prijavljivanje incidenata i sigurno postupanje s dokazima
Uredba EU DORA	Članak 17(1), 17(2)	Osigurava prikupljanje, pohranu i zadržavanje dokaza za incidente povezane s IKT-om, forenzičku ispravnost i postupanje po zahtjevima regulatornih tijela
COBIT 2019	DSS05.06, DSS05.07	Pouzdano evidentiranje i strukturirano postupanje s dokazima radi sigurnih i revizijski provjerljivih istraga

1. Svrha

1.1. Ova politika definira način na koji organizacija postupa s digitalnim dokazima povezanima sa sigurnosnim incidentima, povredama podataka ili internim istragama. Njome se osigurava da se dokazi prikupljaju, pohranjuju i čuvaju na pravno valjan i revizijski spreman način, uz potporu internom odlučivanju i mogućim vanjskim postupanjima.

1.2. Ova politika omogućuje malim organizacijama zaštitu cjelovitosti dnevničkih zapisa, datoteka i slika sustava te dokazivanje dužne pažnje u skladu s normom ISO/IEC 27001, GDPR-om i povezanim standardima.

1.3. Politika podupire forenzičku spremnost bez potrebe za naprednim tehničkim resursima ili stalno zaposlenim IT timom, definiranjem jasnih odgovornosti, procesa i zahtjeva za zadržavanje.

2. Područje primjene

2.1. Ova politika primjenjuje se na:

2.1.1. sve zaposlenike, pružatelje IT usluga i vanjske konzultante uključene u odgovor na incidente, istragu ili analizu povrede

2.1.2. sve sustave društva, uključujući prijenosna računala, mobilne uređaje, poslužitelje, račune e-pošte, SaaS platforme i pohranu u oblaku (npr. Microsoft 365, Google Workspace)

2.1.3. svaki događaj koji zahtijeva dokaze za interne stegovne radnje, pravnu obranu, odštetne zahtjeve prema osiguratelju ili postupanje s regulatornim tijelima

2.2. To uključuje stvarne i sumnjive događaje povezane sa:

2.2.1. curenjem podataka

2.2.2. insajderskim prijetnjama ili zlouporabom

2.2.3. sigurnosnim incidentima (npr. zlonamjerni softver, neovlašteni pristup)

2.2.4. pritužbama klijenata koje zahtijevaju digitalnu provjeru

2.2.5. upitima regulatornih tijela ili tijela kaznenog progona

3. Ciljevi

3.1. Osigurati da se svi dokazi prikupljaju i obrađuju na način koji čuva njihovu cjelovitost, autentičnost i lanac nadzora.

3.2. Spriječiti slučajnu izmjenu, brisanje ili nepravilno postupanje s dnevničkim zapisima, datotekama ili slikama sustava koje mogu biti potrebne za istrage.

3.3. Uspostaviti dosljedan i revizijski provjerljiv pristup upravljanju dokazima koji ispunjava pravna i regulatorna očekivanja (npr. prijava povrede prema GDPR-u, sljedivost prema NIS2).

3.4. Definirati jasne uloge i odgovornosti radi brzog, sigurnog i pravno usklađenog prikupljanja dokaza tijekom sigurnosnih incidenata.

3.5. Poduprijeti forenzičku spremnost na razini SME organizacije uz smanjenje složenosti i izbjegavanje ometanja svakodnevnog poslovanja.

4. Uloge i odgovornosti

4.1. glavni direktor (GM)

4.1.1. Odobrava sve formalne istrage koje zahtijevaju prikupljanje dokaza.

4.1.2. Pregledava i odobrava izvješća o incidentima koja uključuju moguće pravne ili stegovne radnje.

4.1.3. Odlučuje je li potrebno obavijestiti vanjskog pravnog savjetnika ili regulatorna tijela.

4.1.4. Osigurava redovito preispitivanje i ažuriranje politike.

4.2. pružatelj IT usluga / administrator sustava

4.2.1. Prikuplja i čuva digitalne dokaze u skladu sa sigurnim postupcima.

4.2.2. Dokumentira vremenske oznake, pojedinosti o sustavu i korake postupanja.

4.2.3. Sve prikupljene materijale pohranjuje na zaštićenoj lokaciji.

4.2.4. Po potrebi pruža podršku forenzičkoj analizi.

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

9. Zahtjevi za pregled i ažuriranje

9.1. Godišnji pregled politike

9.1.1. Ovu politiku glavni direktor (GM) mora pregledati najmanje jednom svakih 12 mjeseci kako bi potvrdio:

9.1.1.1. usklađenost s kontrolama iz Dodatka A norme ISO/IEC 27001

9.1.1.2. trajnu relevantnost za aktualne digitalne platforme i IT usluge

9.1.1.3. primjerenost postupaka evidentiranja, zadržavanja dokaza i forenzičke spremnosti

9.2. Pokretački događaji za izmjenu politike

9.2.1. Politika se također mora pregledati i ažurirati nakon:

9.2.1.1. bilo kojeg većeg incidenta koji zahtijeva prikupljanje dokaza

9.2.1.2. neuspjele revizije ili regulatornog zahtjeva u kojem je dovedena u pitanje cjelovitost dokaza

9.2.1.3. uvođenja novih alata ili postupaka za odgovor na incidente ili nadzor sustava

9.2.1.4. pravnih promjena (npr. ažurirane smjernice za GDPR ili NIS2)

9.3. Odobravanje promjena i distribucija

9.3.1. Sve promjene mora pregledati i odobriti GM.

9.3.2. Ažurirana verzija mora se podijeliti sa:

9.3.2.1. pružateljima IT usluga i konzultantima uključenima u istrage

9.3.2.2. svim zaposlenicima sa zaduženjima administriranja sustava

9.3.3. Ažurirani primjerak mora se zadržati u arhivi politika društva i na zahtjev dostaviti revizorima.

10. Povezane politike i poveznice

10.1. Ova politika međuovisna je sa sljedećim politikama usklađenima za SME organizacije:

10.1.1. P2S – Politika uloga i odgovornosti u upravljanju: uspostavlja ovlasti nad istragama incidenata, odlukama o dokazima i pokretanjem pravnih postupaka.

10.1.2. P4S – Politika kontrole pristupa: osigurava da samo ovlašteno osoblje može pristupiti osjetljivim sustavima i dnevničkim zapisima tijekom istraga.

10.1.3. P22S – Politika evidentiranja događaja i nadzora: osigurava izvorne podatke koji se koriste kao forenzički dokazi te uspostavlja zahtjeve za zadržavanje, kontrolu pristupa i evidentiranje.

10.1.4. P30S – Politika odgovora na incidente: pokreće potrebu za prikupljanjem dokaza i definira operativni tijek koji vodi do forenzičkog očuvanja dokaza.

10.1.5. P17S – Politika zaštite podataka i privatnosti: osigurava da se svim osobnim podacima prikupljenima kao dokaz postupa zakonito u skladu s GDPR-om i povezanim propisima.

10.2. Ove politike zajedno podupiru pravnu dokazivost, cjelovitost istrage i punu revizijsku spremnost prema normi ISO/IEC 27001:2022.

11. Referentni standardi i okviri

11.1. ISO/IEC 27001

11.1.1. Točka 6.1 – Planiranje temeljeno na riziku uključuje spremnost za odgovor i postupke za dokaze.

11.1.2. Točka 6.3 – Podupire aktivnosti poboljšavanja na temelju dokaza iz incidenata.

11.1.3. Točka 8.1 – Zahtijeva operativne kontrole za cjelovitost dokaza.

11.2. ISO/IEC 27002

11.2.1. Kontrole 5.24–5.27 – Daju smjernice za sigurno postupanje, preispitivanje nakon incidenta i poboljšavanja temeljena na dokazima.

11.3. ISO/IEC 27035-3

11.3.1. Točke 6.3, 6.4 i 7.3 osiguravaju pravilno planiranje, zakonito prikupljanje i sigurno postupanje s digitalnim dokazima tijekom odgovora na incidente, uključujući očuvanje dokaza i dokumentiranje lanca nadzora.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 i AU-12 osiguravaju forenzičku spremnost, zaštitu revizijskih zapisa i učinkovitu integraciju prikupljanja dokaza u životni ciklus odgovora na incidente.

11.5. NIST SP 800-86

11.5.1. Definira najbolje prakse za pribavljanje, analizu i zaštitu digitalnih dokaza tijekom odgovora na incidente.

11.6. GDPR EU

11.6.1. Članci 33–34 – Zahtijevaju dokumentiranje i sljedivost incidenata i dokaza pri prijavljivanju povreda osobnih podataka.

11.7. Direktiva EU NIS2 (2022/2555)

11.7.1. Članak 23 – Zahtijeva sljedivo prijavljivanje incidenata i sigurno postupanje s dokazima za ključne i važne subjekte.

11.8. Uredba EU DORA

11.8.1. Članak 17(1) – Osigurava da se dokazi povezani s incidentima povezanima s IKT-om prikupljaju i pohranjuju na način koji podupire forenzičke istrage.

11.8.2. Članak 17(2) – Zahtijeva da financijski subjekti zadrže sve relevantne podatke i dnevničke zapise povezane sa sigurnosnim događajima, u skladu s forenzičkom ispravnošću i zahtjevima regulatornih tijela.

11.9. COBIT 2019

11.9.1. DSS05.06 – Pratiti, otkrivati i prijavljivati incidente: naglašava pouzdano evidentiranje radi potpore istragama.

11.9.2. DSS05.07 – Istražiti incidente i poduzeti radnje: zahtijeva strukturirano postupanje s dokazima kako bi se omogućile sigurne i revizijski provjerljive istrage.