					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P31S					Naslov dokumenta: **Politika zbiranja dokazov in forenzičnih preiskav**							
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	Klavzule 6.1, 6.3, 8	Načrtovanje na podlagi tveganj, izboljšave in operativne kontrole za zagotavljanje celovitosti dokazov
ISO/IEC 27002:2022	Kontrole 5.24–5.27	Usmerjajo varno ravnanje, preglede po incidentih in izboljšave na podlagi dokazov
ISO/IEC 27035-3:2016	Klavzule 6.3, 6.4, 7	Zagotavlja ustrezno načrtovanje, zakonito zbiranje in varno ravnanje z digitalnimi dokazi z dokumentirano verigo skrbništva
NIST SP 800-53 Rev. 5	IR-07, IR-08, AU-09, AU-12, PE-18	Forenzična pripravljenost, zaščita revizijskih sledi in učinkovita vključitev v odzivanje na incidente
Uredba EU GDPR	Člena 33, 34	Dokumentiranje in sledljivost pri kršitvah varnosti osebnih podatkov
Direktiva EU NIS2	Člen 23	Sledljivo poročanje o incidentih in varno ravnanje z dokazi
Uredba EU DORA	Člen 17(1), 17(2)	Zagotavlja zbiranje, shranjevanje in hrambo dokazov za incidente, povezane s sistemi IKT, forenzično neoporečnost in regulatorne poizvedbe
COBIT 2019	DSS05.06, DSS05.07	Zanesljivo beleženje in strukturirano ravnanje z dokazi za varne preiskave, primerne za revizijo

1. Namen

1.1. Ta politika določa, kako organizacija ravna z digitalnimi dokazi, povezanimi z varnostnimi incidenti, kršitvami varnosti osebnih podatkov ali notranjimi preiskavami. Zagotavlja, da se dokazi zbirajo, shranjujejo in ohranjajo na pravno ustrezen način ter na način, ki zagotavlja pripravljenost na revizijo, in da podpirajo notranje odločanje ter morebitne zunanje postopke.

1.2. Politika malim organizacijam omogoča varovanje celovitosti dnevnikov, datotek in posnetkov sistemov ter izkazovanje skrbnega ravnanja v skladu z ISO/IEC 27001, GDPR in povezanimi standardi.

1.3. Politika podpira forenzično pripravljenost brez potrebe po naprednih tehničnih virih ali stalno prisotni ekipi IT, saj določa jasne odgovornosti, postopke in zahteve glede hrambe.

2. Področje uporabe

2.1. Ta politika se uporablja za:

2.1.1. vse zaposlene, ponudnike IT-storitev in zunanje svetovalce, vključene v odzivanje na incidente, preiskave ali analizo kršitev,

2.1.2. vse sisteme podjetja, vključno s prenosniki, mobilnimi napravami, strežniki, e-poštnimi računi, platformami SaaS in hrambo v oblaku (npr. Microsoft 365, Google Workspace),

2.1.3. vsak dogodek, pri katerem so dokazi potrebni za notranje disciplinske ukrepe, pravno obrambo, zavarovalne zahtevke ali sodelovanje z regulatorjem.

2.2. To vključuje dejanske in sumljive dogodke, povezane z:

2.2.1. uhajanjem podatkov,

2.2.2. notranjimi grožnjami ali neprimerno uporabo,

2.2.3. varnostnimi kršitvami (npr. zlonamerna programska oprema, nepooblaščen dostop),

2.2.4. pritožbami strank, ki zahtevajo digitalno preverjanje,

2.2.5. poizvedbami regulatorjev ali organov pregona.

3. Cilji

3.1. Zagotoviti, da se vsi dokazi zbirajo in obravnavajo na način, ki ohranja njihovo celovitost, avtentičnost in verigo skrbništva.

3.2. Preprečiti nenamerne spremembe, izbris ali nepravilno ravnanje z dnevniki, datotekami ali posnetki sistemov, ki so lahko potrebni za preiskave.

3.3. Vzpostaviti dosleden in za revizijo primeren pristop k upravljanju dokazov, ki izpolnjuje pravne in regulativne zahteve (npr. prijava kršitve po GDPR, sledljivost po NIS2).

3.4. Določiti jasne vloge in odgovornosti za hitro, varno in pravno skladno zajemanje dokazov med varnostnimi incidenti.

3.5. Podpirati forenzično pripravljenost na ravni malih in srednjih podjetij ob hkratnem zmanjševanju kompleksnosti in brez motenj pri vsakodnevnem poslovanju.

4. Vloge in odgovornosti

4.1. Generalni direktor (GM)

4.1.1. Odobri vse formalne preiskave, ki zahtevajo zbiranje dokazov.

4.1.2. Pregleda in potrdi poročila o incidentih, ki vključujejo morebitne pravne ali disciplinske ukrepe.

4.1.3. Odloči, ali je treba obvestiti zunanjega pravnega svetovalca ali regulatorje.

4.1.4. Zagotovi redni pregled in posodabljanje politike.

4.2. Ponudnik IT-storitev / sistemski skrbnik

4.2.1. Zbira in ohranja digitalne dokaze v skladu z varnimi postopki.

4.2.2. Dokumentira časovne žige, podrobnosti o sistemu in korake ravnanja.

4.2.3. Vse zbrane materiale zavaruje na zaščiteni lokaciji.

4.2.4. Po potrebi pomaga pri forenzični analizi.

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

9. Zahteve za pregled in posodobitev

9.1. Letni pregled politike

9.1.1. To politiko mora najmanj enkrat v vsakih 12 mesecih pregledati generalni direktor (GM), da potrdi:

9.1.1.1. skladnost s kontrolami Priloge A standarda ISO/IEC 27001,

9.1.1.2. stalno relevantnost za trenutne digitalne platforme in IT-storitve,

9.1.1.3. ustreznost postopkov beleženja, hrambe dokazov in forenzične pripravljenosti.

9.2. Sprožilni dogodki za revizijo politike

9.2.1. Politiko je treba pregledati in posodobiti tudi po:

9.2.1.1. vsakem večjem incidentu, ki zahteva zbiranje dokazov,

9.2.1.2. neuspešni reviziji ali zahtevi regulatorja, pri kateri je bila pod vprašajem celovitost dokazov,

9.2.1.3. uvedbi novih orodij ali postopkov za odzivanje na incidente ali spremljanje sistemov,

9.2.1.4. pravnih spremembah (npr. posodobljene smernice GDPR ali NIS2).

9.3. Odobritev sprememb in distribucija

9.3.1. Vse spremembe mora pregledati in odobriti GM.

9.3.2. Posodobljena različica mora biti posredovana:

9.3.2.1. ponudnikom IT-storitev in svetovalcem, ki sodelujejo v preiskavah,

9.3.2.2. vsem zaposlenim z odgovornostmi sistemske administracije.

9.3.3. Posodobljena kopija mora biti hranjena v arhivu politik podjetja in na zahtevo posredovana presojevalcem.

10. Povezane politike in povezave

10.1. Ta politika je povezana z naslednjimi politikami, usklajenimi za mala in srednja podjetja:

10.1.1. P2S – Politika vlog in odgovornosti upravljanja: določa pooblastila za preiskave incidentov, odločitve o dokazih in pravno eskalacijo.

10.1.2. P4S – Politika nadzora dostopa: zagotavlja, da imajo med preiskavami dostop do občutljivih sistemov in dnevnikov samo pooblaščene osebe.

10.1.3. P22S – Politika beleženja in spremljanja: zagotavlja izvorne podatke, uporabljene kot forenzični dokazi, ter določa zahteve glede hrambe, nadzora dostopa in beleženja.

10.1.4. P30S – Politika odzivanja na incidente: sproži potrebo po zbiranju dokazov in določa operativni potek, ki vodi do forenzičnega zavarovanja.

10.1.5. P17S – Politika varstva podatkov in zasebnosti: zagotavlja, da se vsi osebni podatki, zbrani kot dokaz, obravnavajo zakonito v skladu z GDPR in povezanimi predpisi.

10.2. Te politike skupaj podpirajo pravno zagovornost, celovitost preiskav in celovito pripravljenost na revizijo po ISO/IEC 27001:2022.

11. Referenčni standardi in okviri

11.1. ISO/IEC 27001

11.1.1. Klavzula 6.1 – Načrtovanje na podlagi tveganj vključuje pripravljenost na odzivanje in postopke za dokaze.

11.1.2. Klavzula 6.3 – Podpira izboljšave na podlagi dokazov iz incidentov.

11.1.3. Klavzula 8.1 – Zahteva operativne kontrole za celovitost dokazov.

11.2. ISO/IEC 27002

11.2.1. Kontrole 5.24–5.27 – Usmerjajo varno ravnanje, preglede po incidentih in izboljšave na podlagi dokazov.

11.3. ISO/IEC 27035-3

11.3.1. Klavzule 6.3, 6.4 in 7.3 zagotavljajo ustrezno načrtovanje, zakonito zbiranje in varno ravnanje z digitalnimi dokazi med odzivanjem na incidente, vključno z ohranjanjem in dokumentiranjem verige skrbništva.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 in AU-12 zagotavljajo forenzično pripravljenost, zaščito revizijskih sledi in učinkovito vključitev zbiranja dokazov v življenjski cikel odzivanja na incidente.

11.5. NIST SP 800-86

11.5.1. Določa dobre prakse za zajem, analizo in zaščito digitalnih dokazov med odzivanjem na incidente.

11.6. Uredba EU GDPR

11.6.1. Člena 33–34 – zahtevata dokumentiranje in sledljivost incidentov ter dokazov pri prijavljanju kršitev varnosti osebnih podatkov.

11.7. Direktiva EU NIS2 (2022/2555)

11.7.1. Člen 23 – zahteva sledljivo poročanje o incidentih in varno ravnanje z dokazi za bistvene in pomembne subjekte.

11.8. Uredba EU DORA

11.8.1. Člen 17(1) – zagotavlja, da se dokazi, povezani z incidenti v zvezi s sistemi IKT, zbirajo in shranjujejo na način, ki podpira forenzične preiskave.

11.8.2. Člen 17(2) – zahteva, da finančni subjekti hranijo vse relevantne podatke in dnevnike, povezane z varnostnimi dogodki, skladno s forenzično neoporečnostjo in regulatornimi poizvedbami.

11.9. COBIT 2019

11.9.1. DSS05.06 – Spremljanje, zaznavanje in poročanje o incidentih: poudarja zanesljivo beleženje za podporo preiskavam.

11.9.2. DSS05.07 – Preiskava incidentov in ukrepanje: zahteva strukturirano ravnanje z dokazi za omogočanje varnih in za revizijo primernih preiskav.