| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vnesite naziv registrirane pravne osebe | | | | | | | |
| Številka dokumenta:<br>P31 | | | | | Naslov dokumenta:<br>**Politika zbiranja dokazov in digitalne forenzike** | | | | | | | |
| Različica:<br>1.0 | | Datum začetka veljavnosti:<br>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 | Klavzula 8 | |
| ISO/IEC 27002:2022 | Kontrole 5.25–5.27, 8 | |
| ISO/IEC 27035:2016 | Deli 1 in 3 | |
| NIST SP 800-53 Rev. 5 | IR-1 do IR-9, AU-6, PL-2 | |
| NIST SP 800-101 Rev. 1 | Forenzika mobilnih naprav in medijev | Forenzika mobilnih naprav in medijev |
| NIST SP 800-86 | Integracija forenzičnih tehnik | Integracija forenzičnih tehnik v odzivanje na incidente |
| Uredba EU GDPR | Člen 5, 33–34 | |
| Direktiva EU NIS2 | Člen 23(1)–(4) | |
| Uredba EU DORA | Člen 17(1)–(3) | |
| COBIT 2019 | DSS01.07, DSS05 | |

**1. Namen**

1.1 Ta politika vzpostavlja strukturiran in pravno vzdržen okvir za identifikacijo, zbiranje, ohranjanje, analizo in odstranitev digitalnih dokazov med dejanskimi ali domnevnimi varnostnimi incidenti.

**1.2 Zagotavlja, da procesi forenzične pripravljenosti in ravnanja z dokazi:**

1.2.1 ohranjajo celovitost dokazov in verigo skrbništva

1.2.2 podpirajo notranje preiskave, sodne postopke ali poročanje regulatorju

1.2.3 so usklajeni z mednarodno priznanimi forenzičnimi standardi in merili pravne dopustnosti

1.3 Politika podpira zavezanost organizacije k proaktivnemu odzivanju na incidente, pravni skladnosti in preglednosti upravljanja, ob hkratnem zmanjševanju operativnih motenj.

**2. Področje uporabe**

**2.1 Ta politika se uporablja za:**

2.1.1 vse zaposlene, pogodbene izvajalce, dobavitelje in ponudnike storitev, vključene v administracijo sistemov, obravnavo incidentov ali preiskovalne dejavnosti

2.1.2 vse končne točke, strežnike, aplikacije, omrežja in oblačne platforme pod nadzorom organizacije ali v njeni pogodbeni odgovornosti

**2.1.3 vsak incident ali dogodek, ki zahteva ravnanje z dokazi, vključno z:**

2.1.3.1 notranjimi grožnjami, kršitvami varnosti osebnih podatkov ali preiskavami goljufij

2.1.3.2 neustrezno uporabo sistemov ali poverilnic

2.1.3.3 incidenti v sistemih operativne tehnologije (OT) ali industrijskih krmilnih sistemih

2.1.3.4 kršitvami fizičnega dostopa, ki vključujejo digitalna sredstva

2.2 Politika ureja tudi vsako sodelovanje z zunanjimi forenzičnimi izvajalci ali organi pregona v okviru pravne eskalacije ali regulatornih postopkov.

**3. Cilji**

3.1 Omogočiti hitro, varno in s to politiko usklajeno pridobivanje dokazov med varnostnimi dogodki ali preiskavami.

3.2 Ohraniti celovitost, avtentičnost in pravno dopustnost zbranih digitalnih dokazov s strogim nadzorom dostopa, beleženjem in postopki preverjanja.

3.3 Zagotoviti, da so vse forenzične dejavnosti usklajene s pravnimi in regulatornimi obveznostmi, vključno z varstvom podatkov, delovnopravno zakonodajo in omejitvami mednarodnih prenosov.

3.4 Podpreti analizo po incidentu, ugotavljanje temeljnega vzroka in izboljševanje kontrol na podlagi kakovostnih forenzičnih rezultatov.

3.5 Vključiti forenzično pripravljenost v celotni sistem upravljanja informacijske varnosti (ISMS) ter s tem podpreti presoje, obvestila o kršitvah in odločanje izvršnega vodstva.

**4. Vloge in odgovornosti**

**4.1 Vodja informacijske varnosti (CISO)**

4.1.1 Je lastnik te politike in zagotavlja, da so vse forenzične dejavnosti pravno vzdržne, revizijsko sledljive in izvedene na podlagi tveganj.

4.1.2 Odobri eskalacijo do zunanjih pravnih subjektov in ponudnikov forenzičnih storitev.

**4.2 Forenzični analitiki / izvajalci obravnave incidentov**

4.2.1 Vodijo pridobivanje, ohranjanje in tehnično analizo dokazov.

4.2.2 Zagotavljajo, da je veriga skrbništva ustrezno evidentirana in vzdrževana.

4.2.3 Dokumentirajo vse ukrepe, ugotovitve in nastavitve orodij, uporabljene med preiskavami.

[ ... 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 Ta politika mora biti pregledana najmanj enkrat letno in po potrebi posodobljena, da odraža:**

9.1.1 spremembe zakonov, predpisov ali sodne prakse, ki vplivajo na forenzične postopke ali ravnanje s podatki

9.1.2 posodobitve panožno priznanih forenzičnih standardov ali naborov orodij

9.1.3 izkušnje, pridobljene pri pregledih po incidentu, pravnih sporih ali ugotovitvah presoje

9.1.4 tehnološke spremembe platform, naprav ali sistemov, ki so predmet preiskave

**9.2 Proces pregleda je v pristojnosti CISO in mora vključevati posvetovanje z:**

9.2.1 pravno službo in funkcijo skladnosti

9.2.2 pooblaščeno osebo za varstvo podatkov (DPO)

9.2.3 ekipami varnostnih operacij in forenzike

9.2.4 notranjo revizijo

**9.3 Vse revizije morajo biti:**

9.3.1 upravljane z različicami in shranjene v repozitoriju politik

9.3.2 sporočene prizadetim zainteresiranim stranem, vključno s forenzičnimi ekipami in ekipami za odzivanje

9.3.3 pospremljene s posodobitvami ustreznih operativnih postopkov in gradiv za usposabljanje

9.4 Vmesni pregledi se morajo sprožiti po vsakem kritičnem incidentu, ki vključuje neustrezno ravnanje z dokazi, prekinitev verige skrbništva ali težave s pravno dopustnostjo.

**10. Povezane politike in povezave**

**10.1 Ta politika je usklajena z naslednjimi organizacijskimi politikami in jih tudi podpira:**

10.1.1 P1 – Politika informacijske varnosti: določa temeljni mandat za preiskave, nadzor nad dokazi in skladnost z veljavno zakonodajo.

10.1.2 P5 – Politika upravljanja sprememb: zagotavlja, da se sistemi, ki so predmet preiskave, med aktivnimi forenzičnimi postopki ne spreminjajo.

10.1.3 P14 – Politika hrambe podatkov in odstranjevanja: ureja varno odstranjevanje in roke hrambe za dokaze in podatke, povezane s primerom.

10.1.4 P18 – Politika kriptografskih kontrol: določa zahteve glede šifriranja za hrambo in prenos občutljivih ali dokaznih podatkov.

10.1.5 P22 – Politika beleženja in spremljanja: zagotavlja razpoložljivost dnevnikov dogodkov in telemetrije za zbiranje dokazov in forenzično korelacijo.

10.1.6 P30 – Politika odzivanja na incidente: določa triažo incidentov in eskalacijske poti, pri katerih se sprožijo forenzični postopki.

10.1.7 P33 – Politika spremljanja presoje in skladnosti: z rednimi presojami preverja upoštevanje forenzičnih protokolov in zahtev glede verige skrbništva.

## 11. Referenčni standardi in okviri

11.1 Ta politika je usklajena z mednarodnimi standardi forenzike in obravnave incidentov ter zagotavlja celovitost dokazov, pravno vzdržnost in skladnost med jurisdikcijami.

### 11.2 ISO/IEC 27001

11.2.1 Klavzula 8.1 – podpira operativni nadzor forenzične pripravljenosti in postopkov ravnanja z dokazi

### 11.3 ISO/IEC 27002

11.3.1 Dodatek A, kontrola 5.25 – Odgovornosti za upravljanje incidentov: zahteva opredeljene vloge za obravnavo incidentov informacijske varnosti in preiskav.

11.3.2 Dodatek A, kontrola 5.26 – Poročanje o dogodkih informacijske varnosti: podpira zbiranje artefaktov, povezanih z dogodki, kot dokazov.

11.3.3 Dodatek A, kontrola 5.27 – Odzivanje na incidente informacijske varnosti: zahteva strukturirano odpravo pomanjkljivosti in preiskavo na podlagi dokazov.

11.3.4 Dodatek A, kontrola 8.27 – Varna arhitektura in inženirska načela (kjer je ustrezno): obravnava zaščito sistemov in orodij med preiskavami.

### 11.4 ISO/IEC 27035:2016 (deli 1 in 3)

11.4.1 Opredeljuje načela odkrivanja incidentov, odzivanja in forenzične pripravljenosti, vključno z načrtovanjem, verigo skrbništva in upravljanjem dokazov incidenta.

### 11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 do IR-9, AU-6, PL-2: določa strukturirane zahteve za načrtovanje, zaznavanje, analizo, zajezitev in odzivanje na varnostne incidente. Podpira zbiranje dokazov in njihovo revizijsko preverljivost (AU-6) ter zagotavlja usklajenost z načrti varnosti in zasebnosti sistemov (PL-2) med forenzičnimi preiskavami.

### 11.6 NIST SP 800-86

11.6.1 Podaja smernice za vključevanje forenzičnih procesov v širši življenjski cikel odzivanja na incidente in za zagotavljanje forenzične pripravljenosti.

### 11.7 NIST SP 800-101 Rev. 1

11.7.1 Osredotoča se na dobre prakse za pridobivanje, ohranjanje in analizo digitalnih medijev ter dokazov z mobilnih naprav na pravno vzdržen način.

### 11.8 Uredba EU GDPR (2016/679)

11.8.1 Člen 5 – Načela v zvezi z obdelavo osebnih podatkov: uporablja se za dokaze, ki vsebujejo osebne ali občutljive podatke, ter zagotavlja minimizacijo in omejitev namena.

11.8.2 Člena 33–34 – Obvestilo o kršitvi varnosti osebnih podatkov: forenzični podatki podpirajo skladnost z obveznostmi obveščanja o kršitvah in postopki pravnega razkritja.

**11.9 Direktiva EU NIS2 (2022/2555)**

11.9.1 Člen 23 – Obveznosti poročanja: forenzična dokumentacija in ugotovitve podpirajo pravočasna in natančna poročila o incidentih pristojnim organom.

**11.10 Uredba EU DORA (2022/2554)**

11.10.1 Člen 17 – Poročanje o IKT-incidentih: zahteva podrobne evidence temeljnega vzroka in dokaznega gradiva o večjih incidentih, povezanih z IKT, zlasti v finančnem sektorju.

**11.11 COBIT 2019**

11.11.1 DSS01.07 – Upravljanje varnostnih incidentov: zahteva dokumentiranje incidentov in ustrezno preiskovalno skrbnost.

11.11.2 DSS05.04 – Upravljanje varnostnih preiskav: poudarja ohranjanje digitalnih dokazov in podporo disciplinskim ter pravnim ukrepom.