					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P31					Dokumenta nosaukums: **Pierādījumu vākšanas un digitālās kriminālistikas politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Juridiskais paziņojums (autortiesības un lietošanas ierobežojumi)
(C) 2025 Clarysec LLC. All rights reserved.

Šis dokuments ir Clarysec LLC intelektuālais īpašums. Nevienu šī dokumenta daļu nedrīkst kopēt, atkārtoti izmantot, izplatīt vai grozīt komerciāliem vai ieviešanas nolūkiem bez iepriekšējas skaidras rakstiskas atļaujas.
Neautorizēta lietošana ir stingri aizliegta un var izraisīt tiesvedību.
Par licencēšanu sazinieties: info@clarysec.com

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	
ISO/IEC 27002:2022	Kontroles pasākumi 5.25–5.27, 8	
ISO/IEC 27035:2016	1. un 3. daļa	
NIST SP 800-53 Rev. 5	IR-1 līdz IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Mobilo ierīču un datu nesēju digitālā kriminālistika	Mobilo ierīču un datu nesēju digitālā kriminālistika
NIST SP 800-86	Digitālās kriminālistikas paņēmienu integrēšana	Digitālās kriminālistikas paņēmienu integrēšana incidentu reaģēšanā
ES VDAR	5. pants, 33.–34. pants	
ES NIS2	23. panta 1.–4. daļa	
ES DORA	17. panta 1.–3. daļa	
COBIT 2019	DSS01.07, DSS05	

1. Mērķis

1.1 Šī politika nosaka strukturētu un juridiski pamatotu ietvaru digitālo pierādījumu identificēšanai, vākšanai, saglabāšanai, analīzei un iznīcināšanai faktisku vai iespējamu drošības incidentu laikā.

1.2 Tā nodrošina, ka kriminālistiskās gatavības un pierādījumu apstrādes procesi:

1.2.1 saglabā pierādījumu integritāti un pierādījumu aprites ķēdi

1.2.2 atbalsta iekšējās izmeklēšanas, tiesvedību vai regulatīvo ziņošanu

1.2.3 atbilst starptautiski atzītiem digitālās kriminālistikas standartiem un juridiskās pieļaujamības kritērijiem

1.3 Šī politika atbalsta organizācijas apņemšanos nodrošināt proaktīvu incidentu reaģēšanu, tiesisko atbilstību un pārvaldības caurskatāmību, vienlaikus samazinot darbības traucējumus.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem darbiniekiem, līgumslēdzējiem, piegādātājiem un pakalpojumu sniedzējiem, kuri iesaistīti sistēmu administrēšanā, incidentu apstrādē vai izmeklēšanas darbībās

2.1.2 visām galiekārtām, serveriem, lietojumprogrammām, tīkliem un mākoņplatformām, kas ir organizācijas kontrolē vai līgumiskajā atbildībā

2.1.3 jebkuru incidentu vai notikumu, kam nepieciešama pierādījumu apstrāde, tostarp:

2.1.3.1 iekšējo apdraudējumu, personas datu aizsardzības pārkāpumu vai krāpšanas izmeklēšanu

2.1.3.2 sistēmu vai autentifikācijas datu ļaunprātīgu vai neatļautu izmantošanu

2.1.3.3 operatīvo tehnoloģiju (OT) vai industriālās vadības incidentus

2.1.3.4 fiziskās piekļuves pārkāpumus, kas skar digitālos aktīvus

2.2 Šī politika nosaka arī kārtību sadarbībai ar trešo pušu digitālās kriminālistikas pakalpojumu sniedzējiem vai tiesībaizsardzības iestādēm, ja notiek materiālu nodošana juridiskai rīcībai vai regulatīvajām procedūrām.

3. Mērķi

3.1 Nodrošināt ātru, drošu un politikai atbilstošu pierādījumu iegūšanu drošības notikumu vai izmeklēšanu laikā.

3.2 Saglabāt savākto digitālo pierādījumu integritāti, autentiskumu un pieļaujamību, stingri kontrolējot piekļuvi, žurnalēšanu un verifikācijas procedūras.

3.3 Nodrošināt, ka visas digitālās kriminālistikas darbības tiek koordinētas ar tiesiskajiem un regulatīvajiem pienākumiem, tostarp personas datu aizsardzības, darba tiesību un starptautiskās datu pārsūtīšanas ierobežojumu prasībām.

3.4 Atbalstīt pēcincidenta analīzi, pamatcēloņa noteikšanu un kontroles pasākumu pilnveidošanu, izmantojot augstas kvalitātes digitālās kriminālistikas rezultātus.

3.5 Integrēt kriminālistisko gatavību kopējā informācijas drošības pārvaldības sistēmā, atbalstot auditus, paziņošanu par pārkāpumiem un izpildvadības lēmumu pieņemšanu.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO)

4.1.1 ir šīs politikas īpašnieks un nodrošina, ka visas digitālās kriminālistikas darbības ir juridiski pamatotas, auditējamas un balstītas uz riska izvērtējumu

4.1.2 autorizē eskalāciju uz ārējām juridiskajām institūcijām un digitālās kriminālistikas pakalpojumu sniedzējiem

4.2 Digitālās kriminālistikas analītiķi / incidentu apstrādes speciālisti

4.2.1 veic pierādījumu iegūšanu, saglabāšanu un tehnisko analīzi

4.2.2 nodrošina, ka pierādījumu aprites ķēde tiek pienācīgi reģistrēta un uzturēta

4.2.3 dokumentē visas darbības, konstatējumus un izmeklēšanā izmantoto rīku iestatījumus

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata vismaz reizi gadā un jāatjaunina pēc nepieciešamības, lai atspoguļotu:

9.1.1 izmaiņas normatīvajos aktos, regulējumā vai judikatūrā, kas ietekmē digitālās kriminālistikas procedūras vai datu apstrādi

9.1.2 izmaiņas nozarē atzītos digitālās kriminālistikas standartos vai rīku kopās

9.1.3 mācības, kas gūtas pēcincidenta pārskatīšanā, juridiskos strīdos vai audita konstatējumos

9.1.4 tehnoloģiskās izmaiņas platformās, ierīcēs vai sistēmās, par kurām notiek izmeklēšana

9.2 Pārskatīšanas procesa īpašnieks ir CISO, un tajā jāiekļauj konsultēšanās ar:

9.2.1 juridisko un atbilstības funkciju

9.2.2 datu aizsardzības speciālistu (DPO)

9.2.3 drošības operāciju un digitālās kriminālistikas komandām

9.2.4 iekšējo auditu

9.3 Visi grozījumi:

9.3.1 jāpārvalda ar versiju kontroli un jāglabā politiku repozitorijā

9.3.2 jāpaziņo ietekmētajām iesaistītajām pusēm, tostarp digitālās kriminālistikas un reaģēšanas komandām

9.3.3 jāpapildina ar atbilstošiem darbības procedūru un apmācību materiālu atjauninājumiem

9.4 Starpposma pārskatīšana jāierosina pēc jebkura kritiska incidenta, kas saistīts ar neatbilstošu rīcību ar pierādījumiem, pierādījumu aprites ķēdes pārtrūkumu vai juridiskās pieļaujamības problēmām.

10. Saistītās politikas un sasaiste

10.1 Šī politika ir saskaņota ar šādām organizācijas politikām un tās atbalsta:

10.1.1 P1 – Informācijas drošības politika: nosaka pamatprasības izmeklēšanai, pierādījumu kontrolei un piemērojamo normatīvo aktu ievērošanai.

10.1.2 P5 – Izmaiņu pārvaldības politika: nodrošina, ka sistēmas, par kurām notiek izmeklēšana, aktīvu digitālās kriminālistikas procesu laikā netiek izmainītas.

10.1.3 P14 – Datu uzglabāšanas politika un Datu iznīcināšanas politika: nosaka drošas iznīcināšanas kārtību un glabāšanas termiņus pierādījumiem un ar lietām saistītajiem datiem.

10.1.4 P18 – Kriptogrāfisko kontroles pasākumu politika: nosaka šifrēšanas prasības sensitīvu datu vai pierādījumu datu glabāšanai un pārsūtīšanai.

10.1.5 P22 – Žurnalēšanas un uzraudzības politika: nodrošina notikumu žurnālu un telemetrijas datu pieejamību pierādījumu vākšanai un digitālās kriminālistikas korelācijai.

10.1.6 P30 – Incidentu reaģēšanas politika: nosaka incidentu triāžas un eskalācijas ceļus, kuros tiek aktivizētas digitālās kriminālistikas procedūras.

10.1.7 P33 – Audita un atbilstības uzraudzības politika: ar regulāru auditu palīdzību validē atbilstību digitālās kriminālistikas protokoliem un pierādījumu aprites ķēdes prasībām.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiskajiem digitālās kriminālistikas un incidentu apstrādes standartiem, nodrošinot pierādījumu integritāti, juridisko pamatojumu un atbilstību dažādās jurisdikcijās.

11.2 ISO/IEC 27001

11.2.1 8. punkts – atbalsta kriminālistiskās gatavības un pierādījumu procedūru darbības kontroli

11.3 ISO/IEC 27002

11.3.1 A pielikuma 5.25. kontrole – pienākumi incidentu pārvaldībā: nosaka nepieciešamību definēt lomas informācijas drošības incidentu un izmeklēšanu apstrādei.

11.3.2 A pielikuma 5.26. kontrole – ziņošana par informācijas drošības notikumiem: atbalsta ar notikumiem saistītu artefaktu vākšanu kā pierādījumus.

11.3.3 A pielikuma 5.27. kontrole – reaģēšana uz informācijas drošības incidentiem: nosaka strukturētu, uz pierādījumiem balstītu trūkumu novēršanu un izmeklēšanu.

11.3.4 A pielikuma 8.27. kontrole – droša izstrāde un digitālā kriminālistika (ja piemērojams): attiecas uz sistēmu un rīku aizsardzību izmeklēšanu laikā.

11.4 ISO/IEC 27035:2016 (1. un 3. daļa)

11.4.1 Nosaka incidentu atklāšanas, reaģēšanas un kriminālistiskās gatavības principus, tostarp plānošanu, pierādījumu aprites ķēdi un ar incidentiem saistīto pierādījumu pārvaldību.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 līdz IR-9, AU-6, PL-2: nosaka strukturētas prasības drošības incidentu plānošanai, atklāšanai, analīzei, ierobežošanai un reaģēšanai. Atbalsta pierādījumu vākšanu un auditējamību (AU-6), kā arī nodrošina saskaņotību ar sistēmu drošības un privātuma plāniem (PL-2) digitālās kriminālistikas izmeklēšanās.

11.6 NIST SP 800-86

11.6.1 Sniedz vadlīnijas digitālās kriminālistikas procesu integrēšanai plašākā incidentu reaģēšanas dzīves ciklā un kriminālistiskās gatavības nodrošināšanai.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Koncentrējas uz labāko praksi digitālo datu nesēju un mobilo ierīču pierādījumu iegūšanā, saglabāšanā un analīzē juridiski pamatotā veidā.

11.8 ES VDAR (2016/679)

11.8.1 5. pants – principi, kas attiecas uz personas datu apstrādi: attiecas uz pierādījumiem, kas satur personas datus vai sensitīvus datus, nodrošinot datu minimizēšanu un mērķa ierobežojumu.

11.8.2 33.–34. pants – paziņošana par personas datu aizsardzības pārkāpumu: digitālās kriminālistikas dati atbalsta atbilstību pienākumiem ziņot par pārkāpumiem un tiesiskās izpaušanas procesiem.

11.9 ES NIS2 direktīva (2022/2555)

11.9.1 23. pants – ziņošanas pienākumi: digitālās kriminālistikas dokumentācija un konstatējumi atbalsta savlaicīgus un precīzus incidentu ziņojumus kompetentajām iestādēm.

11.10 ES DORA (2022/2554)

11.10.1 17. pants – ziņošana par IKT incidentiem: prasa detalizētus pamatcēloņa un pierādījumu ierakstus par būtiskiem ar IKT saistītiem incidentiem, īpaši finanšu nozarē.

11.11 COBIT 2019

11.11.1 DSS01.07 – drošības incidentu pārvaldība: nosaka incidentu dokumentēšanu un rūpīgu izmeklēšanu.

11.11.2 DSS05.04 – drošības izmeklēšanu pārvaldība: uzsver digitālo pierādījumu saglabāšanu un atbalstu disciplinārām un tiesiskām darbībām.