					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P31S					Dokumenta nosaukums: **Digitālo pierādījumu iegūšanas un datorforensikas 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**

Saskaņots ar piemērojamajiem standartiem un normatīvo regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	6.1., 6.3. un 8. punkts	Uz risku balstīta plānošana, pilnveides pasākumi un darbības kontroles pierādījumu integritātes nodrošināšanai
ISO/IEC 27002:2022	5.24.–5.27. kontroles pasākumi	Nosaka drošu apstrādi, pēcincidenta pārskatīšanu un uz pierādījumiem balstītus uzlabojumus
ISO/IEC 27035-3:2016	6.3., 6.4. un 7. punkts	Nodrošina pienācīgu plānošanu, likumīgu digitālo pierādījumu iegūšanu un drošu apstrādi, izmantojot glabāšanas ķēdes dokumentāciju
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Datorforensiskā gatavība, audita žurnālu aizsardzība un efektīva integrācija incidentu reaģēšanā
EU GDPR	33. un 34. pants	Dokumentācija un izsekojamība personas datu aizsardzības pārkāpumu gadījumos
EU NIS2	23. pants	Izsekojama ziņošana par incidentiem un droša pierādījumu apstrāde
EU DORA	17(1), 17(2) pants	Nodrošina ar IKT saistītu incidentu pierādījumu iegūšanu, saglabāšanu un glabāšanu, datorforensisko pamatotību un reaģēšanu uz regulatoru pieprasījumiem
COBIT 2019	DSS05.06, DSS05.07	Uzticama žurnālfiksēšana un strukturēta pierādījumu apstrāde drošai un auditējamai izmeklēšanai

1. Mērķis

1.1. Šī politika nosaka, kā organizācija apstrādā digitālos pierādījumus, kas saistīti ar drošības incidentiem, personas datu aizsardzības pārkāpumiem vai iekšējām izmeklēšanām. Tā nodrošina, ka pierādījumi tiek iegūti, glabāti un saglabāti juridiski pamatotā un auditam gatavā veidā, atbalstot gan iekšējo lēmumu pieņemšanu, gan iespējamās ārējās darbības.

1.2. Politika ļauj mazām organizācijām aizsargāt žurnālu, datņu un sistēmu attēlu integritāti, vienlaikus apliecinot pienācīgu rūpību atbilstoši ISO/IEC 27001, GDPR un saistītajiem standartiem.

1.3. Tā atbalsta datorforensisko gatavību, neprasot sarežģītus tehniskos resursus vai pilna laika IT komandu, nosakot skaidrus pienākumus, procesus un glabāšanas prasības.

2. Piemērošanas joma

2.1. Šī politika attiecas uz:

2.1.1. visiem darbiniekiem, IT pakalpojumu sniedzējiem un ārējiem konsultantiem, kuri iesaistīti incidentu reaģēšanā, izmeklēšanā vai pārkāpumu analīzē

2.1.2. visām uzņēmuma sistēmām, tostarp klēpjdatoriem, mobilajām ierīcēm, serveriem, e-pasta kontiem, SaaS platformām un mākoņkrātuvēm (piemēram, Microsoft 365, Google Workspace)

2.1.3. jebkuru notikumu, kurā nepieciešami pierādījumi disciplinārai rīcībai organizācijas ietvaros, juridiskajai aizstāvībai, apdrošināšanas prasībām vai saziņai ar regulatoriem

2.2. Tā ietver gan faktiskus, gan iespējami notikušus gadījumus, kas saistīti ar:

2.2.1. datu noplūdi

2.2.2. iekšējo apdraudējumu vai neatbilstošu lietošanu

2.2.3. drošības pārkāpumiem (piemēram, ļaunatūru, neatļautu piekļuvi)

2.2.4. klientu sūdzībām, kurām nepieciešama digitāla validācija

2.2.5. regulatoru vai tiesībaizsardzības iestāžu pieprasījumiem

3. Mērķi

3.1. Nodrošināt, ka visi pierādījumi tiek iegūti un apstrādāti tā, lai saglabātu to integritāti, autentiskumu un glabāšanas ķēdi.

3.2. Novērst nejaušu žurnālu, datņu vai sistēmu attēlu modificēšanu, dzēšanu vai neatbilstošu apstrādi, ja tie var būt nepieciešami izmeklēšanai.

3.3. Nodrošināt konsekventu un auditējamu pieeju pierādījumu pārvaldībai, kas atbilst tiesiskajām un regulatīvajām prasībām (piemēram, GDPR paziņošanai par pārkāpumu, NIS2 izsekojamības prasībām).

3.4. Noteikt skaidras lomas un pienākumus, lai drošības incidentu laikā nodrošinātu ātru, drošu un tiesiski atbilstošu pierādījumu fiksēšanu.

3.5. Atbalstīt MVU līmeņa datorforensisko gatavību, vienlaikus mazinot sarežģītību un nepieļaujot traucējumus ikdienas darbībā.

4. Lomas un pienākumi

4.1. ģenerāldirektors (GM)

4.1.1. apstiprina visas formālās izmeklēšanas, kurām nepieciešama pierādījumu iegūšana.

4.1.2. pārskata un apstiprina incidentu ziņojumus, kas saistīti ar iespējamām juridiskām darbībām vai disciplinārpasākumiem.

4.1.3. pieņem lēmumu par ārējā juridiskā konsultanta vai regulatoru informēšanas nepieciešamību.

4.1.4. nodrošina regulāru politikas pārskatīšanu un atjaunināšanu.

4.2. IT pakalpojumu sniedzējs / sistēmu administrators

4.2.1. iegūst un saglabā digitālos pierādījumus atbilstoši drošām procedūrām.

4.2.2. dokumentē laikspiedolus, sistēmas informāciju un apstrādes soļus.

4.2.3. nodrošina visu iegūto materiālu glabāšanu aizsargātā vietā.

4.2.4. ja nepieciešams, sniedz atbalstu datorforensiskajā analīzē.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Ikgadējā politikas pārskatīšana

9.1.1. Šī politika ģenerāldirektoram (GM) jāpārskata vismaz reizi 12 mēnešos, lai apstiprinātu:

9.1.1.1. atbilstību ISO/IEC 27001 A pielikuma kontroles pasākumiem

9.1.1.2. pastāvīgu atbilstību aktuālajām digitālajām platformām un IT pakalpojumiem

9.1.1.3. žurnālfiksēšanas, pierādījumu glabāšanas un datorforensiskās gatavības procedūru pietiekamību

9.2. Politikas pārskatīšanas ierosinātāji

9.2.1. Politika jāpārskata un jāatjaunina arī pēc:

9.2.1.1. jebkura būtiska incidenta, kam nepieciešama pierādījumu iegūšana

9.2.1.2. neveiksmīga audita vai regulatora pieprasījuma, ja tika apšaubīta pierādījumu integritāte

9.2.1.3. jaunu rīku vai procedūru ieviešanas incidentu reaģēšanai vai sistēmu uzraudzībai

9.2.1.4. tiesisko prasību izmaiņām (piemēram, atjauninātām GDPR vai NIS2 vadlīnijām)

9.3. Izmaiņu apstiprināšana un izplatīšana

9.3.1. Visas izmaiņas pārskata un apstiprina GM.

9.3.2. Atjauninātā versija jāizplata:

9.3.2.1. IT pakalpojumu sniedzējiem un konsultantiem, kas iesaistīti izmeklēšanās

9.3.2.2. jebkuram personālam ar sistēmu administrēšanas pienākumiem

9.3.3. Atjaunināta kopija jāsaglabā uzņēmuma politiku arhīvā un pēc pieprasījuma jāiesniedz auditoriem.

10. Saistītās politikas un sasaiste

10.1. Šī politika ir savstarpēji saistīta ar šādām MVU vajadzībām pielāgotām politikām:

10.1.1. P2S – Pārvaldības lomu un atbildības politika: nosaka pilnvaras incidentu izmeklēšanā, lēmumu pieņemšanā par pierādījumiem un nodošanā juridiskai izvērtēšanai.

10.1.2. P4S – Piekļuves kontroles politika: nodrošina, ka izmeklēšanas laikā sensitīvām sistēmām un žurnāliem piekļūst tikai pilnvarots personāls.

10.1.3. P22S – Žurnālfiksēšanas un uzraudzības politika: nodrošina ievaddatus, kas tiek izmantoti kā datorforensiskie pierādījumi, un nosaka glabāšanas, piekļuves kontroles un žurnālfiksēšanas prasības.

10.1.4. P30S – Incidentu reaģēšanas politika: nosaka nepieciešamību iegūt pierādījumus un darbību plūsmu, kas nodrošina datorforensisku saglabāšanu.

10.1.5. P17S – Datu aizsardzības un privātuma politika: nodrošina, ka visi kā pierādījumi iegūtie personas dati tiek apstrādāti likumīgi saskaņā ar GDPR un saistītajiem normatīvajiem aktiem.

10.2. Šīs politikas kopā nodrošina juridisko pamatojumu, izmeklēšanas integritāti un pilnīgu gatavību ISO/IEC 27001:2022 auditam.

11. Atsauces standarti un ietvari

11.1. ISO/IEC 27001

11.1.1. 6.1. punkts – uz risku balstīta plānošana ietver gatavību reaģēšanai un pierādījumu procedūras.

11.1.2. 6.3. punkts – atbalsta pilnveides pasākumus, pamatojoties uz incidentu pierādījumiem.

11.1.3. 8.1. punkts – nosaka darbības kontroles pierādījumu integritātes nodrošināšanai.

11.2. ISO/IEC 27002

11.2.1. 5.24.–5.27. kontroles pasākumi – nosaka drošu apstrādi, pēcincidenta pārskatīšanu un uz pierādījumiem balstītus uzlabojumus.

11.3. ISO/IEC 27035-3

11.3.1. 6.3., 6.4. un 7.3. punkts – nodrošina pienācīgu plānošanu, likumīgu digitālo pierādījumu iegūšanu un drošu apstrādi incidentu reaģēšanas laikā, tostarp saglabāšanu un glabāšanas ķēdes dokumentēšanu.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 un AU-12 nodrošina datorforensisko gatavību, audita žurnālu aizsardzību un efektīvu pierādījumu iegūšanas integrāciju incidentu reaģēšanas dzīves ciklā

11.5. NIST SP 800-86

11.5.1. Nosaka labāko praksi digitālo pierādījumu iegūšanai, analīzei un aizsardzībai incidentu reaģēšanas laikā.

11.6. EU GDPR

11.6.1. 33.–34. pants – nosaka prasību dokumentēt incidentus un nodrošināt pierādījumu izsekojamību, ziņojot par personas datu aizsardzības pārkāpumiem.

11.7. EU NIS2 direktīva (2022/2555)

11.7.1. 23. pants – nosaka izsekojamu ziņošanu par incidentiem un drošu pierādījumu apstrādi būtiskām un svarīgām struktūrām.

11.8. EU DORA

11.8.1. 17(1) pants – nodrošina, ka ar IKT saistītu incidentu pierādījumi tiek iegūti un glabāti tādā veidā, kas atbalsta datorforensisko izmeklēšanu.

11.8.2. 17(2) pants – nosaka, ka finanšu iestādēm jāsaglabā visi attiecīgie dati un žurnāli, kas saistīti ar drošības notikumiem, ievērojot datorforensisko pamatotību un regulatoru pieprasījumus.

11.9. COBIT 2019

11.9.1. DSS05.06 – incidentu uzraudzība, atklāšana un ziņošana: uzsver uzticamas žurnālfiksēšanas nozīmi izmeklēšanas atbalstam.

11.9.2. DSS05.07 – incidentu izmeklēšana un rīcība: nosaka strukturētu pierādījumu apstrādi, lai nodrošinātu drošu un auditējamu izmeklēšanu.