					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P31S					Dokumenttitel: **Politik for bevisindsamling og it-forensik**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og lovkrav

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1, 6.3, 8	Risikobaseret planlægning, forbedringstiltag og operationelle kontroller for bevismaterialets integritet
ISO/IEC 27002:2022	Kontroller 5.24–5.27	Vejleder i sikker håndtering, efterhændelsesgennemgange og forbedringer baseret på bevismateriale
ISO/IEC 27035-3:2016	Klausul 6.3, 6.4, 7	Sikrer korrekt planlægning, lovlig indsamling og sikker håndtering af digitale beviser med dokumentation af chain of custody
NIST SP 800-53 Rev. 5	IR-07, IR-08, AU-09, AU-12, PE-18	It-forensisk beredskab, beskyttelse af revisionslogfiler og effektiv integration i hændelseshåndtering
EU GDPR	Artikel 33, 34	Dokumentation og sporbarhed ved brud på persondatasikkerheden
EU NIS2	Artikel 23	Sporbar rapportering af hændelser og sikker håndtering af bevismateriale
EU DORA	Artikel 17(1), 17(2)	Sikrer indsamling, lagring og opbevaring af bevismateriale ved IKT-relaterede hændelser, forensisk forsvarlighed og regulatoriske forespørgsler
COBIT 2019	DSS05.06, DSS05.07	Pålidelig logning og struktureret håndtering af bevismateriale til sikre og revisionsbare undersøgelser

1. Formål

1.1. Denne politik fastlægger, hvordan organisationen håndterer digitale beviser relateret til sikkerhedshændelser, brud på persondatasikkerheden eller interne undersøgelser. Den sikrer, at bevismateriale indsamles, lagres og bevares på en juridisk forsvarlig og revisionsklar måde, som understøtter både intern beslutningstagning og eventuelle eksterne tiltag.

1.2. Politikken gør det muligt for mindre virksomheder at beskytte integriteten af logfiler, filer og systemimages, samtidig med at rettidig omhu kan dokumenteres efter ISO/IEC 27001, GDPR og relaterede standarder.

1.3. Den understøtter it-forensisk beredskab uden krav om avancerede tekniske ressourcer eller et fuldtidsbemandet it-team ved at fastlægge klare ansvarsområder, processer og krav til opbevaring.

2. Omfang

2.1. Denne politik gælder for:

2.1.1. Alle medarbejdere, it-leverandører og eksterne konsulenter, der er involveret i hændelseshåndtering, undersøgelse eller analyse af brud

2.1.2. Alle virksomhedens systemer, herunder bærbare computere, mobile enheder, servere, e-mailkonti, SaaS-platforme og cloudlagring (f.eks. Microsoft 365, Google Workspace)

2.1.3. Enhver hændelse, der kræver bevismateriale til interne disciplinære tiltag, juridisk forsvar, forsikringskrav eller dialog med tilsynsmyndigheder

2.2. Dette omfatter både faktiske og formodede hændelser, der involverer:

2.2.1. datalækage

2.2.2. insidertrusler eller misbrug

2.2.3. sikkerhedsbrud (f.eks. malware, uautoriseret adgang)

2.2.4. kundeklager, der kræver digital validering

2.2.5. henvendelser fra tilsynsmyndigheder eller retshåndhævende myndigheder

3. Mål

3.1. Sikre, at alt bevismateriale indsamles og håndteres på en måde, der opretholder dets integritet, autenticitet og chain of custody.

3.2. Forebygge utilsigtet ændring, sletning eller fejlhåndtering af logfiler, filer eller systemimages, som kan være nødvendige for undersøgelser.

3.3. Etablere en ensartet og revisionsbar tilgang til håndtering af bevismateriale, der opfylder juridiske og regulatoriske forventninger (f.eks. GDPR-underretning om brud og sporbarhed efter NIS2).

3.4. Fastlægge klare roller og ansvar for at sikre hurtig, sikker og juridisk forsvarlig indsamling af bevismateriale under sikkerhedshændelser.

3.5. Understøtte it-forensisk beredskab på SMV-niveau med mindst mulig kompleksitet og uden unødige forstyrrelser af den daglige drift.

4. Roller og ansvar

4.1. Direktør (GM)

4.1.1. Godkender alle formelle undersøgelser, der kræver indsamling af bevismateriale.

4.1.2. Gennemgår og godkender hændelsesrapporter, der omfatter potentielle juridiske eller disciplinære tiltag.

4.1.3. Afgør, om ekstern juridisk rådgiver eller tilsynsmyndigheder skal underrettes.

4.1.4. Sikrer, at politikken gennemgås og opdateres regelmæssigt.

4.2. Ekstern it-tjenesteudbyder/systemadministrator

4.2.1. Indsamler og bevarer digitale beviser i overensstemmelse med sikre procedurer.

4.2.2. Dokumenterer tidsstempler, systemoplysninger og håndteringstrin.

4.2.3. Sikrer alt indsamlet materiale i et beskyttet lagringsområde.

4.2.4. Bistår med it-forensisk analyse, hvis det er nødvendigt.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1. Årlig gennemgang af politikken

9.1.1. Denne politik skal gennemgås mindst én gang hver 12. måned af direktøren (GM) for at bekræfte:

9.1.1.1. overensstemmelse med kontroller i ISO/IEC 27001 Annex A

9.1.1.2. fortsat relevans for aktuelle digitale platforme og it-tjenester

9.1.1.3. tilstrækkeligheden af procedurer for logning, opbevaring af bevismateriale og it-forensisk beredskab

9.2. Udløsende forhold for revision af politikken

9.2.1. Politikken skal også gennemgås og opdateres efter:

9.2.1.1. enhver større hændelse, der kræver indsamling af bevismateriale

9.2.1.2. en ikke-bestået revision eller regulatorisk forespørgsel, hvor integriteten af bevismateriale blev draget i tvivl

9.2.1.3. indførelse af nye værktøjer eller procedurer til hændelseshåndtering eller systemovervågning

9.2.1.4. juridiske ændringer (f.eks. opdateret vejledning til GDPR eller NIS2)

9.3. Godkendelse og distribution af ændringer

9.3.1. Alle ændringer skal gennemgås og godkendes af direktøren.

9.3.2. Den opdaterede version skal deles med:

9.3.2.1. it-leverandører og konsulenter, der deltager i undersøgelser

9.3.2.2. alle medarbejdere med ansvar for systemadministration

9.3.3. En opdateret kopi skal opbevares i virksomhedens politikarkiv og deles med revisorer efter anmodning.

10. Relaterede politikker og sammenhænge

10.1. Denne politik er indbyrdes afhængig af følgende SME-tilpassede politikker:

10.1.1. P2S – Politik for styringsroller og ansvarsområder: Fastlægger beføjelser i forbindelse med hændelsesundersøgelser, beslutninger om bevismateriale og juridisk eskalering.

10.1.2. P4S – Politik for adgangskontrol: Sikrer, at kun autoriseret personale kan få adgang til følsomme systemer og logfiler under undersøgelser.

10.1.3. P22S – Lognings- og overvågningspolitik: Leverer de rå data, der anvendes som it-forensisk bevismateriale, og fastlægger krav til opbevaring, adgangsstyring og logning.

10.1.4. P30S – Politik for hændelseshåndtering: Udløser behovet for indsamling af bevismateriale og fastlægger det operationelle forløb frem mod forensisk bevaring.

10.1.5. P17S – Databeskyttelses- og privatlivspolitik: Sikrer, at personoplysninger, som indsamles som bevismateriale, håndteres lovligt efter GDPR og relaterede regler.

10.2. Disse politikker understøtter samlet set juridisk forsvarlighed, undersøgelsens integritet og fuldt revisionsberedskab i forhold til ISO/IEC 27001:2022.

11. Referencestandarder og rammeværker

11.1. ISO/IEC 27001

11.1.1. Klausul 6.1 – Risikobaseret planlægning omfatter beredskab for respons og procedurer for bevismateriale.

11.1.2. Klausul 6.3 – Understøtter forbedringstiltag baseret på bevismateriale fra hændelser.

11.1.3. Klausul 8.1 – Kræver operationelle kontroller for bevismaterialets integritet.

11.2. ISO/IEC 27002

11.2.1. Kontroller 5.24–5.27 – Vejleder i sikker håndtering, efterhændelsesgennemgange og forbedringer baseret på bevismateriale.

11.3. ISO/IEC 27035-3

11.3.1. Klausul 6.3, 6.4 og 7.3 skal sikre korrekt planlægning, lovlig indsamling og sikker håndtering af digitale beviser under hændelseshåndtering, herunder bevaring og dokumentation af chain of custody.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 og AU-12 sikrer it-forensisk beredskab, beskyttelse af revisionslogfiler og effektiv integration af bevisindsamling i hændelseshåndteringens livscyklus.

11.5. NIST SP 800-86

11.5.1. Definerer bedste praksis for indsamling, analyse og beskyttelse af digitale beviser under hændelseshåndtering.

11.6. EU GDPR

11.6.1. Artikel 33–34 – Kræver dokumentation og sporbarhed af hændelser og bevismateriale ved indberetning af brud på persondatasikkerheden.

11.7. EU NIS2-direktivet (2022/2555)

11.7.1. Artikel 23 – Kræver sporbar rapportering af hændelser og sikker håndtering af bevismateriale for væsentlige og vigtige enheder.

11.8. EU DORA

11.8.1. Artikel 17(1) – Sikrer, at bevismateriale relateret til IKT-relaterede hændelser indsamles og lagres på en måde, der understøtter it-forensiske undersøgelser.

11.8.2. Artikel 17(2) – Kræver, at finansielle enheder opbevarer alle relevante data og logfiler i forbindelse med sikkerhedshændelser i overensstemmelse med forensisk forsvarlighed og regulatoriske forespørgsler.

11.9. COBIT 2019

11.9.1. DSS05.06 – Overvåg, detektér og rapportér hændelser: Fremhæver pålidelig logning til understøttelse af undersøgelser.

11.9.2. DSS05.07 – Undersøg og reager på hændelser: Kræver struktureret håndtering af bevismateriale for at muliggøre sikre og revisionsbare undersøgelser.