					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P31					Dokumenttitel: **Politik for indsamling af bevismateriale og digital efterforskning**						
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 regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	
ISO/IEC 27002:2022	Kontroller 5.25–5.27, 8	
ISO/IEC 27035:2016	Del 1 og 3	
NIST SP 800-53 Rev. 5	IR-1 til IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Digital efterforskning af mobile enheder og medier	Digital efterforskning af mobile enheder og medier
NIST SP 800-86	Integration af efterforskningsteknikker	Integration af efterforskningsteknikker i hændelseshåndtering
EU GDPR	Artikel 5, 33–34	
EU NIS2	Artikel 23(1)–(4)	
EU DORA	Artikel 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Formål

1.1 Denne politik fastlægger en struktureret og juridisk forsvarlig ramme for identifikation, indsamling, bevaring, analyse og bortskaffelse af digitale beviser ved faktiske eller mistænkte sikkerhedshændelser.

1.2 Den sikrer, at processer for efterforskningsberedskab og håndtering af bevismateriale:

1.2.1 Opretholder bevismaterialets integritet og chain of custody

1.2.2 Understøtter interne undersøgelser, retssager eller rapportering til myndigheder

1.2.3 Er tilpasset internationalt anerkendte standarder for digital efterforskning og kriterier for retlig antagelighed

1.3 Politikken understøtter organisationens forpligtelse til proaktiv hændelseshåndtering, lovmæssig efterlevelse og gennemsigtighed i styringen, samtidig med at driftsforstyrrelser minimeres.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle medarbejdere, kontrahenter, leverandører og tjenesteudbydere, der udfører systemadministration, hændelseshåndtering eller undersøgelsesaktiviteter

2.1.2 Alle slutpunkter, servere, applikationer, netværk og cloudplatforme under organisationens kontrol eller kontraktmæssige ansvar

2.1.3 Enhver hændelse eller begivenhed, der kræver håndtering af bevismateriale, herunder:

2.1.3.1 Insidertrusler, brud på persondatasikkerheden eller undersøgelser af svig

2.1.3.2 Misbrug af systemer eller legitimationsoplysninger

2.1.3.3 Hændelser i operationel teknologi (OT) eller industrielle kontrolsystemer

2.1.3.4 Overtrædelser af fysisk adgang, der involverer digitale aktiver

2.2 Politikken regulerer også enhver interaktion med tredjepartsleverandører af efterforskningstjenester eller retshåndhævende myndigheder ved juridisk eskalering eller myndighedsprocedurer.

3. Mål

3.1 At muliggøre hurtig, sikker og politikafstemt indsamling af bevismateriale ved sikkerhedshændelser eller undersøgelser.

3.2 At bevare integriteten, autenticiteten og antageligheden af indsamlede digitale beviser gennem stram styring af adgang, logning og verifikationsprocedurer.

3.3 At sikre, at alle efterforskningsaktiviteter koordineres med juridiske og regulatoriske forpligtelser, herunder databeskyttelse, arbejdsret og begrænsninger for internationale overførsler.

3.4 At understøtte analyse efter hændelser, fastlæggelse af rodårsag og forbedring af kontroller gennem efterforskningsresultater af høj kvalitet.

3.5 At integrere efterforskningsberedskab i det samlede ledelsessystem for informationssikkerhed (ISMS) som støtte for revisioner, underretning om brud og ledelsesmæssige beslutninger.

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO)

4.1.1 Er ansvarlig for denne politik og sikrer, at alle efterforskningsaktiviteter er juridisk forsvarlige, revisionssporbare og risikobaserede.

4.1.2 Godkender eskalering til eksterne juridiske instanser og leverandører af efterforskningstjenester.

4.2 Efterforskningsanalytikere / hændelseshåndterere

4.2.1 Leder indsamling, bevaring og teknisk analyse af bevismateriale.

4.2.2 Sikrer, at chain of custody registreres korrekt og opretholdes.

4.2.3 Dokumenterer alle handlinger, konstateringer og værktøjsindstillinger, der anvendes under undersøgelser.

[... 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 Denne politik skal gennemgås mindst én gang årligt og opdateres efter behov for at afspejle:

9.1.1 Ændringer i love, regler eller retspraksis, der påvirker efterforskningsprocedurer eller datahåndtering

9.1.2 Opdateringer af brancheanerkendte standarder eller værktøjer til digital efterforskning

9.1.3 Erfaringer fra efterhændelsesgennemgange, retstvister eller revisionskonstateringer

9.1.4 Teknologiske ændringer i platforme, enheder eller systemer, der er omfattet af undersøgelsen

9.2 Gennemgangsprocessen ejes af CISO og skal omfatte høring af:

9.2.1 Juridisk afdeling og Compliance

9.2.2 Databeskyttelsesrådgiveren (DPO)

9.2.3 Sikkerhedsdrift og efterforskningsteams

9.2.4 Intern Revision

9.3 Alle revisioner skal:

9.3.1 Være versionsstyrede og opbevares i politikrepositoryet

9.3.2 Kommunikeres til berørte interessenter, herunder efterforsknings- og responsteams

9.3.3 Ledsages af opdateringer til relevante driftsprocedurer og træningsmaterialer

9.4 Midlertidige gennemgange skal iværksættes efter enhver kritisk hændelse, der involverer fejlhåndtering af bevismateriale, svigt i chain of custody eller problemer med retlig antagelighed.

10. Relaterede politikker og sammenhænge

10.1 Denne politik er tilpasset følgende organisatoriske politikker og understøttes af dem:

10.1.1 P1 – Informationssikkerhedspolitik: Fastlægger det grundlæggende mandat for undersøgelse, styring af bevismateriale og efterlevelse af gældende lovgivning.

10.1.2 P5 – Politik for ændringsstyring: Sikrer, at systemer under undersøgelse ikke ændres under aktive efterforskningsprocesser.

10.1.3 P14 – Dataopbevarings- og bortskaffelsespolitik: Regulerer sikker bortskaffelse og opbevaringsfrister for bevismateriale og sagsrelaterede data.

10.1.4 P18 – Politik for kryptografiske kontroller: Fastlægger krav til kryptering ved opbevaring og overførsel af følsomme data eller bevisdata.

10.1.5 P22 – Lognings- og overvågningspolitik: Sikrer tilgængelighed af hændelseslogfiler og telemetri til indsamling af bevismateriale og retsmedicinsk korrelation.

10.1.6 P30 – Politik for hændelseshåndtering: Fastlægger hændelsestriage og eskalationsveje, hvor efterforskningsprocedurer iværksættes.

10.1.7 P33 – Politik for revision og overvågning af efterlevelse: Validerer efterlevelse af efterforskningsprotokoller og chain-of-custody-krav gennem regelmæssige revisioner.

11. Referencestandarder og rammeværker

11.1 Denne politik er tilpasset internationale standarder for digital efterforskning og hændelseshåndtering og sikrer bevismaterialets integritet, juridisk forsvarlighed og efterlevelse på tværs af jurisdiktioner.

11.2 ISO/IEC 27001

11.2.1 Klausul 8.1 – Understøtter operationel styring af efterforskningsberedskab og procedurer for bevismateriale

11.3 ISO/IEC 27002

11.3.1 Bilag A, kontrol 5.25 – Ansvar for hændelsesstyring: Kræver definerede roller for håndtering af informationssikkerhedshændelser og undersøgelser.

11.3.2 Bilag A, kontrol 5.26 – Rapportering af informationssikkerhedshændelser: Understøtter indsamling af hændelsesrelaterede artefakter som bevismateriale.

11.3.3 Bilag A, kontrol 5.27 – Respons på informationssikkerhedshændelser: Kræver struktureret afhjælpning og undersøgelse baseret på bevismateriale.

11.3.4 Bilag A, kontrol 8.27 – Sikker udvikling og digital efterforskning, hvor relevant: Omhandler beskyttelse af systemer og værktøjer under undersøgelser.

11.4 ISO/IEC 27035:2016 (del 1 og 3)

11.4.1 Beskriver principperne for hændelsesdetektion, respons og efterforskningsberedskab, herunder planlægning, chain of custody og styring af bevismateriale ved hændelser.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 til IR-9, AU-6, PL-2: Definerer strukturerede krav til planlægning, detektion, analyse, inddæmning og respons på sikkerhedshændelser. Understøtter indsamling og revisionssporbarhed af bevismateriale (AU-6) og sikrer overensstemmelse med planer for systemsikkerhed og databeskyttelse (PL-2) under efterforskningsundersøgelser.

11.6 NIST SP 800-86

11.6.1 Giver vejledning om integration af efterforskningsprocesser i den bredere livscyklus for hændelseshåndtering og om at sikre efterforskningsberedskab.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Fokuserer på bedste praksis for indsamling, bevaring og analyse af digitale medier og bevismateriale fra mobile enheder på en juridisk forsvarlig måde.

11.8 EU GDPR (2016/679)

11.8.1 Artikel 5 – Principper for behandling af personoplysninger: Gælder for bevismateriale, der indeholder personoplysninger eller følsomme data, og sikrer dataminimering og formålsbegrænsning.

11.8.2 Artikel 33–34 – Underretning om brud på persondatasikkerheden: Efterforskningsdata understøtter efterlevelse af forpligtelser til anmeldelse af brud og juridiske oplysningsprocesser.

11.9 EU NIS2-direktivet (2022/2555)

11.9.1 Artikel 23 – Rapporteringsforpligtelser: Efterforskningsdokumentation og konstateringer understøtter rettidige og korrekte hændelsesrapporter til kompetente myndigheder.

11.10 EU DORA (2022/2554)

11.10.1 Artikel 17 – Rapportering af IKT-hændelser: Kræver detaljerede registreringer af rodårsag og bevismateriale for større IKT-relaterede hændelser, særligt i den finansielle sektor.

11.11 COBIT 2019

11.11.1 DSS01.07 – Manage Security Incidents: Kræver dokumentation af hændelser og grundighed i undersøgelser.

11.11.2 DSS05.04 – Manage Security Investigations: Fremhæver bevaring af digitale beviser og understøttelse af disciplinære og juridiske handlinger.