					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P31					Documenttitel: **Beleid inzake bewijsverzameling en forensisch onderzoek**						
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:						
X	Beleid		Standaard		Procedure		Formulier		Register		Overig

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 8	
ISO/IEC 27002:2022	Beheersmaatregelen 5.25–5.27, 8	
ISO/IEC 27035:2016	Delen 1 en 3	
NIST SP 800-53 Rev.5	IR-1 tot en met IR-9, AU-6, PL-2	
NIST SP 800-101 Rev.1	Forensisch onderzoek van mobiele apparaten en media	Forensisch onderzoek van mobiele apparaten en media
NIST SP 800-86	Integratie van forensische technieken	Integratie van forensische technieken in incidentrespons
EU AVG	Artikel 5, 33–34	
EU NIS2	Artikel 23(1)–(4)	
EU DORA	Artikel 17(1)–(3)	
COBIT 2019	DSS01.07, DSS05	

1. Doel

1.1 Dit beleid stelt een gestructureerd en juridisch verdedigbaar kader vast voor de identificatie, verzameling, bewaring, analyse en vernietiging van digitaal bewijsmateriaal tijdens feitelijke of vermoedelijke beveiligingsincidenten.

1.2 Het waarborgt dat processen voor forensische gereedheid en bewijsbehandeling:

1.2.1 De integriteit van het bewijsmateriaal en de chain of custody waarborgen

1.2.2 Interne onderzoeken, gerechtelijke procedures of rapportage aan toezichthouders ondersteunen

1.2.3 Aansluiten op internationaal aanvaarde forensische normen en criteria voor juridische toelaatbaarheid

1.3 Dit beleid ondersteunt de inzet van de organisatie voor proactieve incidentrespons, naleving van wet- en regelgeving en transparante governance, met minimale operationele verstoring.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 Alle medewerkers, opdrachtnemers, leveranciers en dienstverleners die betrokken zijn bij systeembeheer, incidentafhandeling of onderzoeksactiviteiten

2.1.2 Alle eindpunten, servers, applicaties, netwerken en cloudplatformen die onder de zeggenschap of contractuele verantwoordelijkheid van de organisatie vallen

2.1.3 Elk incident of elke gebeurtenis waarbij bewijsbehandeling vereist is, waaronder:

2.1.3.1 Dreigingen van binnenuit, datalekken of fraudeonderzoeken

2.1.3.2 Misbruik van systemen of inloggegevens

2.1.3.3 Incidenten met operationele technologie (OT)-systemen of industriële besturingssystemen

2.1.3.4 Schendingen van fysieke toegangsbeveiliging waarbij digitale activa betrokken zijn

2.2 Dit beleid regelt tevens iedere interactie met externe forensische dienstverleners of opsporingsinstanties tijdens juridische escalaties of procedures van toezichthouders.

3. Doelstellingen

3.1 Het mogelijk maken van snelle, veilige en beleidsconforme verwerving van bewijsmateriaal tijdens beveiligingsincidenten of onderzoeken.

3.2 Het borgen van de integriteit, authenticiteit en toelaatbaarheid van verzameld digitaal bewijsmateriaal door strikte beheersing van toegang, logging en verificatieprocedures.

3.3 Het waarborgen dat alle forensische activiteiten in overeenstemming zijn met wettelijke en regelgevende verplichtingen, waaronder gegevensbescherming, arbeidsrecht en beperkingen op internationale doorgiften.

3.4 Het ondersteunen van analyses na incidenten, root cause analysis en verbetering van beheersmaatregelen door middel van forensische output van hoge kwaliteit.

3.5 Het integreren van forensische gereedheid in het managementsysteem voor informatiebeveiliging (ISMS), ter ondersteuning van audits, meldingen van datalekken en besluitvorming door de directie.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO)

4.1.1 Is eigenaar van dit beleid en waarborgt dat alle forensische activiteiten juridisch verdedigbaar, auditeerbaar en risicogebaseerd zijn.

4.1.2 Autoriseert escalatie naar externe juridische partijen en forensische dienstverleners.

4.2 Forensische analisten / incidentresponders

4.2.1 Leiden de verwerving, bewaring en technische analyse van bewijsmateriaal.

4.2.2 Zorgen ervoor dat de chain of custody correct wordt vastgelegd en onderhouden.

4.2.3 Documenteren alle handelingen, bevindingen en toolinstellingen die tijdens onderzoeken worden gebruikt.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Vereisten voor herziening en actualisering

9.1 Dit beleid moet ten minste jaarlijks worden beoordeeld en zo nodig worden bijgewerkt om rekening te houden met:

9.1.1 Wijzigingen in wetgeving, regelgeving of jurisprudentie die gevolgen hebben voor forensische procedures of gegevensverwerking

9.1.2 Actualisaties van door de sector erkende forensische normen of toolsets

9.1.3 Lessen uit evaluaties na incidenten, juridische geschillen of auditbevindingen

9.1.4 Technologische wijzigingen in platformen, apparaten of systemen die onderwerp zijn van onderzoek

9.2 De CISO is eigenaar van het beoordelingsproces en moet daarbij overleg voeren met:

9.2.1 Juridische zaken en compliance

9.2.2 Functionaris voor gegevensbescherming (FG)

9.2.3 Security Operations Center (SOC)- en forensische teams

9.2.4 Interne audit

9.3 Alle herzieningen moeten:

9.3.1 Onder versiebeheer worden geplaatst en worden opgeslagen in de beleidsrepository

9.3.2 Worden gecommuniceerd aan betrokken stakeholders, waaronder forensische teams en responsteams

9.3.3 Gepaard gaan met actualisaties van relevante operationele procedures en opleidingsmaterialen

9.4 Tussentijdse beoordelingen moeten worden gestart na ieder kritiek incident waarbij sprake is van onjuiste behandeling van bewijsmateriaal, een falen van de chain of custody of problemen met juridische toelaatbaarheid.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid is afgestemd op en wordt ondersteund door de volgende beleidslijnen van de organisatie:

10.1.1 P1 – Informatiebeveiligingsbeleid: stelt het fundamentele mandaat vast voor onderzoek, bewijsbehandeling en naleving van toepasselijke wet- en regelgeving.

10.1.2 P5 – Wijzigingsbeheerbeleid: waarborgt dat systemen die onderwerp zijn van onderzoek niet worden gewijzigd tijdens actieve forensische processen.

10.1.3 P14 – Gegevensbewarings- en vernietigingsbeleid: regelt de veilige vernietiging en bewaartermijnen voor bewijsmateriaal en zaakgerelateerde gegevens.

10.1.4 P18 – Beleid inzake cryptografische beheersmaatregelen: stelt eisen aan encryptie voor de opslag en overdracht van gevoelige gegevens of bewijsmateriaal.

10.1.5 P22 – Logging- en monitoringbeleid: waarborgt de beschikbaarheid van gebeurtenislogboeken en telemetrie voor bewijsverzameling en forensische correlatie.

10.1.6 P30 – Incidentresponsbeleid: definieert de triage van incidenten en escalatieprocedures waarbij forensische procedures worden gestart.

10.1.7 P33 – Beleid inzake audit- en nalevingsmonitoring: valideert naleving van forensische protocollen en chain of custody-vereisten door middel van periodieke audits.

11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op internationale normen voor forensisch onderzoek en incidentafhandeling en waarborgt de integriteit van bewijsmateriaal, juridische verdedigbaarheid en naleving over meerdere jurisdicties heen.

11.2 ISO/IEC 27001

11.2.1 Clausule 8.1 – Ondersteunt operationele beheersing van forensische gereedheid en bewijsprocedures

11.3 ISO/IEC 27002

11.3.1 Bijlage A beheersmaatregel 5.25 – Verantwoordelijkheden voor incidentbeheer: vereist vastgelegde rollen voor de afhandeling van informatiebeveiligingsincidenten en onderzoeken.

11.3.2 Bijlage A beheersmaatregel 5.26 – Incidentrapportage: ondersteunt de verzameling van artefacten die verband houden met gebeurtenissen als bewijsmateriaal.

11.3.3 Bijlage A beheersmaatregel 5.27 – Respons op informatiebeveiligingsincidenten: vereist een gestructureerde, op bewijsmateriaal gebaseerde respons en onderzoek.

11.3.4 Bijlage A beheersmaatregel 8.27 – Veilige ontwikkeling en forensisch onderzoek, waar van toepassing: behandelt de bescherming van systemen en tools tijdens onderzoeken.

11.4 ISO/IEC 27035:2016 (delen 1 en 3)

11.4.1 Beschrijft de beginselen voor incidentdetectie, respons en forensische gereedheid, waaronder planning, chain of custody en beheer van incidentbewijsmateriaal.

11.5 NIST SP 800-53 Rev.5

11.5.1 IR-1 tot en met IR-9, AU-6, PL-2: definieert gestructureerde vereisten voor het plannen, detecteren, analyseren, indammen en afhandelen van beveiligingsincidenten. Ondersteunt de verzameling en auditeerbaarheid van bewijsmateriaal (AU-6) en waarborgt afstemming met plannen voor systeembeveiliging en privacy (PL-2) tijdens forensische onderzoeken.

11.6 NIST SP 800-86

11.6.1 Biedt richtlijnen voor de integratie van forensische processen in de bredere levenscyclus van incidentrespons en voor het waarborgen van forensische gereedheid.

11.7 NIST SP 800-101 Rev.1

11.7.1 Richt zich op best practices voor het verwerven, bewaren en analyseren van digitaal bewijsmateriaal van media en mobiele apparaten op juridisch verdedigbare wijze.

11.8 EU AVG (2016/679)

11.8.1 Artikel 5 – Beginselen inzake de verwerking van persoonsgegevens: van toepassing op bewijsmateriaal dat persoonsgegevens of gevoelige gegevens bevat en waarborgt minimale gegevensverwerking en doelbinding.

11.8.2 Artikelen 33–34 – Melding van een datalek: forensische gegevens ondersteunen naleving van meldingsverplichtingen bij inbreuken en processen voor juridische openbaarmaking.

11.9 EU NIS2-richtlijn (2022/2555)

11.9.1 Artikel 23 – Meldingsverplichtingen: forensische documentatie en bevindingen ondersteunen tijdige en nauwkeurige incidentrapportages aan bevoegde autoriteiten.

11.10 EU DORA (2022/2554)

11.10.1 Artikel 17 – Rapportage van ICT-incidenten: vereist gedetailleerde vastlegging van de root cause analysis en het bewijsmateriaal van majeure ICT-gerelateerde incidenten, in het bijzonder in de financiële sector.

11.11 COBIT 2019

11.11.1 DSS01.07 – Beheer van beveiligingsincidenten: schrijft incidentdocumentatie en grondigheid van onderzoek voor.

11.11.2 DSS05.04 – Beheer van beveiligingsonderzoeken: benadrukt het bewaren van digitaal bewijsmateriaal en ondersteuning van disciplinaire en juridische maatregelen.