					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P31S					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	Clausules 6.1, 6.3, 8	Risicogebaseerde planning, verbeteracties en operationele beheersmaatregelen voor de integriteit van bewijsmateriaal
ISO/IEC 27002:2022	Beheersmaatregelen 5.24–5.27	Richtlijnen voor veilige behandeling, evaluaties na incidenten en op bewijsmateriaal gebaseerde verbeteringen
ISO/IEC 27035-3:2016	Clausules 6.3, 6.4, 7	Borgt passende planning, rechtmatige verzameling en veilige behandeling van digitaal bewijsmateriaal met chain-of-custody-documentatie
NIST SP 800-53 Rev. 5	IR-07, IR-08, AU-09, AU-12, PE-18	Forensische gereedheid, bescherming van auditlogboeken en doeltreffende integratie in incidentrespons
AVG	Artikelen 33, 34	Documentatie en traceerbaarheid voor datalekken met persoonsgegevens
NIS2	Artikel 23	Traceerbare incidentrapportage en veilige behandeling van bewijsmateriaal
DORA	Artikel 17(1), 17(2)	Borgt bewijsverzameling, opslag en bewaring voor ICT-gerelateerde incidenten, forensische deugdelijkheid en verzoeken van toezichthouders
COBIT 2019	DSS05.06, DSS05.07	Betrouwbare logging en gestructureerde behandeling van bewijsmateriaal voor veilige, auditeerbare onderzoeken

1. Doel

1.1. Dit beleid bepaalt hoe de organisatie digitaal bewijsmateriaal behandelt dat verband houdt met beveiligingsincidenten, datalekken of interne onderzoeken. Het waarborgt dat bewijsmateriaal op juridisch houdbare wijze wordt verzameld, opgeslagen en bewaard, zodat naleving tijdens audits kan worden aangetoond en zowel interne besluitvorming als mogelijke externe vervolgacties worden ondersteund.

1.2. Dit beleid stelt kleine organisaties in staat de integriteit van logboeken, bestanden en systeemimages te beschermen en tegelijkertijd aantoonbare zorgvuldigheid te betrachten in het kader van ISO/IEC 27001, de AVG en aanverwante normen.

1.3. Het beleid ondersteunt forensische gereedheid zonder geavanceerde technische middelen of een voltijds IT-team te vereisen, door duidelijke verantwoordelijkheden, processen en bewaartermijnen vast te leggen.

2. Reikwijdte

2.1. Dit beleid is van toepassing op:

2.1.1. alle werknemers, IT-dienstverleners en externe consultants die betrokken zijn bij incidentrespons, onderzoek of analyse van inbreuken

2.1.2. alle bedrijfssystemen, waaronder laptops, mobiele apparaten, servers, e-mailaccounts, SaaS-platforms en cloudopslag (bijvoorbeeld Microsoft 365 en Google Workspace)

2.1.3. iedere gebeurtenis waarvoor bewijsmateriaal nodig is ten behoeve van disciplinaire maatregelen, juridische verdediging, verzekeringsclaims of contact met toezichthouders

2.2. Dit omvat zowel feitelijke als vermoedelijke gebeurtenissen die verband houden met:

2.2.1. datalekken

2.2.2. insiderdreigingen of misbruik

2.2.3. beveiligingsincidenten (bijvoorbeeld malware of ongeautoriseerde toegang)

2.2.4. klantklachten waarvoor digitale verificatie vereist is

2.2.5. verzoeken of onderzoeken van toezichthouders of opsporingsinstanties

3. Doelstellingen

3.1. Waarborgen dat al het bewijsmateriaal wordt verzameld en behandeld op een wijze die de integriteit, authenticiteit en chain-of-custody behoudt.

3.2. Voorkomen dat logboeken, bestanden of systeemimages die voor onderzoeken nodig kunnen zijn, per ongeluk worden gewijzigd, verwijderd of onjuist worden behandeld.

3.3. Zorgen voor een consistente en auditeerbare aanpak van bewijsbeheer die voldoet aan juridische en regelgevende verwachtingen, zoals meldingen van inbreuken onder de AVG en traceerbaarheid onder NIS2.

3.4. Duidelijke rollen en verantwoordelijkheden vastleggen om snelle, veilige en juridisch conforme vastlegging van bewijsmateriaal tijdens beveiligingsincidenten te waarborgen.

3.5. Forensische gereedheid op mkb-niveau ondersteunen, met minimale complexiteit en zonder onnodige verstoring van de dagelijkse bedrijfsvoering.

4. Rollen en verantwoordelijkheden

4.1. Algemeen directeur (GM)

4.1.1. Keurt alle formele onderzoeken goed waarvoor bewijsverzameling vereist is.

4.1.2. Beoordeelt en accordeert incidentrapportages met mogelijke juridische of disciplinaire gevolgen.

4.1.3. Beslist of een externe juridisch adviseur of toezichthouders moeten worden geïnformeerd.

4.1.4. Zorgt ervoor dat dit beleid periodiek wordt herzien en bijgewerkt.

4.2. IT-dienstverlener / systeembeheerder

4.2.1. Verzamelt en bewaart digitaal bewijsmateriaal volgens veilige procedures.

4.2.2. Legt tijdstempels, systeemgegevens en de uitgevoerde verwerkingsstappen vast.

4.2.3. Beveiligt al het verzamelde materiaal op een beschermde locatie.

4.2.4. Ondersteunt forensische analyse indien vereist.

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

9. Eisen voor herziening en actualisering

9.1. Jaarlijkse beleidsbeoordeling

9.1.1. Dit beleid moet ten minste eenmaal per 12 maanden door de Algemeen directeur (GM) worden beoordeeld om te bevestigen dat:

9.1.1.1. het in overeenstemming is met de beheersmaatregelen uit Bijlage A van ISO/IEC 27001

9.1.1.2. het blijvend relevant is voor de huidige digitale platforms en IT-diensten

9.1.1.3. de procedures voor logging, bewaring van bewijsmateriaal en forensische gereedheid toereikend zijn

9.2. Triggergebeurtenissen voor beleidsherziening

9.2.1. Het beleid moet ook worden herzien en geactualiseerd na:

9.2.1.1. elk ernstig incident waarvoor bewijsverzameling nodig was

9.2.1.2. een mislukte audit of een verzoek van een toezichthouder waarbij de integriteit van bewijsmateriaal ter discussie werd gesteld

9.2.1.3. invoering van nieuwe tools of procedures voor incidentrespons of systeemmonitoring

9.2.1.4. juridische wijzigingen, zoals geactualiseerde richtsnoeren onder de AVG of NIS2

9.3. Goedkeuring en verspreiding van wijzigingen

9.3.1. Alle wijzigingen moeten door de GM worden beoordeeld en goedgekeurd.

9.3.2. De geactualiseerde versie moet worden gedeeld met:

9.3.2.1. IT-dienstverleners en consultants die betrokken zijn bij onderzoeken

9.3.2.2. medewerkers met verantwoordelijkheden op het gebied van systeembeheer

9.3.3. Een geactualiseerde kopie moet worden bewaard in het beleidsarchief van het bedrijf en op verzoek met auditors worden gedeeld.

10. Gerelateerde beleidsdocumenten en samenhang

10.1. Dit beleid hangt samen met de volgende op het mkb afgestemde beleidsdocumenten:

10.1.1. P2S – Beleid inzake governancerollen en -verantwoordelijkheden: legt bevoegdheden vast voor incidentonderzoeken, beslissingen over bewijsmateriaal en juridische escalatie.

10.1.2. P4S – Beleid inzake toegangsbeheer: waarborgt dat alleen geautoriseerd personeel toegang heeft tot gevoelige systemen en logboeken tijdens onderzoeken.

10.1.3. P22S – Logging- en monitoringbeleid: levert de brongegevens die als forensisch bewijsmateriaal worden gebruikt en stelt eisen aan bewaring, toegangscontrole en logging.

10.1.4. P30S – Incidentresponsbeleid: activeert de noodzaak tot bewijsverzameling en beschrijft de operationele workflow die leidt tot forensische bewaring.

10.1.5. P17S – Beleid inzake gegevensbescherming en privacy: waarborgt dat persoonsgegevens die als bewijsmateriaal worden verzameld, rechtmatig worden behandeld onder de AVG en aanverwante regelgeving.

10.2. Deze beleidsdocumenten ondersteunen gezamenlijk juridische verdedigbaarheid, integriteit van onderzoeken en het vermogen om naleving tijdens audits onder ISO/IEC 27001:2022 aan te tonen.

11. Referentienormen en -kaders

11.1. ISO/IEC 27001

11.1.1. Clausule 6.1 – Risicogebaseerde planning omvat gereedheid voor respons en procedures voor bewijsmateriaal.

11.1.2. Clausule 6.3 – Ondersteunt verbeteracties op basis van bewijsmateriaal uit incidenten.

11.1.3. Clausule 8.1 – Vereist operationele beheersmaatregelen voor de integriteit van bewijsmateriaal.

11.2. ISO/IEC 27002

11.2.1. Beheersmaatregelen 5.24–5.27 – Geven richting aan veilige behandeling, evaluaties na incidenten en op bewijsmateriaal gebaseerde verbeteringen.

11.3. ISO/IEC 27035-3

11.3.1. Clausules 6.3, 6.4 en 7.3 borgen passende planning, rechtmatige verzameling en veilige behandeling van digitaal bewijsmateriaal tijdens incidentrespons, inclusief bewaring en chain-of-custody-documentatie.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 en AU-12 borgen forensische gereedheid, bescherming van auditlogboeken en doeltreffende integratie van bewijsverzameling in de levenscyclus van incidentrespons.

11.5. NIST SP 800-86

11.5.1. Definieert best practices voor het verwerven, analyseren en beschermen van digitaal bewijsmateriaal tijdens incidentrespons.

11.6. AVG

11.6.1. Artikelen 33–34 – Vereisen documentatie en traceerbaarheid van incidenten en bewijsmateriaal bij melding van datalekken met persoonsgegevens.

11.7. NIS2-richtlijn (2022/2555)

11.7.1. Artikel 23 – Vereist traceerbare incidentrapportage en veilige behandeling van bewijsmateriaal voor essentiële en belangrijke entiteiten.

11.8. DORA

11.8.1. Artikel 17(1) – Borgt dat bewijsmateriaal met betrekking tot ICT-gerelateerde incidenten wordt verzameld en opgeslagen op een wijze die forensisch onderzoek ondersteunt.

11.8.2. Artikel 17(2) – Vereist dat financiële entiteiten alle relevante gegevens en logboeken in verband met beveiligingsgebeurtenissen bewaren, in lijn met forensische deugdelijkheid en verzoeken van toezichthouders.

11.9. COBIT 2019

11.9.1. DSS05.06 – Incidenten volgen, detecteren en rapporteren: benadrukt het belang van betrouwbare logging ter ondersteuning van onderzoeken.

11.9.2. DSS05.07 – Incidenten onderzoeken en opvolgen: vereist een gestructureerde behandeling van bewijsmateriaal om veilige en auditeerbare onderzoeken mogelijk te maken.