					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P08					Documenttitel: **Informatiebeveiligingsbewustzijns- en opleidingsbeleid**							
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 7.3, Annex A-beheersmaatregel 6.3	Stelt eisen aan bewustwording en training die in dit beleid zijn opgenomen
ISO/IEC 27002:2022	Beheersmaatregel 6	Ondersteunt passende bewustwordingstraining op basis van functie en rol
NIST SP 800-53 Rev.5	AT-1 tot en met AT-5	Sluit aan op beleid en procedures, bewustwordingstraining, rolgebaseerde training, trainingsregistraties en contact met beveiligingsgroepen
AVG	Artikelen 32, 39; overweging 78	Verplicht training voor verwerkers van persoonsgegevens en algemene bewustwording onder personeel
NIS2-richtlijn	Artikelen 21(2)(a, b), 21(3)	Vereist beleid voor risico- en beveiligingstraining en bewustwordingsinitiatieven
DORA	Artikelen 5, 8, 13	Vereist bewustwording en training inzake ICT-risico's als onderdeel van weerbaarheidsmaatregelen
COBIT 2019	APO07, DSS05, MEA	Bekrachtigt bewustwording binnen het personeelsbestand, gebruikerseducatie en continue nalevingsmonitoring

1. Doel

1.1 Dit beleid stelt het formele kader vast om te waarborgen dat al het personeel op de hoogte is van zijn verantwoordelijkheden op het gebied van informatiebeveiliging en de training ontvangt die nodig is om de vertrouwelijkheid, integriteit en beschikbaarheid (CIA) van informatieactiva te beschermen.

1.2 Het ondersteunt ISO/IEC 27001, clausule 7.3 en Annex A-beheersmaatregel 6.3 door een gestructureerd en risicogebaseerd bewustwordings- en opleidingsprogramma te verplichten dat is afgestemd op organisatorische rollen en veranderende dreigingen.

1.3 Dit beleid draagt bij aan het verminderen van mensgerelateerde kwetsbaarheden, het bevorderen van beveiligingsbewust gedrag en het continu versterken van veilige werkwijzen in overeenstemming met wettelijke, regelgevende en contractuele vereisten.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle interne en externe personen met toegang tot de informatiesystemen, gegevens of faciliteiten van de organisatie, waaronder:

2.1.1 werknemers (voltijd, deeltijd, tijdelijke krachten)

2.1.2 contractanten, consultants, externe leveranciers en stagiairs

2.1.3 derden met logische of fysieke toegang op grond van dienstverleningsovereenkomsten

2.2 De reikwijdte omvat:

2.2.1 initiële beveiligingsbewustwordingstraining bij indiensttreding

2.2.2 rolspecifieke training (bijvoorbeeld voor ontwikkelaars, Finance, gebruikers met uitgebreide bevoegdheden)

2.2.3 periodieke opfristrainingen en bewustwordingscampagnes

2.2.4 ad-hoctraining als reactie op incidenten of nieuwe dreigingen

2.3 Onder dit beleid vallende trainingsvormen omvatten e-learning, klassikale briefings, simulaties, kennistoetsen, posters, beveiligingsnieuwsbrieven en verplichte kennisname.

3. Doelstellingen

3.1 Waarborgen dat al het personeel zijn verantwoordelijkheden begrijpt bij het beschermen van bedrijfsmiddelen van de organisatie en het naleven van beveiligingsbeleid.

3.2 Doorlopende, meetbare bewustwordingstraining bieden die is afgestemd op rolgebonden risicoblootstelling.

3.3 Veilig gedrag verankeren in de dagelijkse operatie door werkwijzen zoals het gebruik van sterke wachtwoorden, incidentmelding en phishingweerbaarheid te versterken.

3.4 Zorgen voor naleving van wet- en regelgeving en auditgereedheid ten aanzien van verplichtingen inzake informatiebeveiligingstraining in verschillende sectoren en rechtsgebieden.

3.5 Beveiligingsincidenten als gevolg van nalatigheid, gebrek aan bewustzijn of onjuist oordeelsvermogen verminderen door gedragsbeïnvloeding en continue versterking.

4. Rollen en verantwoordelijkheden

4.1 Directie

4.1.1 Keurt de informatiebeveiligingsopleidingsstrategie van de organisatie goed, waarborgt dat hiervoor middelen beschikbaar zijn en verankert deze in de bedrijfsprioriteiten.

4.1.2 Ziet op managementniveau toe op naleving en handhaaft naleving van dit beleid binnen alle afdelingen.

4.2 CISO / ISMS-manager

4.2.1 Is eigenaar van dit beleid en stelt het kader voor bewustwording en training vast in lijn met risico's, naleving en bedrijfsbehoeften.

4.2.2 Houdt toezicht op het ontwerp, de uitvoering, de monitoring en de evaluatie van alle beveiligingstrainingsinitiatieven.

4.2.3 Zorgt ervoor dat trainingen periodiek worden vernieuwd en aansluiten op veranderende dreigingen en opkomende technologieën.

[... 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 actualisatie

9.1 Beoordelingsfrequentie

9.1.1 Dit beleid en het bijbehorende trainingsprogramma moeten worden beoordeeld:

9.1.1.1 jaarlijks, of

9.1.1.2 na grote incidenten waarbij menselijke fouten of interne dreigingen betrokken zijn

9.1.1.3 bij invoering van significante nieuwe technologieën of dreigingen

9.1.1.4 als reactie op wijzigingen in wettelijke, contractuele of certificeringsverplichtingen

9.2 Beoordelingsproces

9.2.1 De beoordeling wordt geleid door de CISO in coördinatie met:

9.2.1.1 HR- en trainingsafdelingen

9.2.1.2 Juridische Zaken, de compliancefunctie en functionarissen voor gegevensbescherming

9.2.1.3 IT-beveiligings- en operationele-risicofuncties

9.2.2 Alle actualisaties moeten:

9.2.2.1 worden goedgekeurd door de ISMS-stuurgroep

9.2.2.2 onder versiebeheer vallen en worden gedocumenteerd in het ISMS-documentenregister

9.2.2.3 aan gebruikers worden gecommuniceerd indien materiële wijzigingen gevolgen hebben voor de trainingsreikwijdte of verantwoordelijkheden

9.3 Governance voor actualisatie van inhoud

9.3.1 Trainingsmodules en bewustwordingsmateriaal moeten elke 12 maanden worden beoordeeld om te waarborgen:

9.3.1.1 relevantie voor het dreigingslandschap

9.3.1.2 regelgevende juistheid

9.3.1.3 compatibiliteit van het formaat (bijvoorbeeld toegankelijkheid, lokalisatie)

9.3.2 Verouderde of misleidende inhoud moet onmiddellijk worden ingetrokken en vervangen door goedgekeurde alternatieven.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid wordt ondersteund door, en ondersteunt de handhaving van:

10.1.1 P01 – Informatiebeveiligingsbeleid: stelt beveiligingsbewustzijn vast als een fundamentele beheersmaatregel binnen het ISMS van de organisatie.

10.1.2 P03 – Beleid inzake aanvaardbaar gebruik: vereist beleidskennisname tijdens training en verduidelijkt verantwoordelijkheden die samenhangen met dagelijks technologiegebruik.

10.1.3 P07 – Onboarding- en offboardingbeleid: waarborgt dat training bij indiensttreding is ingebed en gedurende het dienstverband wordt gevolgd.

10.1.4 P06 – Risicomanagementbeleid: koppelt mensgerichte training aan dreigingsmodellering en strategieën voor risicoreductie van restrisico.

10.1.5 P33 – Beleid inzake audit- en nalevingsmonitoring: valideert dat bewustwordingsmaatregelen tijdens audits operationeel, meetbaar en doeltreffend zijn.

10.2 Gezamenlijk vormen deze beleidslijnen een integraal kader voor gedragsgerichte beheersmaatregelen waarin bewustwording, verantwoordingsplicht en culturele verankering samenkomen.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 7.3 – Bewustwording: vereist dat organisaties waarborgen dat medewerkers op de hoogte zijn van het informatiebeveiligingsbeleid en hun verantwoordelijkheden. Dit beleid operationaliseert die eis door middel van gestructureerde onboarding, periodieke training en meetbare deelname aan campagnes.

11.1.2 Annex A-beheersmaatregel 6.3 – bewustwording, educatie en training op het gebied van informatiebeveiliging: volledig ingevuld via initiële, rolgebaseerde en doorlopende trainingsprogramma's die zijn afgestemd op de risicoprofielen van gebruikers.

11.2 ISO/IEC 27002:2022 – Beheersmaatregel 6

11.2.1 Ondersteunt de ontwikkeling en uitvoering van bewustwordingstraining die passend is voor functierollen, met nadruk op het versterken van veilig gedrag en periodieke actualisaties op basis van threat intelligence en auditfeedback.

11.3 NIST SP 800-53 Rev.5

11.3.1 AT-1 tot en met AT-5 (familie Bewustwording en training): dit beleid sluit aan op AT-1 (beleid en procedures), AT-2 (bewustwordingstraining), AT-3 (rolgebaseerde training), AT-4 (trainingsregistraties inzake beveiliging) en AT-5 (contact met beveiligingsgroepen).

11.3.2 IA-5, AC-2: versterkt de verantwoordelijkheid van gebruikers voor veilige authenticatie en aanvaardbaar gebruik, beide kernonderdelen van de gedragsuitkomsten van bewustwordingsprogramma's.

11.3.3 IR-1 tot en met IR-8: paraatheid voor incidentrespons wordt versterkt door gerichte bewustwordingscampagnes en simulaties.

11.4 AVG (2016/679)

11.4.1 Artikel 32 – Beveiliging van de verwerking: verplicht dat personeel dat persoonsgegevens verwerkt, wordt getraind om risico's voor persoonsgegevens te herkennen, te voorkomen en te melden. Dit beleid waarborgt dat verwerkers van persoonsgegevens en alle relevante rollen dienovereenkomstig worden getraind.

11.4.2 Artikel 39 – Taken van de functionaris voor gegevensbescherming: omvat het vergroten van bewustwording en het trainen van personeel dat betrokken is bij verwerkingsactiviteiten.

11.4.3 Overweging 78: moedigt passende bewustwordingsmaatregelen aan om robuuste beveiligingspraktijken en naleving van beleid te waarborgen.

11.5 NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(a, b): vereist dat entiteiten beleid invoeren voor risicoanalyse en beveiligingstraining voor al het relevante personeel. Dit beleid voldoet aan die eis door continue en rolafhankelijke trainingsprocessen vast te stellen.

11.5.2 Artikel 21(3): moedigt aan het bewustzijn van cyberbeveiligingsrisico's onder management en personeel te bevorderen via bewustwordingsinitiatieven en simulaties.

11.6 DORA (2022/2554)

11.6.1 Artikel 13 – Strategie voor digitale operationele weerbaarheid: verplicht dat bewustwording en training inzake ICT-risico's deel uitmaken van het governancemodel. Dit beleid waarborgt dat menselijk risico wordt aangepakt door middel van doorlopende educatie en dreigingssimulatie.

11.6.2 Artikelen 5 en 8: benadrukken het belang van interne beheersingskaders, waarvan bewustwording en training fundamentele onderdelen zijn voor ICT-weerbaarheid en cyberbeveiligingshygiëne.

11.7 COBIT 2019

11.7.1 APO07 – Managed Human Resources: bekrachtigt de noodzaak om bewustzijn van beveiligingsverantwoordelijkheden te ontwikkelen en dit te verankeren in personeelsmanagement.

11.7.2 DSS05 – Managed Security Services: stelt beheersmaatregelen vast voor gebruikerseducatie en incidentmelding, die beide integraal onderdeel zijn van dit beleid.

11.7.3 MEA03 – Monitor, Evaluate, and Assess Compliance: vraagt om beoordeling van de doeltreffendheid van gebruikersgedrag en naleving van beleid; dit wordt hier geïmplementeerd via phishingtests, quizzen en campagnemetrics voor bewustwording.