					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P08S					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	
ISO/IEC 27002:2022	Beheersmaatregel 6	
NIST SP 800-53 Rev.5	AT-2, AT-4	
EU NIS2	Artikel 21(2)(i)	
EU DORA	Artikel 13	
COBIT 2019	BAI08, DSS05	
AVG	Artikel 32, 39	

1. Doel

1.1. Dit beleid waarborgt dat alle medewerkers en contractanten hun verantwoordelijkheden op het gebied van informatiebeveiliging begrijpen.

1.2. Dit beleid heeft tot doel de kans op menselijke fouten te verkleinen, het vermogen om incidenten te detecteren en te melden te versterken en binnen de organisatie een beveiligingsbewuste cultuur te bevorderen.

1.3. Dit beleid ondersteunt de naleving van ISO/IEC 27001, NIS2, de AVG en DORA door beveiligingsbewustzijn te verankeren in het dagelijkse werkgedrag en de rolgebonden verwachtingen.

2. Reikwijdte

2.1. Dit beleid is van toepassing op alle medewerkers, contractanten, stagiairs en derden die toegang hebben tot bedrijfssystemen of gegevens.

2.2. Dit omvat:

2.2.1. initiële bewustwordingstraining op het gebied van informatiebeveiliging bij indiensttreding voor nieuwe medewerkers

2.2.2. jaarlijkse opfristraining informatiebeveiliging

2.2.3. ad-hoctraining en bewustwordingsactiviteiten (bijv. updates naar aanleiding van incidenten, posters of tips)

2.3. Dit beleid geldt voor alle functies, afdelingen en werklocaties.

3. Doelstellingen

3.1. Waarborgen dat alle medewerkers tijdig begrijpelijke en relevante bewustwordingstraining op het gebied van informatiebeveiliging ontvangen.

3.2. Medewerkers in staat stellen veelvoorkomende dreigingen zoals phishing, malware en datalekken te herkennen en te voorkomen.

3.3. Registraties van afgeronde opleidingen vastleggen om naleving van wettelijke, contractuele en auditvereisten aan te tonen.

3.4. De opleidingsinhoud actueel houden, zodat deze aansluit op het beleid, het dreigingslandschap en de toepasselijke regelgeving van de organisatie.

3.5. Een proactieve houding onder medewerkers bevorderen, waarbij informatiebeveiliging wordt beschouwd als onderdeel van de dagelijkse verantwoordelijkheid.

4. Rollen en verantwoordelijkheden

4.1. Algemeen directeur (GM)

4.1.1. Keurt opleidingsvereisten goed en ziet erop toe dat hiervoor voldoende middelen beschikbaar zijn.

4.1.2. Beoordeelt rapportages over voltooiing en escaleert niet-naleving waar nodig.

4.2. Officemanager / HR

4.2.1. Coördineert de uitvoering van opleidingen voor nieuwe medewerkers en de jaarlijkse opfristraining.

4.2.2. Beheert opleidingsregistraties en logboeken van afgeronde opleidingen.

4.2.3. Zorgt ervoor dat medewerkers kennisnemen van de kernbeleidslijnen op het gebied van informatiebeveiliging en van geheimhoudingsovereenkomsten.

[... 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 herziening

9.1.1. Dit beleid moet jaarlijks worden beoordeeld door de Algemeen directeur (GM) en HR om te waarborgen dat het aansluit op actuele risico's, regelgeving en de behoeften van het personeelsbestand.

9.2. Tussentijdse actualiseringen

9.2.1. Het beleid en de opleidingsinhoud moeten ook worden beoordeeld en herzien na:

9.2.1.1. een significant beveiligingsincident

9.2.1.2. juridische of contractuele wijzigingen

9.2.1.3. organisatorische herstructureringen of systeemmigraties

9.3. Versiebeheer en distributie

9.3.1. Elke actualisering moet het volgende bevatten:

9.3.1.1. versienummer en ingangsdatum

9.3.1.2. samenvatting van wijzigingen

9.3.1.3. goedkeuring door de Algemeen directeur (GM)

9.3.1.4. archief van alle eerdere versies, minimaal drie jaar bewaard

9.4. Communicatie aan medewerkers

9.4.1. Actualisaties van het beleid moeten aan alle medewerkers worden gecommuniceerd, en bij materiële wijzigingen moet beleidskennisname worden verkregen.

10. Gerelateerde beleidslijnen en samenhang

10.1. Dit beleid ondersteunt het volgende:

10.1.1. P2S – Beleid inzake governancerollen en -verantwoordelijkheden: wijst verantwoordelijkheid toe voor de coördinatie van opleidingen en het toezicht daarop

10.1.2. P3S – Beleid inzake aanvaardbaar gebruik: bekrachtigt gedragsverwachtingen die in de opleiding aan bod komen

10.1.3. P4S – Beleid inzake toegangsbeveiliging: waarborgt dat gebruikers het belang van toegangsbeveiliging begrijpen

10.1.4. P7S – Onboarding- en offboardingbeleid: verankert opleiding in het instroomproces

10.1.5. P30S – Incidentresponsbeleid (P30): waarborgt dat medewerkers weten hoe zij incidenten tijdig en correct moeten melden

11. Referentienormen en -raamwerken

11.1. ISO/IEC 27001

11.1.1. Clausule 7.3 – Vereist dat organisaties waarborgen dat medewerkers zich bewust zijn van hun verantwoordelijkheden en van de beveiligingsimpact van hun handelen.

11.2. ISO/IEC 27002

11.2.1. Beheersmaatregel 6.3 – Beschrijft de verwachtingen ten aanzien van de reikwijdte en uitvoering van beveiligingsopleidingen.

11.3. NIST SP 800-53 Rev.5

11.3.1. AT-2 – Vereist bewustwordingstraining voor gebruikers met systeemtoegang.

11.3.2. AT-4 – Omvat rolgebaseerde training en de gevolgen van niet-naleving.

11.4. AVG

11.4.1. Artikel 32 – Verplicht beveiligingsmaatregelen, waaronder opleiding van personeel, ter bescherming van persoonsgegevens.

11.4.2. Artikel 39 – Vereist dat functionarissen voor gegevensbescherming, waar van toepassing, toezicht houden op bewustwording en opleiding.

11.5. EU NIS2-richtlijn

11.5.1. Artikel 21(2)(i) – Vereist doorlopende bewustwordings- en opleidingsprogramma's op het gebied van cyberbeveiliging.

11.6. EU DORA

11.6.1. Artikel 13 – Vereist dat financiële entiteiten onderwijs en opleiding implementeren voor alle medewerkers met ICT-gerelateerde verantwoordelijkheden.

11.7. COBIT 2019

11.7.1. BAI08 – Kennis beheren: waarborgt dat medewerkers competent zijn en passend zijn opgeleid.

11.7.2. DSS05 – Beheer van beveiligingsdiensten: benadrukt bewustwording als een belangrijke beschermende beheersmaatregel.