					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P24S					Documenttitel: **Beleid inzake veilige ontwikkeling**							
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	Relevante beheersmaatregelen voor operationele processen, waaronder veilige ontwikkeling
ISO/IEC 27002:2022	Beheersmaatregelen 8.25–8.27	Omvat de levenscyclus van systeemontwikkeling, testen en beveiligingsverantwoordelijkheden van externe ontwikkelaars
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Behandelt veilige softwareontwikkeling, toegangsbeheersing en afhandeling van kwetsbaarheden binnen ontwikkeling
AVG	Artikel 25	Vereist gegevensbescherming door ontwerp en door standaardinstellingen in softwareontwikkeling
NIS2	Artikel 21(2)(a), (e), (h)	Verplicht beleid voor veilige ontwikkeling, toezicht op het gebruik van open source en documentatie van mitigerende maatregelen
DORA	Artikelen 6(7), 9(1)(c), 10(2)(c)	Beveiliging van de ontwikkelingslevenscyclus voor kritieke ICT-systemen in de financiële sector
COBIT 2019	BAI	Raamwerk voor gestructureerd, traceerbaar en weerbaar beheer van veilige ontwikkeling

1. Doel

1.1 Dit beleid waarborgt dat alle software, scripts en webgebaseerde tools die door de organisatie of haar externe partners worden ontwikkeld of gewijzigd, op veilige wijze worden ontwikkeld, zodat het risico op kwetsbaarheden, ongeautoriseerde toegang tot gegevens of verstoring van de bedrijfsvoering tot een minimum wordt beperkt.

1.2 Dit beleid stelt bindende regels vast voor veilige ontwikkeling en programmeerpraktijken die door alle interne ontwikkelaars, opdrachtnemers en leveranciers moeten worden nageleefd, ongeacht de omvang of complexiteit van het project.

1.3 Dit beleid is opgesteld om klantgegevens te beschermen, datalekken te voorkomen en te waarborgen dat software die door of namens de organisatie wordt ontwikkeld of aangepast, beveiligingsaudits kan doorstaan, voldoet aan wettelijke vereisten zoals de AVG, NIS2 en DORA, en certificering conform ISO/IEC 27001 ondersteunt.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle personen en entiteiten die namens de organisatie betrokken zijn bij het ontwikkelen, aanpassen, uitrollen of beheren van het volgende:

2.1.1 Websites, applicaties of automatiseringstools

2.1.2 Intern ontwikkelde scripts of software

2.1.3 Code die is ontwikkeld door externe ontwikkelaars of freelancers

2.1.4 Plug-ins, bibliotheken en softwarecomponenten die in productiesystemen zijn geïntegreerd

2.2 Dit beleid omvat alle omgevingen die voor ontwikkelactiviteiten worden gebruikt, waaronder:

2.2.1 Ontwikkel- en testomgevingen

2.2.2 Acceptatie- en pre-productieomgevingen

2.2.3 Productiesystemen die worden gebruikt voor het uitvoeren van maatwerkcode

2.3 Dit beleid regelt tevens de verwerking van gegevens tijdens ontwikkeling en uitrol, in het bijzonder het gebruik van productiegegevens in niet-productieomgevingen.

3. Doelstellingen

3.1 Het voorkomen van de introductie van beveiligingsfouten of kwetsbaarheden in maatwerksoftware of door derden ontwikkelde software.

3.2 Het waarborgen dat veilige programmeerpraktijken en preventie van kwetsbaarheden in elke fase van de systeemontwikkelingslevenscyclus zijn geïntegreerd.

3.3 Het beperken van risico's die samenhangen met het gebruik van open-sourcecomponenten of componenten van derden door passende beoordeling en opvolging verplicht te stellen.

3.4 Het verplicht stellen van formele codebeoordeling en beveiligingstesten van applicaties vóór vrijgave.

3.5 Het beheersen van toegang tot ontwikkelomgevingen en het waarborgen van scheiding van live-productiesystemen.

3.6 Het voldoen aan verplichte vereisten uit internationale normen en regelgeving, zoals ISO/IEC 27001, de AVG, DORA en NIS2.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Keurt dit beleid goed en is eigenaar van dit beleid.

4.1.2 Borgt dat alle softwareontwikkeling, intern of uitbesteed, voldoet aan dit beleid.

4.1.3 Beoordeelt en ondertekent ontwikkelings- of dienstverleningsovereenkomsten waarin eisen voor veilige ontwikkeling zijn opgenomen.

4.1.4 Verifieert naleving door leveranciers via periodieke afstemming of door beveiligingsbewijsmateriaal op te vragen.

4.2 Interne ontwikkelaar of applicatie-eigenaar

4.2.1 Volgt veilige programmeer- en uitrolpraktijken.

4.2.2 Past de checklist voor veilige ontwikkeling toe op ieder project.

4.2.3 Valideert de beveiliging van alle gebruikte open-sourcecomponenten of componenten van derden.

4.2.4 Meldt ontdekte kwetsbaarheden onmiddellijk aan de algemeen directeur.

[... 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 actualisatie

9.1 Dit beleid moet ten minste eenmaal per jaar door de algemeen directeur worden beoordeeld om:

9.1.1 Voortdurende naleving van ISO/IEC 27001, de AVG, NIS2 en DORA te verifiëren

9.1.2 Gewijzigde dreigingen of wijzigingen in best practices voor veilige ontwikkeling te verwerken

9.1.3 Compatibiliteit met nieuwe tools, platforms of leveranciersrelaties te waarborgen

9.2 Tussentijdse beoordelingen moeten worden gestart naar aanleiding van:

9.2.1 Een gemeld softwarebeveiligingsincident

9.2.2 De introductie van een nieuw ontwikkelframework of hostingplatform

9.2.3 Een wijziging in externe ontwikkelpartners

9.2.4 Actualisaties in regelgeving die gevolgen hebben voor software- of beveiligingsverplichtingen

9.3 Alle wijzigingen in dit beleid moeten:

9.3.1 Worden gedocumenteerd met datum, samenvatting van wijzigingen en goedkeuring door de algemeen directeur

9.3.2 Duidelijk worden gecommuniceerd aan alle interne en externe ontwikkelmedewerkers

9.3.3 Worden opgeslagen als onderdeel van het versiebeheer en de wijzigingshistorie van het beleid van de organisatie

9.4 Geactualiseerde versies moeten eenvoudig toegankelijk worden gemaakt via interne platforms, geprinte documentatie of in de cloud gehoste diensten die toegankelijk zijn voor leveranciers.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid ondersteunt en is afhankelijk van de doeltreffende implementatie van verschillende andere mkb-beleidslijnen:

10.1.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: stelt verantwoordingsplicht vast voor het toewijzen en verifiëren van beveiligingsmaatregelen voor ontwikkeling over projecten en leveranciers heen.

10.1.2 P4S – Beleid inzake toegangscontrole: biedt basisregels voor het beperken van toegang tot ontwikkelomgevingen en coderepositories, inclusief functiescheiding (SoD).

10.1.3 P8S – Informatiebeveiligingsbewustzijns- en opleidingsbeleid: waarborgt dat interne ontwikkelaars en opdrachtnemers veilige programmeerpraktijken en aanverwante beveiligingsverantwoordelijkheden begrijpen.

10.1.4 P17S – Beleid inzake gegevensbescherming en privacy: verduidelijkt hoe persoonsgegevens moeten worden verwerkt tijdens ontwikkeling, testen en loggingprocessen om in overeenstemming met de AVG te blijven.

10.1.5 P30S – Incidentresponsbeleid (P30): definieert hoe ontwikkelingsgerelateerde beveiligingsincidenten moeten worden gemeld, beoordeeld en hersteld, inclusief blootstellingen die verband houden met code.

10.2 Deze beleidslijnen werken gezamenlijk om te waarborgen dat veilige ontwikkeling ook binnen een kleine of niet-technische organisatie uitvoerbaar en aantoonbaar is.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1 – Vereist de implementatie van operationele beheersmaatregelen, waaronder veilige ontwikkeling, die in lijn zijn met bedrijfsdoelstellingen en de risicohouding.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 8.25 – Beveelt aan om beveiliging in de volledige softwarelevenscyclus te integreren, waaronder broncodebeheer, versiebeheer en toegang voor ontwikkelaars.

11.2.2 Beheersmaatregel 8.26 – Specificeert methoden voor het testen van applicaties en verificatie van beveiligingsfunctionaliteit vóór livegang.

11.2.3 Beheersmaatregel 8.27 – Vereist dat externe ontwikkelaars dezelfde ontwikkelingsnormen naleven en dat hun beveiligingsverantwoordelijkheden duidelijk zijn vastgelegd.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 tot en met SA-15 – Definiëren processen voor veilige ontwikkeling, waaronder toegangsbeheersing voor ontwikkelaars, testen, dreigingsmodellering en documentatie.

11.3.2 SI-10 – Vereist dat ontwikkelaars veelvoorkomende softwarezwaktes identificeren en mitigeren en, waar van toepassing, geautomatiseerde tools gebruiken.

11.4 AVG (2016/679)

11.4.1 Artikel 25 – "Gegevensbescherming door ontwerp en door standaardinstellingen" verplicht de integratie van beveiligings- en privacywaarborgen tijdens ontwerp en ontwikkeling van software, in het bijzonder wanneer persoonsgegevens worden verwerkt.

11.5 NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(a), (e) en (h) – Vereist beleid voor veilige ontwikkeling, toezicht op het gebruik van open source en gedocumenteerde mitigatie van toepassingsgerelateerde risico's bij essentiële en belangrijke entiteiten.

11.6 DORA (2022/2554)

11.6.1 Artikelen 6(7), 9(1)(c) en 10(2)(c) – Leggen verplichtingen op voor de beveiliging van de ontwikkelingslevenscyclus voor entiteiten in de financiële sector, waaronder mkb-organisaties, in het bijzonder voor kritieke ICT-systemen.

11.7 COBIT 2019

11.7.1 BAI03 – "Manage Solutions Identification and Build" ondersteunt de implementatie van gestructureerde ontwikkelingsmaatregelen met nadruk op beveiliging, traceerbaarheid en weerbaarheid, afgestemd op beperkingen binnen het mkb.