					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P28S					Documenttitel: **Beleid inzake uitbestede 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	Clausules 5.1, 6.1, 8	Toepasselijke beheersmaatregelen met betrekking tot het ISMS en leveranciers
ISO/IEC 27002:2022	Beheersmaatregelen 5.19, 5.20, 8.25–8.27	Beheersmaatregelen voor leveranciers en veilige levenscycli voor systeemontwikkeling
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Vereisten voor inkoop, toeleveringsketen, veilige ontwikkeling en leveranciersovereenkomsten
AVG	Artikel 28	Contractuele vereisten en vereisten inzake gegevensbescherming voor verwerking door derden
EU NIS2	Artikel 21(2)(a), (h)	Beheersmaatregelen voor de toeleveringsketen en veilige applicatieontwikkeling
EU DORA	Artikel 10	ICT-risicobeheer voor derden, inclusief uitbestede ontwikkeling
COBIT 2019	BAI03, DSS05	Vereisten voor externe ontwikkeling en externe IT-dienstverleners

1. Doel

1.1 Dit beleid waarborgt dat alle uitbestede softwareontwikkeling — ongeacht of deze wordt uitgevoerd door freelancers, bureaus of externe leveranciers — veilig wordt uitgevoerd, contractueel wordt beheerst en in overeenstemming is met toepasselijke wettelijke, regelgevende en auditvereisten.

1.2 Dit beleid beschermt de organisatie tegen risico's die samenhangen met onveilige code, onduidelijk eigenaarschap, gegevensblootstelling en ontoereikend leveranciersbeheer door afdwingbare ontwikkelstandaarden en toezicht op leveranciers op te leggen, ook wanneer geen eigen IT-afdeling aanwezig is.

1.3 Dit beleid ondersteunt certificering volgens ISO/IEC 27001:2022 door duidelijk vastgelegde ontwikkelverwachtingen, verantwoordelijkheden en gedocumenteerde beheersmaatregelen voor ontwikkelactiviteiten van derden te bieden.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle uitbestede ontwikkelaars, waaronder freelancers en ontwikkelbureaus;

2.1.2 alle ontwikkelwerkzaamheden met betrekking tot interne tools, publiek toegankelijke websites, softwaretoepassingen of bedrijfsautomatisering;

2.1.3 medewerkers die verantwoordelijk zijn voor het selecteren, beheren of aansturen van externe ontwikkelaars;

2.1.4 alle systeemintegraties van derden, scripts of ontwikkelwerkzaamheden die interactie hebben met bedrijfsgegevens of systemen.

2.2 Dit beleid omvat tevens iedere partij of ieder platform met toegang tot bedrijfsinloggegevens, repositories, broncoderepositories, stagingomgevingen of productiesystemen.

3. Doelstellingen

3.1 Waarborgen dat alle uitbestede ontwikkeling voldoet aan veilige programmeerpraktijken en dat ontwikkelaars contractueel verplicht zijn gedocumenteerde standaarden en geheimhoudingsclausules na te leven.

3.2 Eigenaarschap vastleggen voor alle opgeleverde resultaten — code, assets, inloggegevens en documentatie — zodat rechten volledig aan het bedrijf worden overgedragen en de overdracht bij afronding van het project traceerbaar is.

3.3 Veelvoorkomende ontwikkelrisico's voorkomen, waaronder hergebruik van bedrijfseigen code, aanvallen op de toeleveringsketen via libraries, gebruik van niet-ondersteunde frameworks en niet-beoordeelde beheerdersrechten.

3.4 Voor elk uitbesteed project voorafgaande documentatie vereisen, waaronder contracten, geheimhoudingsovereenkomsten en minimale beveiligingsverwachtingen.

3.5 Klantgegevens, systemen en interne processen beschermen door effectief toezicht op ontwikkeling, testen na oplevering en veilig beheer van systeemtoegang af te dwingen.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Keurt alle leveranciersrelaties goed en ondertekent ontwikkelovereenkomsten.

4.1.2 Ziet erop toe dat alle uitbestede ontwikkeling voldoet aan dit beleid.

4.1.3 Trekt toegang tot bedrijfssystemen in na afronding van het project.

4.1.4 Beoordeelt documentatie en resultaten na oplevering.

4.2 Projecteigenaar (doorgaans een interne medewerker of aangewezen coördinator)

4.2.1 Verzorgt de dagelijkse afstemming met de externe ontwikkelaar.

4.2.2 Verifieert dat aan functionele eisen is voldaan en dat opgeleverde resultaten zijn getest.

4.2.3 Waarborgt veilige overdracht van code en inloggegevens.

4.2.4 Meldt ontwikkelgerelateerde kwesties of incidenten aan de GM.

[... 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 ten minste eenmaal per jaar door de algemeen directeur (GM) worden herzien. De herziening waarborgt dat het beleid blijft voldoen aan:

9.1.1.1 de certificeringsvereisten van ISO/IEC 27001;

9.1.1.2 wijzigingen in wettelijke verplichtingen, bijvoorbeeld AVG artikel 28 en DORA artikel 10;

9.1.1.3 actuele ontwikkelpraktijken op MKB-niveau en risico's van derden.

9.2 Tussentijdse herzieningen

9.2.1 Beleidsherzieningen moeten ook plaatsvinden wanneer:

9.2.1.1 een nieuwe leverancier of een nieuw platform voor uitbestede ontwikkeling wordt geonboard;

9.2.1.2 een significant incident met betrekking tot uitbestede ontwikkeling plaatsvindt;

9.2.1.3 wezenlijke wijzigingen optreden in de gebruikte tools, platforms of omgevingen.

9.3 Herzieningsproces

9.3.1 De GM is verantwoordelijk voor:

9.3.1.1 het verifiëren dat contracten, geheimhoudingsovereenkomsten en processen voor toegangsbeheer doeltreffend blijven;

9.3.1.2 het bevestigen dat huidige leveranciers en freelancers in overeenstemming zijn met dit beleid;

9.3.1.3 het actualiseren van bepalingen op basis van feedback uit eerdere projecten of incidenten.

9.4 Versiebeheer en communicatie

9.4.1 Alle wijzigingen moeten:

9.4.1.1 worden vastgelegd met datum, reden en beschrijving van de wijziging;

9.4.1.2 worden goedgekeurd door de GM en worden toegevoegd aan de versiehistorie;

9.4.1.3 worden gecommuniceerd aan alle medewerkers of projecteigenaren die met externe ontwikkelaars werken;

9.4.1.4 waar nodig opnieuw worden verstrekt aan alle betrokken leveranciers en derden.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid ondersteunt rechtstreeks de implementatie van de volgende op het MKB afgestemde beleidslijnen en is daarvan afhankelijk:

10.1.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: Verduidelijkt wie verantwoordelijk is voor goedkeuring van leveranciers, toegangsbeheer en risicoacceptatie bij het inzetten van uitbestede ontwikkelaars.

10.1.2 P4S – Beleid inzake toegangscontrole: Definieert de juiste aanmaak, beperking en beëindiging van gebruikersaccounts en beheerdersrechten die tijdens uitbestede ontwikkeling worden gebruikt.

10.1.3 P8S – Beleid inzake informatiebeveiligingsbewustzijn en opleiding: Zorgt ervoor dat interne medewerkers begrijpen hoe zij veilig met externe ontwikkelaars moeten samenwerken, inclusief de omgang met inloggegevens en projectbestanden.

10.1.4 P17S – Beleid inzake gegevensbescherming en privacy: Legt beveiligings- en wettelijke vereisten vast voor de verwerking van persoonsgegevens die door uitbestede ontwikkelaars onder de AVG kunnen worden verwerkt.

10.1.5 P24S – Beleid inzake veilige ontwikkeling: Bepaalt hoe interne en externe ontwikkeling veilige programmeerpraktijken en beoordeling van libraries en frameworks moet volgen.

10.1.6 P30S – Incidentresponsbeleid (P30): Bepaalt wanneer uitbestede ontwikkeling leidt tot beveiligingsincidenten of kwetsbaarheden en biedt richting voor gecoördineerd onderzoek en herstel.

10.2 Deze beleidslijnen moeten gelijktijdig worden geïmplementeerd om te waarborgen dat uitbestede ontwikkeling geen onbeheerst risico creëert en niet leidt tot schending van nalevingsverplichtingen voor het MKB.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 6.1 – Organisaties moeten informatiebeveiligingsrisico's in verband met leveranciers beoordelen en behandelen.

11.1.2 Clausule 8.1 – Vereist operationele planning en beheersing, inclusief diensten van derden zoals uitbestede ontwikkeling.

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 5.19 – Beveelt aan het vermogen van leveranciers te beoordelen om aan informatiebeveiligingsvereisten te voldoen.

11.2.2 Beheersmaatregel 5.20 – Stimuleert regelmatige monitoring en periodieke beoordeling van diensten van derden.

11.2.3 Beheersmaatregelen 8.25–8.27 – Beschrijven praktijken voor veilige levenscycli van systeemontwikkeling die van toepassing zijn op uitbestede ontwikkeling.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Vereist dat inkoopstrategieën informatiebeveiligingsmaatregelen omvatten.

11.3.2 SA-9 – Behandelt externe systeemontwikkeling en risico's in de toeleveringsketen.

11.3.3 SA-11 – Definieert veilige ontwikkelpraktijken, waaronder code review en herstel van tekortkomingen.

11.3.4 SA-15 – Stimuleert geautomatiseerde tools voor detectie van tekortkomingen en software assurance.

11.3.5 SR-3 – Vereist dat leveranciersovereenkomsten cyberbeveiligingsvereisten bevatten.

11.4 Algemene Verordening Gegevensbescherming (AVG)

11.4.1 Artikel 28 – Vereist contracten met verwerkers van derde partijen om passende waarborgen voor gegevensbescherming te bieden, rechtstreeks van toepassing op ontwikkelaars die persoonsgegevens verwerken of benaderen.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(a), (h) – Vereist beheersmaatregelen voor beveiliging van de toeleveringsketen en veilige softwareontwikkeling voor digitale dienstverleners die binnen de reikwijdte vallen, inclusief MKB-organisaties indien van toepassing.

11.6 EU Digital Operational Resilience Act (DORA)

11.6.1 Artikel 10 – Vereist ICT-risicobeheer voor derden, inclusief ontwikkelovereenkomsten, beveiligingsverplichtingen en risicobeheersmaatregelen met betrekking tot externe leveranciers.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build – Waarborgt dat externe ontwikkeling voldoet aan bedrijfsvereisten en beveiligingsverwachtingen.

11.7.2 DSS05 – Manage Security Services – Vereist dat externe beveiligingsdiensten en ontwikkelproviders werken onder afgedwongen beveiligingsregels en toezicht.