					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P28					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	Clausule 8.1	N.v.t.
ISO/IEC 27002:2022	Beheersmaatregelen 5.19-5.22, 8	N.v.t.
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-10	N.v.t.
AVG	Artikelen 28, 32	N.v.t.
EU NIS2	Artikelen 21(2)(a), (h), 23	N.v.t.
EU DORA	Artikelen 28(1), (2)	N.v.t.
COBIT 2019	APO10, BAI03, DSS05	N.v.t.

1. Doel

1.1 Dit beleid definieert verplichte beheersmaatregelen voor het uitbesteden van software- of systeemontwikkeling aan externe leveranciers, opdrachtnemers of bureaus, zodat veilige werkwijzen in de volledige softwareontwikkelingslevenscyclus zijn verankerd.

1.2 Dit beleid beoogt beveiligingskwetsbaarheden, gegevensverlies, blootstelling van intellectuele eigendom (IP) en nalevingsinbreuken als gevolg van externe ontwikkeltrajecten te voorkomen.

1.3 Dit beleid verplicht tot leveranciersbeheer, standaarden voor veilig programmeren, beheer van gebruikersrechten, monitoringverplichtingen en offboarding aan het einde van het contract om de vertrouwelijkheid, integriteit en beschikbaarheid van ontwikkelde software te waarborgen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle organisatieonderdelen die externe partijen inschakelen voor software- of systeemontwikkeling, waaronder:

2.1.1 webapplicaties, mobiele apps, embedded systemen, API's, scripts, automatiseringsworkflows of platformmodules

2.1.2 maatwerkontwikkeling voor interne platforms, klantgerichte systemen of commerciële producten

2.1.3 samenwerkingen met externe ontwikkelaars, freelancers, bureaus of offshoreteams

2.2 Dit beleid is ook van toepassing op iedere externe partij die tijdens de ontwikkeling toegang heeft tot broncode, testomgevingen of CI/CD-pijplijnen.

2.3 De vereisten zijn afdwingbaar ongeacht het contracttype, de ontwikkelmethodologie of de geografische locatie van de uitbestede dienstverlener.

3. Doelstellingen

3.1 Het afdwingen van veilige ontwikkelpraktijken binnen de Software Development Life Cycle (SDLC) voor alle uitbestede trajecten, van planning tot validatie na ingebruikname.

3.2 Waarborgen dat alle contracten met externe ontwikkelaars verplichte clausules bevatten inzake gegevensbescherming, veilig programmeren en eigendom van intellectuele eigendom.

3.3 Het vaststellen van vereisten voor toegangsbeheersing, monitoring en audits voor externe ontwikkelaars die met interne systemen werken.

3.4 Het beschermen van de organisatie tegen risico's in de toeleveringsketen, overtreding van wet- en regelgeving en reputatieschade in verband met extern ontwikkelde software.

3.5 Het borgen van continue naleving van beveiligingsraamwerken, waaronder ISO/IEC 27001, NIST, AVG, NIS2, DORA en COBIT 2019.

4. Rollen en verantwoordelijkheden

4.1 Directie

4.1.1 Keurt uitbestede ontwikkelingsprojecten met een hoog risico goed en valideert, indien gerechtvaardigd, beleidsuitzonderingen.

4.1.2 Ziet erop toe dat uitbestedingsbeslissingen in lijn zijn met de strategische doelstellingen en de risicobereidheid van de organisatie.

4.2 Chief Information Security Officer (CISO)

4.2.1 Keurt de onboarding van leveranciers goed vanuit informatiebeveiligingsperspectief.

4.2.2 Stelt vereisten voor beveiligingsmaatregelen vast voor uitbestede trajecten en beoordeelt incidentrapportages.

[... 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 actualisering

9.1 Dit beleid moet ten minste jaarlijks worden herzien of vaker onder de volgende omstandigheden:

9.1.1 invoering van nieuwe modellen voor uitbestede ontwikkeling, leveranciers of rechtsgebieden

9.1.2 wijzigingen in regelgevende kaders zoals de AVG, NIS2 of DORA

9.1.3 na een beveiligingsincident met betrekking tot uitbestede code, toegang of op te leveren resultaten

9.1.4 als onderdeel van bevindingen uit interne audits of verbeteringen aan het ISMS

9.2 De Chief Information Security Officer (CISO) is verantwoordelijk voor het initiëren en coördineren van de beleidsevaluatie in overleg met:

9.2.1.1 Juridische Zaken en Inkoop (voor afstemming van contractuele handhaving)

9.2.1.2 projecteigenaren en producteigenaren (voor operationele haalbaarheid)

9.2.1.3 Informatiebeveiliging (voor actualisaties van dreigingen en beheersmaatregelen)

9.2.1.4 Directie (voor definitieve goedkeuring)

9.3 Alle beleidsactualisaties moeten:

9.3.1.1 onder versiebeheer worden geplaatst en opgeslagen in een aangewezen documentrepository

9.3.1.2 worden gecommuniceerd aan stakeholders die betrokken zijn bij activiteiten op het gebied van uitbestede ontwikkeling

9.3.1.3 worden gekoppeld aan eventuele wijzigingen in gerelateerde beleidsdocumenten of procedurele documentatie

9.4 Iedere beleidsversie moet vergezeld gaan van een wijzigingslogboek om de traceerbaarheid van wijzigingen en goedkeuringen te waarborgen.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 Dit beleid ondersteunt en wordt ondersteund door de volgende gerelateerde documenten:

10.1.1 P1 - Informatiebeveiligingsbeleid: Stelt beveiligingsprincipes op organisatieniveau vast die van toepassing zijn op interne ontwikkeling en ontwikkeling door derden.

10.1.2 P5 - Wijzigingsbeheerbeleid: Borgt dat alle implementatiegerelateerde wijzigingen vanuit uitbestede codebases vóór ingebruikname worden beoordeeld en goedgekeurd.

10.1.3 P13 - Beleid inzake gegevensclassificatie en etikettering: Bepaalt hoe gevoelige gegevens worden geïdentificeerd voordat zij worden blootgesteld aan ontwikkelleveranciers of repositories.

10.1.4 P18 - Beleid inzake cryptografische beheersmaatregelen: Geeft richting aan de wijze waarop sleutels, secrets en gevoelige referenties tijdens ontwikkeling en oplevering moeten worden behandeld.

10.1.5 P24 - Beleid inzake veilige ontwikkeling: Definieert baselinevereisten voor interne en externe softwareontwikkelpraktijken.

10.1.6 P30 - Incidentresponsbeleid: Regelt hoe inbreuken of beveiligingskwesties met betrekking tot uitbestede ontwikkeling worden geëscaleerd, onderzocht en opgelost.

10.1.7 P33 - Beleid inzake audit- en nalevingsmonitoring: Biedt vereisten voor het beoordelen van activiteiten op het gebied van uitbestede ontwikkeling tijdens audits of nalevingsbeoordelingen.

11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op internationaal erkende beveiligingsraamwerken en regelgeving om veilige uitbesteding van softwareontwikkeling en de bijbehorende leveranciersbeheerpraktijken te waarborgen.

11.2 ISO/IEC 27001

11.2.1 Clausule 8.1 - Operationele planning en beheersing: Verplicht procesbeheersmaatregelen voor veilige ontwikkeling en levering door derden.

11.3 ISO/IEC 27002:2022 - Beheersmaatregelen 5.19 tot en met 5.21, 8.27

11.3.1 Bijlage A Beheersmaatregel 5.19 - Beheer van leveranciersrelaties: Vereist formele overeenkomsten met clausules inzake beveiliging en naleving.

11.3.2 Bijlage A Beheersmaatregel 5.20 - Informatiebeveiliging adresseren binnen leveranciersovereenkomsten: Borgt dat ontwikkelingsspecifieke beheersmaatregelen in contracten zijn opgenomen.

11.3.3 Bijlage A Beheersmaatregel 5.21 - Beheer van dienstverlening door leveranciers: Omvat het monitoren van op te leveren resultaten en risico's van ontwikkeling door derden.

11.3.4 Bijlage A Beheersmaatregel 8.27 - Uitbestede ontwikkeling: Verplicht vastgelegde beveiligingsvereisten en toegangsbeheersing voor extern ontwikkelde software.

11.3.5 Deze beheersmaatregelen definiëren gestructureerde vereisten voor het selecteren, contracteren en aansturen van uitbestede ontwikkelaars, waaronder veilige ontwikkelpraktijken, omgang met code en validatie van prestaties.

11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - Verwervingsproces: Vereist dat vereisten voor veilige ontwikkeling tijdens de verwerving worden vastgelegd.

11.4.2 SA-9 - Externe systeemdiensten: Regelt hoe externe ontwikkelaars op veilige wijze met interne diensten interacteren.

11.4.3 SA-10 - Configuratiebeheer voor ontwikkelaars: Sluit aan op verplichtingen inzake versiebeheer, codetoegang en wijzigingsopvolging voor externe teams.

11.5 AVG (EU 2016/679)

11.5.1 Artikel 28 - Verplichtingen van de verwerker: Vereist dat contracten met externe ontwikkelaars beveiligings-, beheersings- en auditvereisten specificeren voor de verwerking van persoonsgegevens.

11.5.2 Artikel 32 - Beveiliging van de verwerking: Verplicht passende waarborgen (bijv. encryptie, toegangsbeheersing) bij de ontwikkeling van systemen die persoonsgegevens verwerken.

11.6 EU NIS2-richtlijn (2022/2555)

11.6.1 Artikelen 21(2)(a), (h), 23: Verplichten dat veilige ontwikkelpraktijken worden toegepast binnen opdrachten aan derden en digitale toeleveringsketens, met toezicht en technische verificatie.

11.7 EU DORA (2022/2554)

11.7.1 Artikelen 28(1), (2): Vereisen dat financiële entiteiten ICT-risico's van derde partijen beheren door middel van contractuele beheersmaatregelen en toezicht op veilige ontwikkeling, met name bij kritieke uitbestede ontwikkeling.

11.8 COBIT 2019

11.8.1 APO10 - Leveranciers beheren: Stelt gestructureerde vereisten vast voor leveranciersbeoordeling, contracten en prestatiemonitoring.

11.8.2 BAI03 - Oplossingen ontwikkelen en bouwen beheren: Sluit rechtstreeks aan op veilige SDLC-processen, codereviews en validatie van ontwikkeling.

11.8.3 DSS05 - Beveiligingsdiensten beheren: Sluit aan op de monitoring en bescherming van systemen die extern of door derden zijn ontwikkeld.