					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P25					Documenttitel: **Beleid inzake vereisten voor applicatiebeveiliging**							
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	—
ISO/IEC 27002:2022	Beheersmaatregelen 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
AVG	Artikelen 25, 32	—
EU NIS2	Artikelen 21(2)(f), 23	—
EU DORA	Artikelen 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Doel

1.1 Dit beleid definieert verplichte beveiligingsvereisten op applicatieniveau voor software die door de organisatie wordt ontwikkeld, verworven, geïntegreerd of uitgerold. Het waarborgt dat alle applicaties worden ontworpen, geïmplementeerd en onderhouden in overeenstemming met principes voor veilige ontwikkeling, nalevingsverplichtingen en de risicobereidheid van de organisatie.

1.2 Dit beleid schrijft voor dat beveiliging gedurende de volledige applicatielevenscyclus wordt ingebed, waaronder gebruikersauthenticatie, gegevensverwerking, interfacebescherming en veilige interactie met API's of diensten.

1.3 Met de invoering van dit beleid beoogt de organisatie de introductie van softwarekwetsbaarheden te voorkomen, gevoelige gegevens te beschermen en traceerbaarheid en weerbaarheid tegen exploitatie en misbruik te waarborgen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle:

2.1.1 intern ontwikkelde of extern verworven applicaties, met inbegrip van SaaS-oplossingen en maatwerktools

2.1.2 applicaties die kritieke bedrijfsprocessen ondersteunen, klanttoegang faciliteren of gereguleerde gegevens verwerken

2.1.3 ontwikkel-, DevOps-, QA-, product- en beveiligingsteams

2.1.4 externe ontwikkelaars, softwareleveranciers en integratiepartners met toegang tot applicaties of API's van de organisatie

2.2 Dit beleid geldt voor alle omgevingen: ontwikkeling, testen, acceptatie, productie en disaster recovery, ongeacht of deze worden gehost op on-premises infrastructuur, in private datacenters of in publieke cloudomgevingen.

3. Doelstellingen

3.1 Het vaststellen van baseline-beveiligingsvereisten, zowel functioneel als niet-functioneel, waaraan alle applicaties moeten voldoen, ongeacht de ontwikkelmethode of technologiestack.

3.2 Het waarborgen van de integratie van beveiligingsmaatregelen op applicatieniveau, waaronder invoervalidatie, uitvoercodering, foutafhandeling en sessiebeveiliging.

3.3 Het voorschrijven van een veilige implementatie van authenticatie-, autorisatie- en toegangscontrolemechanismen, in lijn met het Beleid inzake toegangscontrole van de organisatie.

3.4 Het verplichten van veilige interactie met API's, webinterfaces en componenten van derden door gebruik van goedgekeurde protocollen en beveiligingsmaatregelen.

3.5 Het mogelijk maken van vroegtijdige detectie en mitigatie van kwetsbaarheden door middel van statische en dynamische analyse, code review en dreigingsmodellering.

3.6 Het beschermen van gevoelige gegevens in overeenstemming met wettelijke vereisten door versleuteling, classificatie van bedrijfsmiddelen en bewaartermijnen af te dwingen.

3.7 Het waarborgen van continue validatie van de informatiebeveiligingsrisico's van applicaties na uitrol door middel van testen, monitoring en auditgereedheid.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO)

4.1.1 Is eigenaar van dit beleid en waarborgt afstemming op de informatiebeveiligingsstrategie en risicohouding van de organisatie.

4.1.2 Keurt vereisten voor applicatiebeveiliging goed en dwingt verplichte beheersmaatregelen af binnen ontwikkel- en inkoopfuncties.

4.2 Verantwoordelijke voor applicatiebeveiliging / DevSecOps-manager

4.2.1 Definieert de baseline van beveiligingsmaatregelen en testmethodologieën voor applicatiecomponenten.

4.2.2 Houdt toezicht op de veilige integratie van tools zoals SAST, DAST, IAST en SCA in de softwareleveringsketen.

4.2.3 Beheert de checklist met vereisten voor applicatiebeveiliging en de validatiecriteria.

[... 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 Dit beleid moet jaarlijks worden herzien, of vaker als reactie op:

9.1.1 openbaarmakingen van kritieke kwetsbaarheden die gangbare frameworks of afhankelijkheden raken

9.1.2 wijzigingen in nalevingsverplichtingen voor applicatiebeveiliging, zoals NIS2 en DORA

9.1.3 majeure wijzigingen in de softwareontwikkelpraktijken, tooling of cloudarchitectuur van de organisatie

9.1.4 bevindingen uit interne audits of externe penetratietests

9.2 De herziening wordt geleid door de verantwoordelijke voor applicatiebeveiliging, in afstemming met de CISO en de verantwoordelijken voor DevOps Engineering, Juridische Zaken, Inkoop en QA.

9.3 Alle herzieningen moeten onder versiebeheer worden opgenomen in het ISMS-documentenregister en worden verspreid onder alle betrokken ontwikkel- en productteams.

9.4 Vervangen versies moeten gedurende ten minste drie jaar worden gearchiveerd ten behoeve van traceerbaarheid, auditbaarheid en ondersteuning bij onderzoek naar inbreuken.

10. Gerelateerd beleid en samenhang

10.1 P1 – Informatiebeveiligingsbeleid. Dit beleid vormt de basis voor de bescherming van systemen en gegevens, waaronder beheersmaatregelen op applicatieniveau vereist zijn om ongeautoriseerde toegang, datalekken en exploitatie te voorkomen.

10.2 P4 – Beleid inzake toegangscontrole. Dit beleid definieert de normen voor identiteits- en sessiebeheer die door alle applicaties moeten worden afgedwongen, waaronder sterke authenticatie, het beginsel van minimale bevoegdheden en vereisten voor periodieke beoordeling van toegangsrechten.

10.3 P5 – Wijzigingsbeheerbeleid. Dit beleid reguleert de promotie van applicatiecode en configuraties naar productieomgevingen en waarborgt dat ongeautoriseerde of niet-geteste wijzigingen worden geblokkeerd.

10.4 P17 – Beleid inzake gegevensbescherming en privacy. Dit beleid verplicht applicaties privacy by design toe te passen en een rechtmatige verwerking, versleuteling en bewaring van persoonsgegevens en gevoelige gegevens in alle omgevingen te waarborgen.

10.5 P24 – Beleid inzake veilige ontwikkeling. Dit beleid biedt het bredere kader voor het inbedden van beveiliging in de levenscycli van systeemontwikkeling, waarvan dit beleid de concrete vereisten en technische beheersmaatregelen op applicatieniveau vastlegt.

10.6 P30 – Incidentresponsbeleid (P30). Dit beleid schrijft een gestructureerde afhandeling voor van beveiligingsincidenten met betrekking tot applicaties, waaronder kwetsbaarheden die na uitrol of tijdens penetratietesten zijn vastgesteld, en beschrijft escalatie-, indammings- en herstelprocedures.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001:2022

11.1.1 Clausule 8.1 – Operationele planning en beheersing: Vereist dat applicatiebeveiliging in processen en systemen wordt ingebed om vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen.

11.2 ISO/IEC 27002:2022

11.2.1 Beheersmaatregelen 8.25–8.26: Beschrijven de verwachtingen voor beveiliging op applicatieniveau, waaronder veilige programmeerpraktijken, dreigingsmodellering, architectuurbeheersmaatregelen en validatie van software van derden.

11.2.2 Bijlage A, beheersmaatregel 8.25 – Levenscycli van systeemontwikkeling: Schrijft integratie van beveiliging voor gedurende de volledige applicatielevenscyclus.

11.2.3 Bijlage A, beheersmaatregel 8.26 – Vereisten voor applicatiebeveiliging: Verplicht het definiëren en afdwingen van technische beheersmaatregelen ter bescherming van applicaties tegen misbruik en compromittering.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Security testing and evaluation door ontwikkelaars: Verplicht statische tests, dynamische tests en penetratietests tijdens ontwikkeling.

11.3.2 SA-15 – Ontwikkelproces, standaarden en tools: Stelt formele standaarden vast voor veilige applicatieontwikkeling.

11.3.3 SI-10 – Validatie van informatie-invoer: Vereist beheersingsmechanismen ter voorkoming van injectie- en parseraanvallen.

11.4 AVG (2016/679)

11.4.1 Artikel 25 – Gegevensbescherming door ontwerp en door standaardinstellingen: Vereist integratie van gegevensbescherming en privacy in applicatielogica en werkstromen.

11.4.2 Artikel 32 – Beveiliging van de verwerking: Verplicht passende technische maatregelen, zoals invoervalidatie, versleuteling en veilige toegangsbeheersmaatregelen.

11.5 EU NIS2-richtlijn (2022/2555)

11.5.1 Artikel 21(2)(f): Vereist afhandeling van kwetsbaarheden en veilige praktijken voor de applicatielevenscyclus voor essentiële en belangrijke entiteiten.

11.5.2 Artikel 23 – Melding van beveiligingsincidenten: Vereist logging- en monitoringmogelijkheden op applicatieniveau om significante incidenten te detecteren en te melden.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 9 – ICT-risicobeheer: Verplicht financiële entiteiten ervoor te zorgen dat applicaties veilig en getest zijn en bestand zijn tegen cyberdreigingen.

11.6.2 Artikel 11 – Testen van ICT-tools: Stimuleert periodieke penetratietesten en red-teamoefeningen voor kritieke applicaties en diensten.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build: Stelt ontwerp- en beheersingsvereisten vast tijdens applicatieontwikkeling.

11.7.2 BAI09 – Manage Applications: Benadrukt veilig onderhoud, monitoring en verbetering van productieapplicaties.

11.7.3 DSS05 – Manage Security Services: Verbindt applicatiebeveiliging met bredere beveiligingsoperaties en beheersmaatregelen van de organisatie.