| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Voer hier de naam van de geregistreerde rechtspersoon in | | | | | | | |
| Documentnummer:<br>P25S | | | | | Documenttitel:<br>**Beleid inzake vereisten voor applicatiebeveiliging** | | | | | | | |
| Versie:<br>1.0 | | Ingangsdatum:<br>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 | Operationele beheersmaatregelen, waaronder applicatiebeveiliging |
| ISO/IEC 27002:2022 | Beheersmaatregelen 8.25–8.26 | Veilig ontwerp, veilige ontwikkeling, testen en codereview |
| NIST SP 800-53 Rev.5 | SA-11, SI-10 | Testen door ontwikkelaars van applicaties, codeanalyse, preventie van fouten |
| AVG | Artikel 25 | Gegevensbescherming door ontwerp en door standaardinstellingen |
| NIS2 | Artikel 21(2)(a), (e) | Technische maatregelen om applicaties te beveiligen en risico's te detecteren |
| DORA | Artikelen 9(2)(c), 10(2)(c) | Applicatiebeveiliging ten behoeve van digitale operationele weerbaarheid |
| COBIT 2019 | BAI03 | Beheer van veilige softwareontwikkeling en -verwerving |

**1. Doel**

1.1 Dit beleid definieert de minimaal verplichte beheersmaatregelen voor applicatiebeveiliging voor alle software- en systeemoplossingen die door de organisatie worden gebruikt, ongeacht of deze intern zijn ontwikkeld of zijn ingekocht bij externe leveranciers.

1.2 Het waarborgt dat applicaties zodanig worden ontworpen, geïmplementeerd en onderhouden dat klantgegevens, persoonsgegevens van werknemers en bedrijfsgegevens worden beschermd tegen ongeautoriseerde toegang, misbruik, wijziging of vernietiging.

1.3 Dit beleid ondersteunt de inspanningen van de organisatie om ISO/IEC 27001-certificering te behalen en te behouden, te voldoen aan verplichtingen uit de AVG en NIS2, en operationele risico's die samenhangen met onveilige software-uitrol te beperken.

1.4 Het bevordert een consistente en auditeerbare aanpak van applicatiebeveiliging voor het mkb door een uniforme checklist van beveiligingsfunctionaliteiten en verplichte configuraties en werkwijzen vast te stellen, afgestemd op omgevingen met beperkte interne technische capaciteit.

**2. Reikwijdte**

**2.1 Dit beleid is van toepassing op alle applicaties, systemen, tools en platforms die:**

2.1.1 intern worden ontwikkeld, aangepast of gescript voor intern gebruik

2.1.2 worden aangeschaft als commerciële software, SaaS of cloudgehoste systemen

2.1.3 persoonlijk identificeerbare informatie (PII), bedrijfsgegevens of gevoelige operationele informatie verwerken, opslaan of verzenden

2.1.4 worden benaderd door werknemers, contractanten, klanten of partners via interne netwerken, het internet of mobiele platforms

**2.2 Dit beleid geldt voor:**

2.2.1 ontwikkelaars (intern of ingehuurd)

2.2.2 softwareleveranciers en cloudproviders

2.2.3 IT-supportmedewerkers of beheerders die verantwoordelijk zijn voor uitrol en ondersteuning

2.2.4 applicatie-eigenaren en zakelijke gebruikers die betrokken zijn bij systeemgoedkeuring en toezicht

**3. Doelstellingen**

3.1 Waarborgen dat alle door de organisatie gebruikte applicaties ingebouwde en verifieerbare beveiligingsmaatregelen bevatten die veelvoorkomende softwarekwetsbaarheden mitigeren.

3.2 De vertrouwelijkheid, integriteit en beschikbaarheid (CIA) beschermen van gegevens die door applicaties worden verwerkt, ongeacht waar deze worden gehost.

3.3 Formele beveiligingstesten, beoordeling en validatie van applicatiebeveiliging vereisen voordat een nieuwe applicatie of majeure update voor productiegebruik wordt goedgekeurd.

3.4 Consistente en veilige verwerking van gebruikersreferenties, sessiegegevens en toegangsrechten mogelijk maken voor alle bedrijfskritische systemen.

3.5 Vereisen dat alle applicaties veilige logvoorzieningen, auditmogelijkheden en functionaliteit voor monitoring en dreigingsdetectie bevatten ter ondersteuning van de detectie van en respons op verdachte activiteiten.

3.6 Juridische en compliance-risico's verminderen door te waarborgen dat applicaties voldoen aan toepasselijke beveiligingsvereisten uit wet- en regelgeving.

**4. Rollen en verantwoordelijkheden**

**4.1 Algemeen directeur (GM)**

4.1.1 Draagt de eindverantwoordelijkheid voor applicatiebeveiliging binnen de organisatie.

4.1.2 Keurt dit beleid goed en waarborgt dat alle inkoop- of ontwikkelingsprojecten hieraan voldoen.

4.1.3 Waarborgt dat leveranciers en dienstverleners contractueel zijn gebonden aan vereisten voor applicatiebeveiliging.

4.1.4 Beoordeelt en keurt risico-uitzonderingen goed wanneer volledige naleving wegens zakelijke beperkingen niet haalbaar is.

**4.2 Applicatie-eigenaar (indien aangewezen)**

4.2.1 Identificeert applicatiespecifieke beveiligingsbehoeften tijdens systeemselectie of projectinitiatie.

4.2.2 Verifieert dat kernfunctionaliteiten zoals aanmeldbeveiliging, versleuteling en activiteitenlogging zijn opgenomen.

4.2.3 Neemt deel aan risicobeoordelingen voorafgaand aan uitrol en bevestigt dat beveiligingsmaatregelen aansluiten op zakelijke behoeften.

[ ... 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 eenmaal per kalenderjaar door de algemeen directeur worden beoordeeld om:**

9.1.1 wijzigingen in vereisten uit wet- en regelgeving te verwerken (bijvoorbeeld AVG, NIS2, DORA)

9.1.2 nieuwe of opkomende dreigingen en aanvalstechnieken op te nemen

9.1.3 formuleringen en vereisten bij te werken in lijn met wijzigingen in platforms, leveranciers of ontwikkelmethoden

**9.2 Tussentijdse beoordelingen moeten eveneens worden uitgevoerd wanneer:**

9.2.1 nieuwe applicaties worden geïntroduceerd

9.2.2 bestaande applicaties significante updates of integraties ondergaan

9.2.3 zich een applicatiegerelateerd incident of een applicatiegerelateerde inbreuk voordoet

9.2.4 nieuwe risico's worden vastgesteld op basis van externe dreigingsinformatie of waarschuwingen uit de sector

**9.3 Alle actualisaties van dit beleid moeten:**

9.3.1 worden goedgekeurd door de algemeen directeur

9.3.2 worden gedocumenteerd met versiehistorie en reden voor wijziging

9.3.3 worden gecommuniceerd aan alle werknemers, ontwikkelaars en leveranciers die betrokken zijn bij applicatiebeheer

9.3.4 veilig worden opgeslagen ten behoeve van audit- en compliancereferentie

## 10. Gerelateerde beleidslijnen en samenhang

**10.1 Dit beleid wordt rechtstreeks ondersteund door en draagt bij aan de handhaving van de volgende op het mkb afgestemde beveiligingsbeleidslijnen:**

10.1.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: wijst verantwoordelijkheid toe voor het goedkeuren van applicaties, het handhaven van beleid en het beheren van leveranciers.

10.1.2 P4S – Beleid inzake toegangscontrole: waarborgt dat applicatietoegang aansluit op het beginsel van minimale bevoegdheden en principes van sessiebeheer.

10.1.3 P8S – Informatiebeveiligingsbewustzijns- en opleidingsbeleid: waarborgt dat gebruikers en ontwikkelaars zijn opgeleid in het herkennen en melden van applicatiegerelateerde dreigingen.

10.1.4 P17S – Beleid inzake gegevensbescherming en privacy: biedt waarborgen voor gegevensprivacy die moeten worden afgedwongen door iedere applicatie die persoonsgegevens verwerkt.

10.1.5 P14S – Gegevensbewarings- en vernietigingsbeleid: regelt hoe door applicaties gegenereerde logboeken, back-ups en gevoelige gegevens moeten worden bewaard, gearchiveerd en veilig vernietigd.

10.1.6 P30S – Incidentresponsbeleid (P30): beschrijft de stappen voor het identificeren, melden en indammen van applicatiegerelateerde beveiligingsgebeurtenissen.

10.2 Gezamenlijk waarborgen deze beleidslijnen dat applicatiebeveiliging volledig is geïntegreerd in het managementsysteem voor informatiebeveiliging (ISMS) van de organisatie en aantoonbaar compliant is.

## 11. Referentienormen en -raamwerken

**11.1 ISO/IEC 27001**

11.1.1 Clausule 8.1 – Vereist dat organisaties operationele beheersmaatregelen vaststellen om informatiebeveiligingsrisico's te adresseren, waaronder risico's die verband houden met applicaties en softwaresystemen.

**11.2 ISO/IEC 27002**

11.2.1 Beheersmaatregel 8.25 – Adviseert het implementeren van veilige ontwerp-, ontwikkelings- en codereviewpraktijken voor alle applicaties, inclusief applicaties die door leveranciers worden geleverd.

11.2.2 Beheersmaatregel 8.26 – Beveelt formele testen aan van beheersmaatregelen voor applicatiebeveiliging, met name op gebieden zoals toegangscontrole, invoervalidatie en sessieafhandeling.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 SA-11 – Specificeert vereisten voor testen door ontwikkelaars, codeanalyse en dynamische applicatiescans vóór uitrol.

11.3.2 SI-10 – Richt zich op detectie en preventie van veelvoorkomende softwarefouten, met nadruk op bewustwording bij ontwikkelaars en technische waarborgen.

**11.4 AVG (EU 2016/679)**

11.4.1 Artikel 25 – 'Gegevensbescherming door ontwerp en door standaardinstellingen' vereist dat privacy en beveiliging in het kernontwerp van applicaties die persoonsgegevens verwerken worden ingebed.

**11.5 NIS2-richtlijn (EU 2022/2555)**

11.5.1 Artikel 21(2)(a) en (e) – Vereist dat essentiële en belangrijke entiteiten technische maatregelen implementeren om applicaties te beveiligen en softwarerisico's te detecteren.

**11.6 DORA (EU 2022/2554)**

11.6.1 Artikel 9(2)(c), 10(2)(c) – Vereist dat mkb-organisaties in de financiële sector beveiligingsmaatregelen op applicatieniveau inbedden en periodieke beoordelingen uitvoeren om de digitale operationele weerbaarheid te behouden.

**11.7 COBIT 2019**

11.7.1 BAI03 – 'Manage Solutions Identification and Build' geeft richting aan de ontwikkeling of verwerving van veilige software die is afgestemd op risico's, naleving en zakelijke vereisten, ook in mkb-omgevingen met beperkte middelen.