

Beleid Systeem & Software ontwikkeling

Proceseigenaar: Alex Baltus

15-06-2026 | 2.2

Inhoud

1	Over dit document	3
1.1	Doel, toepassingsgebied en gebruikers	3
1.2	Normatieve verwijzingen Annex A.....	4
1.3	Gerefereerde documenten	4
1.4	Geldigheid en documentbeheer	4
2	Betrokkenheid van het management bij dit beleid.....	5
2.1	Rollen en verantwoordelijkheden.....	5
3	Beleid	6
3.1	Toepassingsbeveiligingseisen en Veilige systeemarchitectuur en technische uitgangspunten.....	6
3.2	Beveiligen tijdens de ontwikkelcyclus en Testen van de beveiliging tijdens ontwikkeling en acceptatie	6
3.3	Uitbestede systeemontwikkeling en Veilig Coderen	7
3.4	Scheiding van ontwikkel-, test en productieomgevingen.....	8
3.5	Testgegevens.....	9
4.	Van toepassing zijnde controls.....	9

1 Over dit document

1.1 Doel, toepassingsgebied en gebruikers

Om zorg te dragen dat VfPf en VfPf medewerkers altijd in staat zijn om de kerntaken van de organisatie uit te voeren dient de bedrijfsvoering beschermd te worden tegen inbreuken op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie en processen.

Dit document is bedoeld om de eisen en richtlijnen weer te geven waar leveranciers zich aan dienen te houden bij het ontwikkelen van software en informatiesystemen ten behoeve van VfPf.

Normatieve verwijzingen Annex A

Dit beleid geeft invulling aan de volgende elementen van de Annex A – ISO 27001:2022:

- A8.25 Beveiligen tijdens de ontwikkelcyclus
- A8.26 Toepassingsbeveiligingseisen
- A8.27 Veilige systeemarchitectuur en technische uitgangspunten
- A8.28 Veilig coderen
- A8.29 Testen van de beveiliging tijdens ontwikkeling en acceptatie
- A8.30 Uitbestede systeemontwikkeling
- A8.31 Scheiding van ontwikkel-, test en productieomgevingen
- A8.33 Testgegevens

1.2 Gerefereerde documenten

In dit beleidsdocument wordt gerefereerd aan de volgende beleidsdocumenten en richtlijnen:

- ISO 27001 – 2022
- ISO 27002 – 2022
- Technisch Security Beleid (TSB)
- De richtlijnen voor het bouwen van webapplicaties NCSC
- Handreiking Cybersecuritymaatregelen van het NCSC
- Proces afhandelen wijziging
- Factsheet ransomware van het NCSC
- CIP document “testen met persoonsgegevens”

1.3 Geldigheid en documentbeheer

De eigenaar van dit document is het procesverantwoordelijke IT. Deze dient het document minimaal één keer per jaar te beoordelen. Jaarlijks vindt er een review van dit document plaats, deze is als terugkerende taak #432 opgenomen in de GRC-tool (Trustbound).

Versie:	2.2
Versiedatum:	15-06-2026
Gemaakt door:	Jacqueline de Jonge
Goedgekeurd door:	Alex Baltus
Classificatie:	Intern

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
16-04-2025	2.0	Joost Vaessen	Vernieuwing beleid systeem & software ontwikkeling t.b.v. nieuwe ISO 27001 norm.

9-7-2025	2.0	Jacqueline de Jonge	Controls in samenspraak met Contractmanager aangepast.
13-07-2025	2.0	Alex Baltus	Goedgekeurd
16-12-2025	2.1	Marco Osephius	Aanvulling mbt Saas-diensten
15-06-2026	2.2	Jacqueline de Jonge	Jaarlijkse review document
20-07-2026	2.2	Alex Baltus	Goedgekeurd (via Trustbound)

2 Betrokkenheid van het management bij dit beleid

2.1 Rollen en verantwoordelijkheden

Om te kunnen waarborgen dat de bedrijfsvoering van VfPf beschermd is tegen inbreuken op de BIV van processen en informatie dient dit document onderhouden te worden. Het management heeft de taak om:

- Review van dit document mee te nemen tijdens de review van het bovenliggende beleid, namelijk het Technisch Security Beleid, dit TSB wordt jaarlijks geëvalueerd of wanneer dit nodig is.
- Voldoende tijd, geld, kennis en andere middelen beschikbaar te stellen voor review en onderhoud.

Aan het opstellen van dit document zijn rollen en verantwoordelijkheden verbonden. Deze zijn hieronder weergegeven in een RASCI-Matrix, de uitleg van de matrix is te vinden in bijlage 2 van het Technisch Security Beleid.

	Change	Proceseigenaar IT	Run	Privacy&Security, Align	Contract-manager	Procesmanager
Beleid Systeem en Software ontwikkeling	R	A	S	C	I	I
Jaarlijkse controls bij leveranciers	C	A	S	C	R	I

R= Responsible; A= Accountable; S=Supportive; C= Consulted; I= informed

3 Beleid

Informatiebeveiliging dient integraal onderdeel uit te maken van informatiesystemen in de gehele levenscyclus. Dit betreft ook eisen voor de informatiesystemen die via openbare netwerken worden geleverd.

3.1 Toepassingsbeveiligingseisen en Veilige systeemarchitectuur en technische uitgangspunten

Bij nieuwe informatiesystemen, of uitbreidingen daarop, gelden de volgende regels:

- Bij het ontwikkelen van webapplicaties worden ICT-Beveiligingsrichtlijnen voor Webapplicaties van het Nationaal Cyber Security Centrum (NCSC) gehanteerd
- Het ontwikkelen (bouwen), opleveren en koppelen van nieuwe IT-systemen (t/m besturingssystemen) moet uitgevoerd worden volgens de daarvoor opgestelde procedures
- Bij grote wijzigingen (projecten) moet in een vroeg stadium een risicobeoordeling worden uitgevoerd om de benodigde beheersmaatregelen te identificeren ("Risk & Impact analyse")
- De communicatieroute tussen alle betrokken partijen moet versleuteld zijn
- De protocollen voor de communicatie tussen alle betrokken partijen moeten beveiligd zijn
- Wanneer gebruik wordt gemaakt van een vertrouwde autoriteit (bijvoorbeeld voor het uitgeven en onderhouden van elektronische handtekeningen en/of digitale certificaten) is de beveiliging geïntegreerd en ingebed in de gehele keten van het certificaat/handtekeningbeheerproces.

3.2 Beveiligen tijdens de ontwikkelcyclus en Testen van de beveiliging tijdens ontwikkeling en acceptatie

Voordat een wijziging van de applicaties wordt doorgevoerd:

- Moet er een beoordeling plaatsvinden van de beheersmaatregelen en integriteitprocedures voor de toepassing, om te waarborgen dat zij niet gecompromitteerd worden door de wijzigingen in het bedieningsplatform
- Moet gezorgd worden dat wijzigingen in het bedieningsplatform tijdig worden aangekondigd, zodat de noodzakelijke tests en beoordelingen kunnen worden uitgevoerd voordat de wijzigingen worden geïmplementeerd

- Moeten er testplannen ontwikkeld worden of aanwezig zijn
- Er wordt binnen VfPf, zover mogelijk en praktisch uitvoerbaar, gebruik gemaakt van kant-en-klaar geleverde (vendor supplied) programmatuur
- Systeem- en acceptatietesten vereisen doorgaans grote hoeveelheden testgegevens, die een zo getrouw mogelijke weergave moeten zijn van operationele gegevens
- Het gebruik van kopieën van operationele data voor testdoeleinden, moet worden vermeden. Indien er, voor bepaalde tests, toch gebruikt gemaakt moet worden van operationele data, wordt er een omgeving gemaakt die dezelfde security bevat als de productie omgeving. Als dit nodig is, dan alleen als uitzondering en met strikte voorwaarden die vooraf door het management moet worden goedgekeurd.
- Bij een acceptatietest kan het in uitzonderlijke gevallen noodzakelijk zijn de originele klantgegevens te gebruiken. Aanvullende maatregelen zijn dan nodig.

3.3 Uitbestede systeemontwikkeling en Veilig Coderen

VfPf heeft alle softwareontwikkeling volledig uitbesteed bij leveranciers. Daarbij is in de basis de paragraaf rondom Veilig Coderen niet van toepassing op VfPf. Wel stelt VfPf iedere leverancier verantwoordelijk voor het veilig ontwikkelen van de software die zijn aan VfPf leveren.

Onder deze verantwoordelijkheden vallen:

1. In het geval van het ontwikkelen van (informatiesystemen) wordt een Programma van Eisen opgesteld welke bestaat uit de eisen van het beleid binnen het ISO 27001 managementsysteem van VfPf
2. Iedere leverancier heeft minimaal een ISO 27001 certificering met daarbij systeemontwikkeling en/of softwareontwikkeling in scope
3. Iedere leverancier laat minimaal jaarlijks vulnerabilities scannen en voert pentesten uit. Resultaten worden gedeeld met VfPf
4. Waarborgen dat alleen bevoegd personeel wordt ingezet bij softwareontwikkeling waarbij geheimhouding onderdeel is van contracten
5. Industriestandaards worden gehanteerd op basis van door het NCSC voorgeschreven beveiligingsniveau op vlakken van encryptie en netwerken
6. Iedere leverancier stelt een OTAP Straat ter beschikking
7. Iedere leverancier hanteert een Risk & Impact analyse
8. In het geval van softwareontwikkeling heeft de leverancier een professioneel ontwikkelingsproces gedefinieerd en geïmplementeerd, waarbij minimaal rekening wordt gehouden met:
 - a. Scheiding in rollen tussen development en deployment;
 - b. Kwaliteitscontroles en vier-ogen-principes;
 - c. Toepassing van het OWASP-Top 10 model;
 - d. Toetsing van code op basis van de CVE-Vulnerabilities database;

VfPf voert audits uit om deze standaarden te toetsen bij de leverancier.

3.4 Scheiding van ontwikkel-, test en productieomgevingen

Bij het ontwikkelen, gebruiken en deactiveren van software kunnen veel risico's voor de bedrijfsvoering komen kijken. Denk bijvoorbeeld aan het doorvoeren van een niet goed geteste change (wijziging) waardoor informatie niet langer beschikbaar is, of het gebruiken van een softwareversie die het mogelijk maakt om onbevoegd toegang te krijgen tot de informatiesystemen van VfPf. Om te voorkomen dat fouten bij softwareontwikkeling nadelige gevolgen creëren voor de bedrijfsvoering van VfPf moeten de omgevingen voor het ontwikkelen, testen, accepteren en de productie omgeving van elkaar gescheiden worden.

Aanvullende eis voor SaaS-diensten

Voor alle door VfPf afgenomen SaaS-diensten moet de leverancier beschikken over een aantoonbaar gecontroleerd wijzigings- en releaseproces, ingericht conform de uitgangspunten van ISO/IEC 27001 voor wijzigingsbeheer en risicobeheersing.

De SaaS-dienst moet aan VfPf minimaal een productieomgeving én een daarvan logisch en/of technisch gescheiden acceptatieomgeving, acceptatie-achtige omgeving of functioneel equivalent ter beschikking stellen. Deze omgeving moet VfPf in staat stellen om wijzigingen, updates, releases, configuratieaanpassingen en koppelingen vooraf te toetsen en te accepteren voordat deze impact hebben op de productieomgeving.

Wijzigingen mogen niet rechtstreeks in productie worden doorgevoerd zonder voorafgaande validatie en beheerste vrijgave. De leverancier moet aantonen dat productiegegevens, test-/acceptatiegegevens en gegevensstromen gescheiden blijven en dat beheer, logging, autorisaties en releasebesluiten per omgeving controleerbaar zijn ingericht.

Verantwoordelijkheden van leveranciers

Leveranciers zijn verantwoordelijk voor het volgende:

- Beleid en procedures opstellen voor het scheiden van omgevingen op basis van het VfPf classificatiebeleid en de meest recent gebruikte versie van ISO 27001/2. Hierbij hoort ook een operationeel beleidsdocument waarin de uitgangspunten die per zone gehanteerd worden staan beschreven. Er wordt, minimaal eens per jaar beoordeeld of de inrichting van systemen in zones nog optimaal is.
- Het bezitten van een ISO 27001 certificaat met het scheiden van omgevingen binnen de scope van dit certificaat.
- Het scheiden van omgevingen in een OTAP-straat. Op basis van de Richtlijnen voor het bouwen van webapplicaties vanuit het NCSC. Dit is van toepassing voor de applicaties welke zijn vastgesteld als zijnde bedrijf kritisch en waarbij de BIV-classificatie hoog scoort ten aanzien van Beschikbaarheid.
- Beleid en procedures op te stellen om te waarborgen dat omgevingen correct gescheiden worden en informatie op veilige wijze van omgeving naar omgeving gemigreerd wordt.
- Zorg te dragen dat ontwikkelsoftware en productiesoftware op virtuele systemen in verschillende domeinen draaien.

- Zorg dragen dat de acceptatie omgeving een accurate reflectie is van de inrichting van de productie omgeving en dat tests niet uitgevoerd worden op productie omgevingen.
- Zorg te dragen dat alleen goedgekeurde en geauthentiseerde bedrijfsmiddelen beveiligd worden aangesloten op een vertrouwde zone.
- Zorg te dragen dat gebruikers activiteiten uitvoeren waarbij gebruik gemaakt wordt van verschillende profielen die zijn goedgekeurd voor gebruik voor operationele of testsystemen.
- Beveiliging van de respectievelijke omgevingen op basis van de informatie die daarop te vinden is en de classificatie van deze informatie volgens het VfPf classificatiebeleid.
- Het sluiten van gateways (poorten), diensten en soortgelijke voorzieningen op netwerken die niet vereist zijn voor het uitvoeren van de dienst.

Rol van de Managed Service Provider

De Managed Service Provider heeft de taak om werkstations zo in te richten dat het routeren van verkeer tussen zones of netwerken niet mogelijk is.

3.5 Testgegevens

Het gebruik van kopieën van operationele data voor testdoeleinden, moet worden vermeden. Indien noodzakelijk, worden geanonimiseerde gegevens gebruikt welke na de test zorgvuldig worden verwijderd.

Ook worden er eisen gesteld aan het testen van de BIV van persoonsgegevens op basis van het CIP document “testen met persoonsgegevens”.

4. Van toepassing zijnde controls

Onderstaande controls dienen te voldoen aan de hiervoor de van toepassing zijnde beheersmaatregelen zijn afgeleid van het Privacybeleid & Securitybeleid en het Technisch Security Beleid (TSB) van VfPf.

Nummer	Control doelstelling	Control beschrijving	Frequentie
SO 1.1	Systeem en softwareontwikkeling wordt beheerst	Jaarlijks wordt op de kritische leveranciers een audit uitgevoerd ten behoeve van de processen voor systeem- en/of softwareontwikkeling.	Zie security assessment kalender in Trustbound taak #306 (Leveranciersmanagement)

SO 1.2	Systeem en softwareontwikkeling wordt beheerst	Jaarlijks wordt aan de hand van de leveranciersbeoordeling beoordeeld of leveranciers waar systeem en softwareontwikkeling naar wordt uitbesteed een ISO 27001 certificering hebben met daarbij systeemontwikkeling en/of softwareontwikkeling in scope.	Zie security assessment kalender in Trustbound taak #322 (Leveranciersmanagement)
SO 1.3	Systeem en softwareontwikkeling wordt beheerst	Jaarlijks wordt gecontroleerd of iedere leverancier die systemen of software ontwikkeld op verzoek van VfPf Vulnerability Scans uitvoert en de resultaten deelt met VfPf.	Zie security assessment kalender in Trustbound taak #324 (Leveranciersmanagement)
SO 1.4	Systeem en softwareontwikkeling wordt beheerst	Jaarlijks wordt gecontroleerd of iedere leverancier die systemen of software ontwikkeld op verzoek van VfPf een Pentest heeft uitgevoerd en de resultaten daarvan heeft gedeeld met VfPf.	Zie security assessment kalender in Trustbound taak #325 (Leveranciersmanagement)

Met opmerkingen [JJ1]: In SLA rapportage?