c

Technisch Security Beleid VfPf

21-06-2024 | 1.4

Vervangingsfonds
Participatiefonds

Inhoud

Documentinformatie en -geschiedenis

Versie:	1.4
Versiedatum:	21-06-2024
Gemaakt door:	J. Jansen
Goedgekeurd door:	A. Baltus
Classificatie:	intern

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
21-5-2021	0.9	M. Engels	Concept basisdocument
05-7-2021	0.95	M. Engels	Aanpassingen naar aanleiding van feedback op eerste stuk.
18-11-2021	1.0	M. Engels	Terminologie afgestemd op bovenliggend beleid
14-7-2022	1.1	M. Engels	Aanpassing A9 m.b.t authenticatie en autorisatie
25-7-2022	1.1	M. Engels	Aanpassing Documenteigenaar
10-8-2022	1.1	Alex Baltus	Goedkeuring versie 1.1
05-06-2023	1.2	Patrick van den Heuvel	Aanvullingen n.a.v. ISO audit, evaluatie van onder- en bovenliggende stukken
28-09-2023	1.25	Patrick van den Heuvel	Aanvullingen van hoofdstuk 11 koppeling aan leveranciersbeoordeling en evaluaties van applicaties
21-05-2024	1.3	Joop Jansen	Aanvullingen hoofdstuk 4 n.a.v. afwijkingenregister
21-06-2024	1.4	Joop Jansen	Aanvulling hoofdstuk 9 Communicatiebeveiliging

1. Over dit beleidsdocument

Doel, toepassingsgebied en gebruikers

Dit Technisch Security-Beleid is gericht op het definiëren van het doel, de richting, de principes en de basisregels voor Informatiebeveiliging binnen de technische omgevingen van VfPf. Het vormt hierbij op strategisch en tactisch niveau kaders ten behoeve van procedures en technische maatregelen.

Naast dit technisch Security Beleid heeft VfPf ook een Privacy en Securitybeleid opgesteld voor alle medewerkers.

Dit technisch Security Beleid is van toepassing op het toepassingsgebied (de scope) van het Informatie Security Managementsysteem (ISPMS), zoals bepaald in P&S Handboek.

Gebruikers van dit document zijn alle werknemers van het IV-regieteam en de facilitaire afdeling van VfPf, als ook de relevante externe partijen.

Gerefereerde documenten

- ISO/IEC 27001
- ISO/IEC 27002
- Begrippenlijst Privacy & Security (P&S)
- Uitleg RASCI model
- Classificatiebeleid VfPf
- Privacy- en Security-beleid VfPf
- P&S Handboek

Geldigheid en documentbeheer

Dit document is geldig vanaf de definitieve versie datum.

De eigenaar van dit document is de Procesverantwoordelijke IT binnen VfPf. Deze dient het document te minsten één keer per jaar te beoordelen en indien nodig te laten bijwerken. Volgens de PDCA Cyclus.

Gehanteerde definities en concepten

Zero trust[1]

Zero trust is een principe dat ontwikkeld door John Kindervag, met als basisgedachte; never trust, always verify. Volgens het zero trust principe wordt niet vertrouwd op het bestaan van een 'veilig

[1] Bron: https://www.ncsc.nl/actueel/weblog/weblog/2020/what-about-zero-trust

intern netwerk'. Dit principe gaat uit van segmentering waarmee er een opdeling in verschillende zones ontstaat.

Deze helpen bij het structureren van een of meerdere functionaliteiten door het implementeren van een set aan beveiligingseisen. Eenmaal voldaan aan deze eisen, kan er toegang worden verkregen. Toegang tot deze zones gaat gepaard met sterke authenticatie en autorisatie en het monitoren hierop.

Het zero trust gedachtengoed heeft drie overkoepelende hoofdconcepten.

1. Authenticatie en autorisatie
   Zero trust gaat uit van: “Never trust, always verify”. Dit bestaat uit een sterke controle van identiteit. Wanneer een gebruiker voldoet aan bepaalde vooraf gestelde bedrijfs-policies, dan pas krijgt deze gebruiker toegang tot de functionaliteit.
   Elke keer wanneer een gebruiker toegang wil tot functionaliteiten, dient een verificatie van diens geclaimde identiteit plaats te vinden.
   Autorisatie dient plaatst te vinden op functionaliteiten en op basis van het need-to-know principle. Dit betekent dat de gebruiker alleen toegang krijgt tot tools, data en zones die daadwerkelijk nuttig zijn voor het werk dat diegene doet.
2. Netwerk segmentatie
   Segmentering is het opdelen van zones. Het hebben van kleinere zones (e.g. microservices in containers) is meer in lijn met de zero trust gedachte in plaats van grotere zones (e.g. netwerksegmenten). In grotere netwerksegmenten is er minder controle mogelijk. Praktisch is dit een balans vinden van zo klein mogelijke functionele netwerksegmenten en een werkbare controle op de toegang van die segmenten.
3. Monitoring
   Een ander onderdeel van zero trust is het monitoren van apparaten, gebruikers en services. Een monitorproces inrichten kan op basis van vooraf bepaalde rollen en policies. Het doel hiervan is om mogelijk misbruik te detecteren en zo dreigingen het hoofd te bieden.
   Het monitorproces gebruikt logging om inzicht te krijgen. Zo kan bijvoorbeeld geverifieerd worden of gebruikers geen rollen/policies overschrijden. Een mogelijk respons hierop kan toegang ontzegging tot een zone zijn.

De bovenstaande concepten hebben we (mede) gebruikt om verschillende onderwerpen in dit document vorm te geven. Enkele voorbeelden hiervan zijn:

- Gebruik van MFA om toegang te krijgen tot systemen.
- Gebruikers en systeemaccounts hebben alleen toegang tot die informatie die ze nodig hebben om hun werk te doen.
- Netwerk is gesegmenteerd in applicatie zones.
- Inloggen in applicaties wordt gemonitord, samen met het aanmaken van accounts en wijzigen van rechten.

2. Betrokkenheid van het management bij dit beleid

De Procesverantwoordelijk IT levert met dit beleid een adequate, effectieve en efficiënte bijdrage aan de implementatie van het ISPMS en de doelstellingen die zijn genoemd in het P&S Beleid en het P&S Handboek. Dit betreft een algemeen beleid dat dat bekend moet zijn bij alle betrokken in het ISPMS.

Team P&S zal de opvolging en effectiviteit van dit beleid evalueren en rapporteren aan de directie.

Alle medewerkers van het IV Regieteam, Facilitair en alle van toepassing zijnde externe partijen die een rol hebben in het ISPMS, zorgen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.

3. Rollen en verantwoordelijkheden

Aan het Technisch Security Beleid zijn een aantal rollen en verantwoordelijkheden verbonden. In de onderstaande tabel zijn de rollen en verantwoordelijkheden vertaald in een RASCI-tabel en die zijn gekoppeld aan rollen binnen de VfPf organisatie. In bijlage 2 is de uitleg van het RASCI-model beschreven.

	Proces-verantwoordelijk IT	Systeem-eigenaar	Architect	Service Management	Change	Run	Facilitair	Privacy & Security
Technisch Security Beleid	A		R	C				C
Beheer van bedrijfsmiddelen (A8)	A		S	I		R		I
Logisch Toegangsbeleid (A9)	R	A		I		R		I
Cryptografie (A10)	A		R	I				I
Fysieke toegangsbeveiliging (A11)	A			I		S	R	I
Beveiliging Bedrijfsvoering A12)	A		C	I	R	S		I
Communicatiebeveiliging (A13)	A			S				I
Acq, ontw, en onderhoud IV (A14)	A		C	S	R	S		C
Controleren van gestelde kaders en beleid	A		R	C	I	I		C

4. Beheer van bedrijfsmiddelen (A8)

Bedrijfsmiddelen in de context van dit document zijn informatiesystemen en andere informatie/apparatuur, inclusief papieren documenten, mobiele telefoons, draagbare computers, media voor gegevensopslag, enz. Deze dienen op een gestructureerde manier te worden uitgegeven en ingenomen. Tevens dient ieder bedrijfsmiddelmiddel te zijn geïdentificeerd en dienen passende maatregelen ter bescherming van de data en informatie te zijn gedefinieerd.

Het beleid op beheer van bedrijfsmiddelen is als volgt gedefinieerd:

Informatie / Informatiesystemen

- Voor ieder bedrijfsmiddel binnen VfPf is een eigenaar gedefinieerd.
- Ieder bedrijfsmiddel binnen VfPf is voorzien van een Data- en BIV classificatie.
- Voor ieder bedrijfsmiddel worden toegangsbeperking en bescherming overeenkomstig met de maatregelenset van VfPf gehanteerd op basis van de opgestelde Data- en BIV classificatie.

Apparatuur (Devices)

Laptops manged devices.

- Uitgangspunt bij het gebruik van laptops is het gebruik van managed devices. Medewerkers kunnen alleen inloggen vanaf apparaten die worden beheerd en goedgekeurd door VfPf. Apparaten die niet worden beheerd door VfPf worden geblokkeerd en krijgen dus geen toegang tot onze omgeving.
- Met Mobile Device Management (MDM) worden laptops op afstand beheerd. Zodat VfPf de controle houdt over de data waarmee medewerkers werken op mobiele apparaten.
- Het is niet mogelijk om verwijderbare media zoals USB sticks, CD-roms te gebruiken op de door VfPf uitgegeven (managed) devices zoals laptops en telefoons.
- Bij inname van media zoals telefoons, laptops e.d. worden harde schijven gewist.

Mobile Devices worden met MAM beheerd.

- Met Mobile Application Management (MAM) zijn apps op mobile devices van de medewerkers te publiceren, pushen, configureren, beveiligen, controleren en bij te werken. Zodat medewerkers werken met de laatste versie van de juiste apps en data van de organisatie veilig blijft. Dit is beschikbaar voor IOS en Android OS devices.

5. Beleid voor logische toegangsbeveiliging (A.9)

Logische toegangsbeveiliging moet ervoor zorgen dat toegang tot voorzieningen en gegevens wordt verleend aan gebruikers die daartoe zijn gerechtigd en wordt geweigerd aan anderen. Het doel ervan is te waarborgen dat het lezen, toevoegen, wijzigen en verwijderen van gegevens en programmatuur alleen door bevoegden en gecontroleerd kan plaatsvinden. Toegangsbeveiliging strekt zich uit over alle middelen voor de informatievoorziening: centrale computers, netwerken, werkstations, systeem- en toepassingsprogrammatuur en gegevens. Voor het beleid logische toegangsbeveiliging VfPf worden de volgende uitgangspunten worden gehanteerd:

- VfPf maakt, waar mogelijk, gebruik van eHerkenning voor bedrijven en DigiD voor personen ten behoeve van authenticatie en autorisatie.
- VfPf maakt ten behoeve van authenticatie en autorisatie voor interne medewerkers en medewerkers van externe partijen, die namens VfPf werkzaamheden uitvoeren aan het informatielandschap van VfPf, gebruik van standaardprofielen in de Microsoft Azure AD.
- Het regieteam IV Run is verantwoordelijk voor het opstellen van generieke autorisatieprocedures en daarbij behorende instrumenten zoals de autorisatiematrix.
- Voor elk informatiesysteem en gegevensverzameling is een verantwoordelijke eigenaar benoemd.
- Iedere systeemeigenaar is verplicht tot het (laten) uitvoeren van een baselinetoets ISO27001 en, afhankelijk van de uitkomsten van deze baselinetoets ISO27001, ook nog voor een diepgaande risicoanalyse voor de informatiesystemen waarvan hij eigenaar is.
- Iedere systeemeigenaar is verplicht tot het maken van een specifieke autorisatiematrix voor elk informatiesysteem waarvan hij eigenaar is.
- Het IV regieteam Run en de systeemeigenaren dienen bij het opstellen en uitvoeren van een specifieke autorisatieprocedure de volgende uitgangspunten te hanteren:
    - De autorisatiestructuur van een informatiesysteem is uniform voor VfPf.
    - De autorisatiestructuur van een informatiesysteem sluit aan bij goedgekeurde procesbeschrijvingen.
    - Er worden in de regel geen ‘algemene’ (ongepersonaliseerde) identiteiten gebruikt. Dit geldt ook voor ‘API-users’.
    - Gegevens worden alleen gemuteerd door de dataeigenaar of de daartoe, door de gegevenseigenaar, gemachtigde functionarissen.
    - De systeemeigenaar overlegt met de betrokken gegevenseigenaren en proceseigenaren over de vraag wie geautoriseerd wordt op basis van het ‘need to know’ en ‘need to use’-principe en op welke manier dat gebeurt.
    - Er is een centraal overzicht van toegangsrechten die een gebruikersidentificatie zijn toegekend om toegang te verkrijgen tot informatiesystemen en –diensten (Identity Access Management IAM).

Functiescheiding

- De beschikkende, bewarende en controlerende taken worden in beginsel nooit in één functionaris tezamen gebracht. Indien dit toch noodzakelijk is dan wordt door de systeemeigenaar apart toezicht georganiseerd op de betreffende functionaris.
- (Technische) beheerders mogen in beginsel geen toegang hebben tot de data van het informatiesysteem waar zij (technisch) beheerder van zijn. Indien dit toch noodzakelijk is dan wordt door de systeemeigenaar apart toezicht georganiseerd op de betreffende functionaris.

Inhuur externen

- De door VfPf ingehuurde externen vallen onverkort onder het beleid logische toegangsbeveiliging en dienen conform deze regels te handelen.
- Aan de hand van hun taken/functie zal hun toegang verleend worden tot de gegevens en informatiesystemen.

Uitbesteding aan een ICT-dienstverlener

- De ICT-dienstverlener dient ISO 27001 te zijn gecertificeerd. Waarbij de afgenomen dienstverlening binnen scope valt van certificering en de verklaring van toepasselijkheid hierbij aansluit.
- De ICT-dienstverlener dient een beveiligingsbeleid en geëffectueerde maatregelen te hebben, die zij aan VfPf inzichtelijk maakt die in lijn zijn met dit beleid.
- De ICT-dienstverlener voldoet aan de normen en eisen die gesteld zijn in het Technisch Security Beleid van VfPf en de van toepassing zijnde wet- en regelgeving, en zorgt voor de naleving hiervan.
- Binnen de ICT-dienstverlener is een aanspreekpunt voor security aanwezig die verantwoordelijk is voor het Security-beleid van de ICT-dienstverlener en die contactpersoon is voor VfPf.
- De normen en eisen aangaande de beveiliging zijn onderdeel van contractuele afspraken.
- De ICT-dienstverlener stelt uitsluitend in opdracht van VfPf toegang tot VfPf-informatie beschikbaar aan medewerkers van VfPf, de ICT-dienstverlener en aan derde partijen.
- De ICT-dienstverlener stelt capaciteit en informatie beschikbaar aan audits op gebied van autorisaties, die in opdracht van VfPf uitgevoerd worden.
- Voor de dagelijkse operatie is er bij de ICT-dienstverlener een autorisatiebeheerder aanwezig die verantwoordelijk is voor een correcte inrichting van de autorisaties en die aanspreekpunt is voor het IV Regieteam van VfPf.

Beoordeling van de uitvoering van het beleid

- De systeemeigenaar dient het toezicht op de uitvoering van de autorisatieprocedure goed te regelen en te documenteren. Hij neemt interne beheersmaatregelen die in overeenstemming zijn met de eisen die uit de baselinetoets ISO27001 of risicoanalyse voortvloeien.
- Jaarlijks wordt door het IV Regieteam een zelfassessment uitgevoerd op de uitvoering van het beleid logische toegangsbeveiliging. (1st line of defence)
- Jaarlijks dient de beoordeling van het beleid (het Technisch Security Beleid) plaats te vinden op basis van de PDCA cyclus en betrokkenen vanuit de RACI-matrix.
- Tussentijdse controles kunnen plaatsvinden door team P&S. De bevindingen en verbeteringen worden opgenomen in de P&S Jaarkalender en zijn mede onderdeel van de jaarlijkse controle door de onafhankelijke partij. Beoordeling vindt plaats op de volgende punten/onderdelen:
    - Of het beleid logische toegangsbeveiliging in overeenstemming is met de wet- en regelgeving en ander beleidsstukken.
    - Of de maatregelen passend zijn voor het beleid logische toegangsbeveiliging.
    - Of VfPf in voldoende mate het beleid naleeft.

Wachtwoordbeleid (gebruiker)

- Standaard of tijdelijke wachtwoorden, die in systemen zitten, worden voor ingebruikname gewijzigd.
- Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt de hashwaarde van het wachtwoord gecombineerd met een Salt opgeslagen of een minimaal gelijkwaardige oplossing.

Ten aanzien van wachtwoorden geldt:

- Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
- Tijdelijke wachtwoorden zijn in principe maximaal 24uur geldig.
- Gebruikers bevestigen de ontvangst van een wachtwoord.
- Wachtwoorden zijn alleen bij de gebruiker bekend.
- Wachtwoorden dienen te bestaan uit minimaal 8 karakters. Daarnaast stellen we de onderstaande aanvullende eisen voor wachtwoorden van normale gebruikers:
    1. Minimaal 1 hoofdletter
    2. Minimaal 1 cijfer en 1 bijzonder teken (!@#$ etc.)
    3. Je inlognaam mag niet gebruikt worden in het wachtwoord
    4. Je mag een wachtwoord 2 jaar lang niet hergebruiken
    5. Wachtwoorden worden elke 90 dagen gewijzigd
- Waar mogelijk maken we gebruik van MFA/2FA.

Aanvullend beleid voor accounts met verhoogd risico, systeembeheerders en systeemaccounts

Toegang tot besturingssystemen van VfPf behoort te worden beheerst met een beveiligde inlogprocedure. Hierbij worden de onderstaande uitgangspunten gehanteerd. Mochten deze maatregelen niet toepasbaar zijn, dan wordt de afwijking geregistreerd in het architectuur afwijkingen register met daarbij eventuele aanvullende maatregelen.

- Toegang tot kritische toepassingen of toepassingen met een hoog belang wordt verleend op basis van twee-factor authenticatie (Zie ISA BIV Classificatie).
- Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
- Voorafgaand aan het aanmelden wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
- Bij een succesvol loginproces wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.
- Gebruikers met speciale toegang kennen een wachtwoord van minimaal 16 karakters lang, maken gebruiken van multi-factor authenticatie en voldoen daarbij aan de dezelfde aanvullende eisen zoals gesteld voor normale gebruikers.
- Voor accounts met een verhoogd risico waaronder systeemaccounts (bv. systemen die bij andere systemen inloggen) geldt dat wachtwoorden minimaal 24 karakters lang zijn en voldoen daarbij aan de dezelfde aanvullende eisen zoals gesteld voor normale gebruikers. Wachtwoorden dienen ieder jaar te worden gewijzigd.

Wachtwoordbeheer

Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

- Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).
- Wachtwoorden hebben een geldigheidsduur. Binnen deze tijd dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd.
- Wachtwoorden die gereset zijn en initiële wachtwoorden hebben een geldigheidsduur van maximaal een dag (24h) en moeten bij het eerste gebruik worden gewijzigd.
- De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Bij het kiezen van een wachtwoord moet het wachtwoord voldoen aan de regels gesteld in het wachtwoord beleid.
- Voordat een gebruiker zijn wachtwoord kan wijzigen, wordt de gebruiker opnieuw geauthentiseerd.

6. Cryptografie (A10)

Cryptografie heeft als doel om correct en doeltreffend de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen. De Security-beleidsregels van VfPf met betrekking tot encryptie en Public Key Infrastructure (PKI) zijn:

- Alle gegevens (data at rest en data in transit) anders dan classificatiegroep 0, worden versleuteld conform beveiligingseisen die zijn beschreven in de maatregelenset naar aanleiding van Data en BIV-classificatie.
- Versleuteling vindt plaats conform passende standaarden vanuit NCSC richtlijnen waarbij geldt dat de vereiste encryptie sterker is naarmate het classificatieniveau hoger wordt. Hiervoor wordt gebruik gemaakt van het forum standaardisatie op basis van pas toe of leg uit. Dataverkeer tussen systemen ('machine to machine') wordt conform classificatie beveiligd met certificaten, waarbij:
    - PKIO certificaten worden toegepast op omgevingen waar productie data wordt gebruikt.
    - Self-signed certificaten worden toegepast op ontwikkel, test en acceptatie omgevingen.
- Het gebruik van https en hsts is verplicht (vanuit overheidswege).
- Om authenticatiemiddelen zoals wachtwoorden te beschermen tegen inzage en wijzigingen door onbevoegden tijdens transport en opslag, dienen deze te worden versleuteld.
- Om een correcte en veilige bediening van mobiele apparatuur en thuiswerkplek te waarborgen, is VfPf bevoegd om beveiligingsinstellingen af te dwingen. Dit heeft betrekking op alle door VfPf verstrekte middelen.
- Binnen VfPf zijn in de regel enkel managed devices toegestaan voor het inzien en verwerken van bedrijfsinformatie.
- Om bedrijfsinformatie op mobiele apparaten te beveiligen zijn deze zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ('zero footprint'). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, wordt de toegang tot het apparaat beschermd door middel van een wachtwoord en is apparaat versleuteling geïmplementeerd (conform classificatie-eisen). Dit gebeurt in ieder geval bij beveiligde opslag van VfPf informatie en bedrijfsinformatie van derde partijen, waar VfPf niet de bronhouder is, maar via het VfPf platform wordt ontsloten.
- Voor Clouddiensten (bijvoorbeeld toepassingen in SaaS, O365) geldt dat versleuteling geregeld is op een manier die recht doet aan de VfPf beschermingseisen op basis van het Classificatiebeleid en de daarbij behorende maatregelenset.

7. Fysieke beveiliging en beveiliging van de omgeving (A11)

Ten behoeve van de beveiliging van informatie is er toegangsbeleid voor alle VfPf voorzieningen. Het doel van dit beleid is te voorkomen dat onbevoegden toegang krijgen tot ruimtes met informatie waar zij geen kennis van behoren te nemen dan wel dat informatie kan worden aangepast. Het toegangsbeleid spitst zich daarnaast toe op de fysieke beveiliging van kantoren, ruimten en faciliteiten. VfPf hanteert de volgende beleidsuitgangspunten en deze zijn ontleend uit de ISO27002:

- VfPf heeft barrières aangebracht om ruimten te beschermen waar zich ICT-voorzieningen dan wel persoonsgegevens en/of gevoelige gegevens bevinden (op basis van het classificatiebeleid).
- Er is een zoneringsplan met daarin opgenomen de volgende zones: Openbaar, wachtruimten en spreekkamers, werkruimten, ICT-ruimte/beveiligde ruimte (persoons- of gevoelige gegevens).
- Gebouwen bieden voldoende weerstand bij gewelddadige aanvallen zoals inbraak en vandalisme, hierbij wordt ook rekening gehouden met de omgeving.
- De kwaliteit van de toegangsmiddelen hoort in overeenstemming te zijn met de zonering.
- Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie.
- In gebouwen met beveiligde zones houdt beveiligingspersoneel toezicht op de toegang en houdt hiervan een registratie bij.
- Er is 24 uur, 7 dagen per week bewaking met een inbraak alarm gekoppeld aan een alarmcentrale. Voor alle medewerkers die autorisatie hebben om het alarm te bedienen dient een persoonlijke code gebruikt te worden; er wordt geen gebruik gemaakt van een generieke code.
- Medewerkers/bezoekers zonder autorisatie mogen alleen onder begeleiding van bevoegd personeel en als er een noodzaak is, toegang krijgen tot de beveiligde omgeving.
- Zonder expliciete toestemming mogen in beveiligde ruimtes geen opnames (beeld en/of geluid) worden gemaakt.
- Niet uitgegeven toegangsmiddelen worden beveiligd opgeborgen.
- Toegangsmiddelen vallen onder de verantwoordelijkheid van HR / de facilitaire dienst.
- Er vindt één keer per half jaar een controle/evaluatie plaats op de autorisaties voor fysieke toegang. Voor speciale toegangsrechten is dat minimaal ieder kwartaal.
- De huisregels voor toegangsbeleid worden bekend gesteld aan al het personeel en de bezoekers.

8. Beveiliging bedrijfsvoering (A12)

Activiteiten op het gebied van ontwikkeling en testen kunnen ernstige problemen veroorzaken, zoals onbedoelde wijziging van bestanden of de systeemomgeving, of storingen in het systeem. In dit geval is een bekende en stabiele omgeving essentieel waarin zinvolle proeven kunnen worden uitgevoerd en waarin ongewenste toegang door ontwikkelaars kan worden voorkomen.

Om problemen in de operationele (productie)omgeving te voorkomen dienen de volgende punten te worden gehanteerd:

- Voor alle applicaties die het primaire proces ondersteunen hanteren we verschillende omgevingen om wijzigingen gecontroleerd in productie te nemen. We hanteren hiervoor een Ontwikkel, (Test,) Acceptatie en Productie omgeving.
- Er zijn regels gedefinieerd en gedocumenteerd voor het overdragen van programmatuur van ontwikkeling, via test en acceptatie naar operationele (productie) status;
- Ontwikkelings- en operationele programmatuur draait op verschillende systemen en in verschillende domeinen of directory's;
- Compilers en andere systeemhulpmiddelen zijn niet toegankelijk vanuit productiesystemen wanneer ze niet nodig zijn;
- De testomgeving komt zo goed mogelijk overeen met de productieomgeving;
- Gebruikers hebben verschillende gebruiksprofielen voor operationele- en testsystemen. Menu's tonen de juiste identificatieboodschappen teneinde het risico op fouten te verminderen;
- Er mogen geen gevoelige (vertrouwelijke) gegevens vanuit productiedata naar een ontwikkel-, test- en/of acceptieomgeving worden gekopieerd.

Bescherming tegen malware

De volgende uitgangspunten zijn vastgesteld voor VfPf en deze zijn ontleend aan het VfPf Security-beleid, de Code voor Informatiebeveiliging (NEN-EN-ISO/IEC 27002:2017 nl):

- Het is verboden om ongeautoriseerde software te downloaden of draaien op computersystemen van VfPf. Installatie van software wordt centraal door de managed service provider in opdracht van het Regieteam IV uitgevoerd.
- De processen wijzigingsbeheer en patchmanagement zijn ingericht. Alle computersystemen zijn altijd voorzien van de laatste firmware, software updates en patches, tenzij door een risicoafweging is vastgesteld en geaccordeerd, dat een bepaalde software update de dienstverlening van VfPf kan verstoren, in dat geval moeten er andere maatregelen worden onderzocht en genomen.
- Op alle systemen/applicaties/portalen van VfPf is anti-malware software aanwezig die geautomatiseerd controleert op de aanwezigheid van virussen, trojans en andere malware.
- Alle binnenkomende en uitgaande e-mails worden gecontroleerd op malware.
- De emailbeveiligingsstandaarden SPF, DKIM, DMARC en DANE zijn voor het domein van VfPf ingericht volgens de streefbeeldafspraken van forum standaardisatie. Daarbovenop is ook DNSSEC ingericht op het domein.
- De anti-malware software en bijbehorende herstelsoftware wordt regelmatig automatisch voorzien van nieuwe updates en dit moet centraal bewaakt worden. Uitzonderingen hierop moeten actief worden gemonitord en gerapporteerd aan het management en aan team P&S.

- Malware besmettingen en de vermoedens daarvan dienen onverwijld gemeld te worden volgens het Incident response plan.
- Alle malware besmettingen zijn incidenten van de zwaarste categorie. De gelogde incidentinformatie wordt minimaal 3 jaar bewaard en behandeld als bewijsmateriaal. Het Incident Responseplan van P&S dient daarbij te worden gevolgd.
- De backup en recovery procedures zijn opgesteld en ook getest op werking. Bij een malware besmetting kunnen originele bestanden worden teruggezet.
- VfPf heeft t.b.v. Informatiebeveiligingscontinuïteit processen, procedures en beheersmaatregelen vastgesteld om adequaat te kunnen reageren op een grote malware uitbraak. In het continuïteitplan is er een scenario opgenomen voor een grote malware uitbraak.

Back-up

Ten behoeve van de beveiliging van informatie is er back-up en recovery beleid voor alle VfPf voorzieningen. Het doel van dit beleid is te voorkomen dat in geval van gedeeltelijk of geheel verlies of beschadiging van data en/of programmatuur de dienstverlening van VfPf geen hinder ondervindt.

VfPf hanteert de volgende beleidsuitgangspunten en deze zijn ontleend aan de ISO27002 en aanvullend op het algemene beveiligingsbeleid van VfPf:

- VfPf heeft back-up en recovery processen bij leveranciers ingeregeld om de gevolgen van de uitval en/of het verlies van informatie te minimaliseren;
- Op basis van de data en BIV classificatie van het informatiesysteem worden Recovery Time Objective (RTO) en Recovery Point Objective (RPO) vastgesteld.
- In de SLA met de leverancier worden concreet de RTO en RPO vastgelegd.
- Vereiste back-up documentatie omvat de identificatie van alle belangrijke gegevens, programma's, documentatie en support items die nodig zijn om essentiële taken tijdens een herstelperiode te voeren. Documentatie van het recoveryproces moet procedures omvatten voor het herstel van single-systeem of applicatiestoringen, alsmede voor een totale database ramp scenario, indien van toepassing;
- De back-up en recovery procedures moet worden getest conform de documentatie en deze moet regelmatig worden bijgewerkt om rekening te houden met nieuwe technologie, veranderingen in het bedrijf, en de migratie van toepassingen naar alternatieve platforms;
- Recovery procedures moeten minimaal op jaarbasis worden getest;

Verslaglegging en monitoren

Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

- Van logbestanden worden rapportages en analyses gemaakt die periodiek, minimaal maandelijks, worden beoordeeld. Er is vastgesteld welke persoon en/of rol hier verantwoordelijk voor is.
- Een logregel bevat minimaal:
  - Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
  - De gebeurtenis
  - Waar mogelijk de identiteit van het werkstation of de locatie:
  - Host naam
  - Operating System (OS)
  - Naam van de toepassing
  - IP-adres(sen)
  - Locatie(s)
  - Het object waarop de handeling werd uitgevoerd
  - Het resultaat van de handeling
  - De datum en het tijdstip van de gebeurtenis
- In een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden, inbelnummers, et cetera). In de logregel mogen ook geen persoonsgegevens worden opgenomen uit systemen van VfPf zelf (dus wel gebruikersnamen of inlog accounts).
- Controle op opslag van logging: het vol lopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt ook gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld een logserver die niet bereikbaar is).
- Alle ongeautoriseerde toegangspogingen zijn beveiligingsincidenten en vereisen directe opvolging door melding aan Privacy & Security van VfPf.

Bescherming van informatie in logbestanden

Logbestanden dienen te worden beschermd tegen modificatie, inzien door onbevoegden en verwijdering. De volgende beleidsregels zijn hierop van toepassing:

- Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.
- Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
- Het raadplegen van logbestanden is voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
- Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
- De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden zal daarbij altijd het ‘vier ogen’ principe toegepast worden.
- De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoedelijk) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
- Het goed functioneren van de logging wordt continue gemonitord voor essentiële systemen.
- Controle op opslag van de logs: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld: een logserver die niet bereikbaar is).

Synchronisatie van systeemklokken

De klokken van alle relevante informatiesystemen van VfPf behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

- Systeemklokken worden zodanig gesynchroniseerd dat altijd een betrouwbare analyse van logbestanden mogelijk is. Binnen VfPf wordt hiervoor de Central European Time (CET) gehanteerd.

Beheersing van operationele software

Besturingssystemen dienen alleen te worden geactualiseerd wanneer daar een dwingende reden voor is, bijvoorbeeld indien de huidige versie van het besturingssysteem niet langer de bedrijfseisen ondersteunt. Het enkele feit dat een nieuwe versie van het besturingssysteem beschikbaar is, is geen reden voor installeren van een upgrade. Nieuwe versies van besturingssystemen kunnen minder veilig zijn, minder stabiel en minder begrijpelijk dan de huidige systemen.

Om het risico van corrumperen van productiesystemen tot een minimum te beperken gelden de volgende regels om wijzigingen te beheersen:

- het actualiseren van productieprogrammatuur, -toepassingen en -programmabibliotheken wordt uitsluitend uitgevoerd door ervaren beheerders na goedkeuring de change coördinator van VfPf;
- op productiesystemen is alleen goedgekeurde uitvoerbare programmatuur aanwezig, geen ontwikkelcode of compilers;
- toepassingen en besturingssysteemprogrammatuur worden geïmplementeerd na uitgebreide en succesvolle tests; er wordt o.a. getest op bruikbaarheid, beveiliging, effecten op andere systemen en gebruikersvriendelijkheid en de tests worden op gescheiden systemen uitgevoerd; er wordt gewaarborgd dat alle bijbehorende broncodebibliotheken zijn geactualiseerd;
- er wordt een configuratiebeheerssysteem gebruikt om alle geïnstalleerde programmatuur en de systeemdocumentatie te kunnen beheersen;
- er is een terugdraaistrategie vastgesteld voordat wijzigingen worden doorgevoerd;
- er wordt een auditlogbestand bijgehouden van elke update van besturingsprogrammabibliotheken;
- eerdere versies van de toepassingsprogrammatuur worden bewaard voor noodgevallen; oude versies van programmatuur worden gearchiveerd, samen met alle vereiste informatie en parameters, procedures, configuratiedetails en ondersteunende programmatuur zolang er gegevens in het archief worden bewaard.
- Programmatuur van leveranciers die in productiesystemen wordt gebruikt, worden op een niveau onderhouden dat door de leverancier wordt ondersteund. Na verloop van tijd zullen programmatuurleveranciers de ondersteuning van oudere versies van de programmatuur staken. VfPf onderkent de risico's van het vertrouwen op niet-ondersteunde programmatuur.
- Bij ieder besluit over upgraden naar een nieuwe programmatuurversie wordt rekening gehouden met de bedrijfseisen voor de wijziging en de veiligheid van deze versie, d.w.z. de invoering van nieuwe beveiligingsfunctionaliteit of het aantal en de ernst van de beveiligingsproblemen die met deze versie samenhangen. Eventueel worden herstelprogramma's (patches) in de programmatuur geïmplementeerd om zwakke plekken in de beveiliging te verhelpen of te verminderen.
- Leveranciers krijgen alleen fysieke of logische toegang wanneer dit noodzakelijk is voor ondersteunende diensten en met toestemming van de systeemeigenaar.
- Indien programmatuur steunt op externe programmatuur en modules worden deze gevallen gemonitord en gecontroleerd om onbevoegde wijzigingen te vermijden ter voorkoming van zwakke plekken in de beveiliging.

Beheer van technische kwetsbaarheden

Voor het beheer van technische kwetsbaarheden gelden de volgende regels:

- De verantwoordelijke medewerkers binnen het Regieteam IV (tactisch niveau) en de betrokken leveranciers (operationeel niveau) houden zich via de media en specifieke trainingen op de hoogte van actuele bedreigingen ten aanzien van informatiesystemen.
- Er is een proces ingericht voor het beheer van technische kwetsbaarheden; dit omvat minimaal de procedure voor het melden van incidenten, periodieke penetratietests, risicoanalyses van kwetsbaarheden en patching.
- Van softwarematige voorzieningen van de technische infrastructuur kan (bij voorkeur geautomatiseerd) gecontroleerd worden of de laatste updates (patches) in zijn doorgevoerd. Het doorvoeren van een update vindt niet geautomatiseerd plaats, tenzij hier speciale afspraken over zijn met de leverancier.
- Indien een patch beschikbaar is, dienen de risico's verbonden met de installatie van de patch te worden geëvalueerd (de risico's verbonden met de kwetsbaarheid dienen vergeleken te worden met de risico's van het installeren van de patch).
- Updates/patches voor kwetsbaarheden waarvan de kans op misbruik hoog is en waarvan de schade hoog is worden zo spoedig mogelijk doorgevoerd, echter minimaal binnen één week. Minder kritische beveiligings-updates/patches moeten worden ingepland bij de eerst volgende onderhoudsronde.
- Indien nog geen patch beschikbaar is dient gehandeld te worden volgens het advies van het Nationaal Cyber Security Centrum (NCSC).

9. Communicatiebeveiliging (A13)

Tot de netwerkdiensten worden gerekend het leveren van aansluitingen, private netwerkdiensten, netwerken met toegevoegde waarde en beheerde beveiligingsoplossingen zoals firewalls en ‘intrusion prevention’.

Beveiligingskenmerken van netwerkdiensten zijn:

- technologie toegepast voor de beveiliging van netwerkdiensten, zoals authenticatie, encryptie en netwerkverbindingscontroles (zie Toegangsbeheer: A9 en Versleuteling: A10);
- technische parameters vereist voor beveiligde verbinding met de netwerkdiensten in overeenstemming met de beveiligings- en netwerkaansluitingsregels;
- procedures voor het gebruik van netwerkdiensten om de toegang tot netwerkdiensten of toepassingen, waar nodig, te beperken.

Vereisten dienen in een overeenkomst met de leverancier te worden vastgelegd.

- Bepaal de kundigheid van de aanbieder van netwerkdiensten om overeengekomen diensten op een veilige manier te beheren en controleer deze regelmatig. Verlang het recht op audit.
- Stel de beveiligingsprocedures vast die voor bepaalde diensten nodig zijn, zoals beveiligingskenmerken, dienstverleningsniveaus en eisen voor beheer. Stel zeker dat de leveranciers van netwerkdiensten de verlangde maatregelen implementeren.
- Indien er klantgegevens worden verwerkt is het van belang zorgvuldig na te gaan welke gevolgen het wegvallen van netwerkdiensten kan hebben op de dienstverlening.

Scheiding in netwerken

- Netwerken moeten zo worden ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.
- Van systemen moet worden bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal één keer per jaar, geëvalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.
- Elke zone heeft een gedefinieerd beveiligingsniveau zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.
- Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.
- Zonering moet worden ingericht met voorzieningen waarvan de functionaliteit is beperkt tot het strikt noodzakelijke (hardening van voorzieningen).

- **Webfiltering**

Om het risico ten opzichte van inbreuk op het netwerk te verminderen, in combinatie met het voorkomen van virussen en malware door malifide websites is er binnen VfPf een beleid voor webfiltering geimplementeerd. Daarin zijn de volgende regels vastgesteld:

1. Toegang tot de Office omgeving is standaard alleen vanuit de EU mogelijk;
   (EU = EEA landen, EVA landen en Groot-Brittannië)
2. In het geval van toegang van een medewerker buiten de EU, dan dient hiervoor een wijzigingsverzoek te worden ingediend bij de IT Servicedesk.
3. Daarnaast worden de door Microsoft Defender gehanteerde richtlijnen toegepaste ten aanzien van het blokkeren van verkeer richting vaste categorieën websites. De minimaal te hanteren categorieën zijn:
    1. Cults
    2. Gambling
    3. Nudity
    4. Pornography / Secually Explicit Content
    5. Sex education
    6. Tasteless
    7. Violence
    8. Child Abuse Images
    9. Criminal Activity
    10. Hacking
    11. Hate & Intolerance
    12. Illegal Drug
    13. Illegal Software
    14. School Cheating
    15. Self-Harm
    16. Weapons
4. Logs ten aanzien van pogingen om deze website te bezoeken worden door Microsoft Defender bijgehouden, echter behoeven geen actieve monitoring.

10. Acquisitie, ontwikkeling en onderhoud van informatiesystemen (A14)

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.

Beveiligingseisen voor informatiesystemen

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.

Beveiliging bij ontwikkelings- en ondersteuningsprocessen

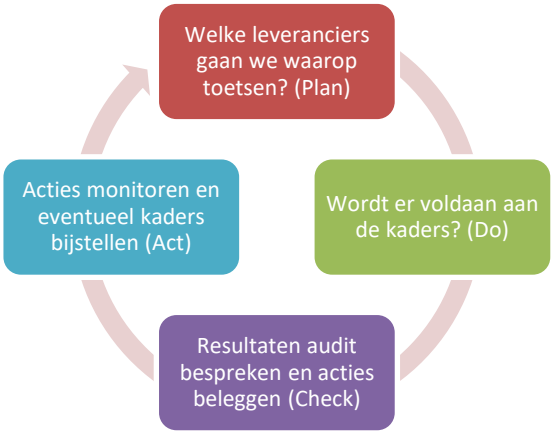
Voordat een wijziging van een bedieningsplatform wordt doorgevoerd:

- 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 noodzakelijk, worden geanonimiseerde gegevens gebruikt welke na de test zorgvuldig worden verwijderd.
- Bij een acceptatietest kan het in uitzonderlijke gevallen noodzakelijk zijn de originele klantgegevens te gebruiken. Aanvullende maatregelen zijn dan nodig.

11. Controleren van gestelde kaders en beleid (audits)

Dit document en de verschillende gerefereerde documenten vormen de kaders waar wij zelf en onze leveranciers aan moeten voldoen. Dit wordt gecontroleerd door het uitvoeren van interne en externe audits.

Periodiek zal VfPf een plan en planning opstellen waarin de diverse eisen rondom het beheer en onderhoud van applicaties, systemen doormiddel van een steekproef getoetst wordten. Dit plan zal gebruikt worden om voorafgaand aan een audit ronde te bepalen welke leverancier(s) we gaan auditen en waarop we de leverancier(s) gaan bevragen. Als we een leverancier hebben geselecteerd voor een audit zullen we het moment van de audit afstemmen om het bedrijfsproces zo min mogelijk te hinderen.



Audits op basis van steekproeven stelt VfPf in staat om systematisch de kwaliteit, naleving en effectiviteit van hun activiteiten te evalueren zonder overmatige middelen te besteden.

De periodieke audits worden in meer detail gepland in de jaarlijkse audit planning. Daarnaast worden de audit activiteiten gekoppeld aan de jaarlijkse leveranciersbeoordeling en aan applicatie evaluaties, zo vindt er geen dubbele uitvraag bij betrokkenen plaats.

Naast de periodieke audit rondes kan een significante wijziging leiden tot een audit om vast te stellen dat aan de gestelde eisen voldaan wordt.

Bij het vaststellen van de inhoud van een audit zal rekening gehouden worden met diverse maatregelen uit o.a. ISO27001, te denken valt aan:

- A.12.7.1 (afstemming auditeisen en -activiteiten om bedrijfsprocessen zo min mogelijk / niet te verstoren),
- A.14.2.3 (technische beoordeling van toepassingen),
- A.14.2.8 (testen van systeembeveiliging),
- A.14.2.9 (meenemen systeemacceptatietests),
- A.15.2 (beoordeling dienstverlening Leveranciers) en
- A.18.2.3 (beoordeling technische naleving).

Na de audit bespreken we de resultaten van de audit met de leverancier en koppelen we acties aan eventuele bevindingen. Vervolgens monitoren we de acties in het periodiek leveranciersoverleg. Tenslotte kan een bevinding ook reden geven om het beleid en de kaders van VfPf te evalueren en eventueel bij te stellen.

Bijlage 1 BEGRIPPENLIJST Privacy & Security (P&S)

Applicatie: een computerprogramma dat bedoeld is voor eindgebruikers. Letterlijk vertaald betekent het "toepassing"; vaak ook afgekort als “app”.

Bedrijfsmiddelen: informatiesystemen en andere informatie/apparatuur, inclusief papieren documenten, mobiele telefoons, draagbare computers, media voor gegevensopslag, enz.

Beschikbaarheid: kwaliteitseis aan data/informatie en systemen/applicaties die moet verzekeren dat de data/informatie en systemen/applicaties beschikbaar zijn voor bevoegde personen als dat nodig is.

Betrouwbaarheidseisen: eisen die VfPf stelt aan data/informatie en systemen/applicaties op het gebied van Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).

Calamiteit: zodanig ernstige incidenten dat de continuïteit van VfPf op het spel komt te staan doordat bepaalde diensten en/of producten niet meer beschikbaar zijn.

Classificaties: groepen van data en/of informatie en systemen/applicaties met gelijksoortige betrouwbaarheidseisen.

Classificeren: indelen in classificaties.

Data: (in een bestand) opgenomen uitdrukkingen van feiten. Zie ook gegevens.

Datalekken: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Gegevens: (in een bestand) opgenomen uitdrukkingen van feiten. Zie ook: data.

Incident: een gebeurtenis met ongewenste gevolgen, bv. een Security-incident.

Informatie: data of gegevens die zijn geïnterpreteerd en geïntegreerd, zodat die informatie kennis oplevert.

Informatiegroepen: groepen van verschillende soorten data/informatie die een bepaalde mate van vertrouwelijkheid gemeen hebben.

Informatiesystemen: alle servers en cliënts, netwerkinfrastructuur, systeem en ondersteuning bij programmeren, gegevens en andere computer subsystemen en onderdelen die eigendom zijn van of worden gebruikt door VfPf of die onder de verantwoordelijkheid van VfPf vallen. Het gebruik van informatiesystemen bevat alle interne en externe diensten, zoals internettoegang, e-mail, social media, enz.

Information Security Information Management System (ISMS): deel van het gehele managementproces dat zorg draagt voor de planning, implementatie, het onderhoud, de beoordeling, en het verbeteren van Privacy & Security.

Bijlage 2 Uitleg RASCI Matrix

Inleiding

Binnen VfPf wordt om verantwoordelijkheden en bevoegdheden te duiden veelal de RASCI matrix gehanteerd. RASCI is een hulpmiddel om verantwoordelijkheden en bevoegdheden in een organisatie op een zeer eenvoudige manier in kaart te brengen. RASCI is gebaseerd op een techniek, die 'responsibility charting' heet, en komt oorspronkelijk uit de Verenigde Staten. Met RASCI is het mogelijk exact aan te geven wat de rolverdeling is tussen personen, die samen een bijdrage in een proces moeten leveren.

RASCI uitleg

Dit zijn de rollen binnen de RASCI-matrix:

Responsible: verantwoordelijk voor de uitvoering van een proces of activiteit. Deze persoon legt verantwoording af aan de persoon die accountable is.

Accountable: de eindverantwoordelijke die ook goedkeuring moet geven aan het resultaat.

Support: de persoon die ondersteuning verleent aan het proces of project en de werkzaamheden uitvoert.

Consulted: de persoon die moet worden geraadpleegd, goedkeuring verleent of input levert aan de ‘responsible’ persoon, voorafgaand aan een stap in het proces.

Informed: degene die geïnformeerd wordt over de beslissingen, de voortgang en de bereikte resultaten, zodat er een volgende stap kan worden gezet.