Incident Response Plan (IRP)

Team P&S

8-3-2024 | Versienummer 1.2

Classificatie: Intern gebruik

Vervangingsfonds
Participatiefonds

Versiebeheer

Versie	Datum	Wijziging	Auteur(s)
1.1	28-3-2023	Finalisering	M. Wieërs, privacy en security officer
1.2 concept	6-3-2024	Afstemming met FG	M. Wieërs, privacy en security officer
1.2	8-3-2024	Finalisering	M. Wieërs, privacy en security officer

Goedkeuring c.q. herbevestiging

Gremium	Datum	Besluit
Directeur en MT	31-3-2024	Akkoord

Rollen en verantwoordelijkheden

Aan het Incident response plan zijn een aantal rollen en verantwoordelijkheden verbonden. In de onderstaande tabel zijn de rollen en verantwoordelijkheden vertaald in een RASCI-tabel.

	Procesverantwoordelijke ICT	Delivery Coördinator	Service management	Team P&S	Directie
Incident response plan	C	I	I	R	A

Inhoudsopgave

1. Relatie van dit plan met ISO27001

Dit plan is bedoeld als implementatie van de volgende ISO27001 beheersmaatregelen:

- 5.24 Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten (Verantwoordelijkheden en procedures)
- 5.25 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen
- 5.26 Reageren op informatiebeveiligingsincidenten
- 5.27 Lering uit informatiebeveiligingsincidenten
- 5.28 Verzamelen van bewijsmateriaal
- 6.8 Rapportage van informatiebeveiligingsgebeurtenissen
- 6.8 Rapportage van zwakke plekken in de informatiebeveiliging

Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer:

- 5.29 Informatiebeveiligingscontinuïteit tijdens een verstoring (plannen, implementeren, verifiëren, beoordelen en evalueren)
- 5.30 ICT-gereedheid voor bedrijfscontinuïteit
- 8.14 Redundantie van informatieverwerkende faciliteiten

2. Inleidende opmerkingen

2.1 Doelstelling

De doelstelling van het Vervangingsfonds/Participatiefonds (VfPf) bij dit plan is dat op alle bedreigende en verstorende gebeurtenissen voor VfPf, de gegevens van VfPf en de hierbij opgestelde processen zo snel mogelijk wordt geanticipeerd met de juiste acties en maatregelen. Al deze gebeurtenissen worden beoordeeld en geanalyseerd vanuit de standaard werkwijze in dit plan. Op deze manier is duidelijk waar en wanneer zich incidenten voordoen of voor hebben gedaan en of er sprake is van een datalek. Hoe helderder dit beeld, des te eerder en beter kunnen de juiste corrigerende of herstellende maatregelen worden getroffen en kan schade worden voorkomen.

In het kader van de plan-do-check-act-cyclus moet er ook lering worden getrokken uit alle gebeurtenissen om preventief betere maatregelen te implementeren om de frequentie, schade en kosten van toekomstige gebeurtenissen te voorkomen dan wel zoveel als mogelijk te beperken; dit leidt ook tot een verbetering van dit plan. Daarnaast draagt de cyclus bij aan borging van een zorgvuldige omgang met persoonsgegevens en wordt de verwijtbaarheid, aansprakelijkheid en gevolgschade voor betrokkenen voorkomen en/of geminimaliseerd.

2.2 Reikwijdte en beveiligingsprincipes

Dit document richt zich op het gehele proces van omgang met en beheersen van security gebeurtenissen en security incidenten (waaronder datalekken). Dit vanuit de context van data/informatie (waaronder persoonsgegevens) van VfPf of die namens VfPf wordt beheerd. In dit document leggen we het kader vast voor de melding, beoordeling en behandeling van security gebeurtenissen en security incidenten (waaronder datalekken) conform het beheer van informatiebeveiligingsincidenten uit de ISO27002.

Met dit plan wordt uitvoering gegeven aan het vastgestelde P&S-beleid en de hierin opgenomen fundamentele Beveiligingsprincipes om informatiebeveiliging effectief door te voeren binnen de organisatie, te weten:

- ***Beschikbaarheid****: data/informatie en systemen/applicaties moeten op de juiste momenten Beschikbaar zijn: hebben gebruikers op de juiste momenten toegang tot de data/informatie en systemen/applicaties die ze voor hun werk nodig hebben?*
- ***Integriteit****: de data/informatie en systemen/applicaties moeten Integer zijn: is waar we mee werken en hoe we dat doen juist, is het volledig?*
- ***Vertrouwelijkheid****: de data/informatie en systemen/applicaties moeten Vertrouwelijk zijn en blijven waar dat nodig is: hebben alléén personen toegang tot data/informatie.*

Er zijn situaties mogelijk waarbij de continuïteit van VfPf op het spel komt te staan omdat kritieke processen, diensten en/of producten niet meer beschikbaar zijn of de dreiging speelt dat ze niet meer beschikbaar zullen zijn. Dit noemen we een **calamiteit**. De gevolgen van calamiteiten voor de security maatregelen die VfPf genomen heeft vallen buiten de scope van dit document en worden behandeld in het ***'Bedrijfscontinuïteitsplan (BCP) VfPf V1.0'***. Zodra tijdens de beoordeling in het kader van het Incident response plan blijkt van zo'n calamiteit, dan treden de acties van het BCP in werking; de acties uit het Incident response plan lopen waar nodig parallel hieraan.

Uit het Handboek P&S volgt dat security gebeurtenissen/incidenten niet als afwijkingen worden beschouwd. Afwijkingen komen voort uit interne audits, externe audits, document reviews en zijn afwijkingen die ontdekt worden door Team P&S, voordat een gebeurtenis zich voordoet. Incidenten kunnen wel het gevolg zijn van afwijkingen.

2.3 Algemene verantwoordelijkheid

Dit plan is gericht op iedereen die voor het VfPf werkt. In paragraaf 4 en 5 worden de verantwoordelijkheden verder uitgewerkt. Kortweg geldt dat het irrelevant is of een medewerker nu in vaste dienst is of op tijdelijke basis voor VfPf werkt dan wel voor een leverancier van VfPf werkt. Alle medewerkers en leveranciers zijn op de hoogte van deze werkwijze rondom security gebeurtenissen en security incidenten en zijn verantwoordelijk voor het melden van deze gebeurtenissen en incidenten.

3. Security gebeurtenissen en security incidenten

Er kan binnen dit plan op verschillende manieren sprake zijn van bedreigende en verstorende gebeurtenissen gericht op systemen, gegevens en processen van VfPf en die de informatiebeveiliging van VfPf in gevaar brengen. In deze paragraaf wordt een onderverdeling aangebracht; al deze gebeurtenissen zijn in scope van dit plan en behoren te worden ontdekt, herkend, gemeld en behandeld.

Security gebeurtenissen en security incidenten kunnen zich op elk moment van de dag voordoen. Dit IRP richt zich dan ook op security gebeurtenissen en security incidenten die zich binnen en buiten kantoortijd voordoen.

3.1 Wat is een security gebeurtenis?

Het VfPf omschrijft een security gebeurtenis als een gebeurtenis die zich voordoet waarbij de Beschikbaarheid, Integriteit en/of Vertrouwelijkheid van systemen/applicaties en data/informatie van VfPf ***mogelijk*** in gevaar is of wordt gebracht. Het betreft de fase waarbij er twijfels zijn over een gebeurtenis en het nog niet duidelijk is of een dreiging zich daadwerkelijk heeft gerealiseerd of zal realiseren.

Bij een security gebeurtenis valt te denken aan de mogelijkheid van een zwakke plek/kwetsbaarheid in de informatiebeveiliging, een potentiële overtreding op het beleid voor informatiebeveiliging, een mogelijk falen van beveiligingsmaatregelen en/of een andere onbekende, onduidelijke of twijfelachtige situatie die relevant kan zijn voor de door VfPf getroffen Beveiligingsprincipes en beveiligingsmaatregelen.

Security gebeurtenissen kunnen zich ontwikkelen tot een security incident met als gevolg dat de belangen van VfPf in ernstige mate geraakt kunnen worden. Hierop moet tijdig en adequaat gereageerd worden. Alle gebeurtenissen worden daarom altijd beoordeeld en geanalyseerd. Dit onderzoek geeft uitsluitsel of de gebeurtenis effect heeft gehad op de genoemde Beschikbaarheid, Integriteit en/of Vertrouwelijkheid en of sprake is van een security incident.

3.2 Wat is een security incident?

Het VfPf omschrijft een security incident als een gebeurtenis die plaatsvindt, bijvoorbeeld door techniek of door (bewust of onbewust) menselijk handelen, en de Beveiligingsprincipes Beschikbaarheid, Integriteit en Vertrouwelijkheid van data/informatie[1] en/of de systemen/applicaties dan wel de processen van VfPf ***daadwerkelijk*** in gevaar brengt (poging), heeft gebracht, heeft misbruikt of heeft verstoord.

Het gaat hierbij om fysieke en digitale inbrekers, kwetsbaarheden/zwakke plekken in systemen/applicaties van VfPf (met direct gevolg) of virussen op het netwerk, maar ook om langdurige (stroom-)storingen, het verlies van documenten, het achterlaten van een vertrouwelijk document bij een printer of het ontbreken (of fout lopen) van een back-up met als gevolg het niet beschikbaar zijn van gegevens.

Ook de volgende situaties zijn security incidenten:

- *Alle hackpogingen (gelukt of mislukt) en DDoS aanvallen, of autorisaties die ten onrechte verleend maar niet gebruikt zijn*
- *Een phishing mail die is ontvangen;*
- *Een phishing mail waarbij op de bijlage is gedrukt of de link is geopend;*
- *Het langdurig (ongeaccepteerde overschrijding van in afspraken vastgelegde downtime) niet beschikbaar en/of toegankelijk zijn van gegevens en systemen/applicaties voor VfPf en voor schoolbesturen;*
- *Een malware-besmetting;*
- *Een handeling wordt verricht in strijd met interne en/of externe afspraken, richtlijnen en/of beleid zoals de Gedragscode uit het Personeelshandboek;*
- *Inbreuk op fysieke beveiligingsvoorzieningen;*
- *Toegangsovertredingen;*
- *Beschadigen of vernielen van (kritische) apparatuur;*
- *Onbevoegd inzien van vertrouwelijke informatie;*
- *Onbedoelde openbaarmaking van bedrijfsvertrouwelijke vertrouwelijke informatie;*
- *E-mail met onversleutelde bedrijfsvertrouwelijke informatie;*
- *Kenbaar maken (waaronder uitwisselen) van of onzorgvuldig omgaan met wachtwoorden;*
- *Etc.*

3.3 Wat is een datalek?

Van een datalek (in de zin van artikel 4 sub 12 van de Algemene verordening gegevensbescherming) is sprake als er bij een security incident ook persoonsgegevens[2] zijn betrokken. Een datalek is dus een speciale vorm van een security incident.

Bij een datalek speelt de situatie dat een inbreuk in verband met de persoonsgegevens per ongeluk of bewust op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van die persoonsgegevens. Een datalek is dus ook altijd een security incident. In sommige gevallen moet zo'n datalek worden gemeld bij de Autoriteit Persoonsgegevens en soms óók bij de betrokkenen om wiens gegevens het gaat.

[1] Met data/informatie worden de categorieën bedoeld zoals omschreven in het Classificatiebeleid, te weten de Informatiegroepen: openbaar, intern gebruik, bedrijfsvertrouwelijk en persoonsgegevens.

[2] Volgens artikel 4, sub 1, AVG wordt onder een persoonsgegeven verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Voorbeelden van datalekken zijn:

- *het verlies van niet of niet voldoende versleutelde persoonsgegevens;*
- *een cyberaanval waarbij persoonsgegevens zijn buitgemaakt, of zijn benaderd;*
- *een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt;*
- *een e-mail met persoonsgegevens is (onbeveiligd) verzonden naar een verkeerd mailadres;*
- *verzending van bulk e-mail waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden;*
- *een account wordt aangemaakt voor een verkeerde gebruiker waardoor onbevoegde inzage plaatsvindt van persoonsgegevens;*
- *Achtergelaten kopie met persoonsgegevens in de printer;*
- *Onbedoelde doorgifte van gegevens aan een betrouwbare derde;*
- *Fout bij bezorging per post;*
- *Een door VfPf gecontracteerde dienstverlener deelt informatie met persoonsgegevens met de verkeerde persoon;*
- *Etc.*

Een datalek kent drie varianten[3]:

- er is sprake van een datalek, maar hoeft **níet** te worden gemeld bij de Autoriteit Persoonsgegevens omdat het onwaarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van betrokkenen inhoudt;
- er is sprake van een datalek, dat **wél** gemeld moet worden bij de AP omdat het waarschijnlijk is dat de inbreuk **een risico** voor de rechten en vrijheden van betrokkenen inhoudt;
- er is sprake van een datalek, dat **wél** gemeld moet worden bij de AP **én** bij betrokkene(n) omdat het waarschijnlijk is dat de inbreuk **een hoog risico** voor de rechten en vrijheden van betrokkenen inhoudt.

4. Acties bij een security gebeurtenis en security incident

4.1 Actie Ontdekker: herkennen en melden

In de keten van VfPf hebben in ieder geval de volgende afdelingen en personen de verantwoordelijkheid security gebeurtenissen en security incidenten te herkennen, ontdekken en te melden bij Team P&S:

- **Alle interne en externe medewerkers VfPf:** dit zijn alle medewerkers binnen alle gelederen en afdelingen van VfPf die zich met de dagdagelijkse werkzaamheden en dienstverlening bezig houden.
- **Medewerkers van de helpdesk (WWplus)**: schoolbesturen nemen om verschillende redenen contact op met de helpdesk en de helpdeskmedewerker legt elke melding vast in het Klantregistratiesysteem; voor elke melding die technisch van aard is wordt een Topdesk-melding aangemaakt.

[3] Bij het bepalen of sprake is van een datalek en de inhoudelijke beoordeling daarvan, hanteert Team P&S de van toepassing zijnde richtsnoeren voor het melden van inbreuken (waaronder in ieder geval: *'Guidelines on Personal data breach notification under Regulation 2016/679'* én '*Guidelines 01/2021 on Examples regarding Data Breach Notification')*. Afstemming vindt plaats met de FG.

- **Leden van Team P&S**: eigen waarneming dan wel het contactpunt binnen kantooruren per e-mail en 24/7 beschikbaar via in ieder geval telefoon.
- **Medewerkers bij leveranciers:** dit zijn medewerkers bij opdrachtnemers en/of Verwerkers die de systemen/applicaties voor VfPf hosten en beheren. Met deze partijen zijn afspraken gemaakt over de melding van security gebeurtenissen en datalekken en vastgelegd in Verwerkersovereenkomsten. Leveranciers melden alle gebeurtenissen en zwakke plekken binnen 24 uur nadat de gebeurtenis of zwakke plek is ontdekt in ieder geval telefonisch bij Team P&S.
- Leveranciers die opdrachtnemer zijn van VfPf én zelfstandig Verwerkingsverantwoordelijke, melden security gebeurtenissen en security incidenten ook bij hun contactpersoon binnen VfPf zodat VfPf kan bepalen of sprake is van een gebeurtenis of incident welke onder de reikwijdte van dit plan valt en waarbij de acties uit dit plan in werking moeten treden.
- **Automatische response vanuit systemen/applicaties**: beheerders van systemen/applicaties die van een automatisch alarmsysteem zijn voorzien en die bij specifieke events berichten stuurt naar medewerkers van het IV Regieteam, servicemanagers en/of naar leveranciers.

Buiten de hierboven genoemde categorieën bestaat ook de mogelijkheid dat kwetsbaarheden en dreigingen door **NCSC** en **OCW** gemeld kunnen worden. Daarnaast kunnen meldingen binnenkomen via het door VfPf ingeschakelde **'Security.txt'**.

4.2 Meldingsproces

Het meldingsproces is een gezamenlijke verantwoordelijkheid waarbij de functionarissen uit de afdelingen zoals genoemd in de vorige paragraaf (1st line) en Team P&S (2nd line) samen het proces rondom ontdekken, melden en afhandelen oppakken.

Team P&S is het vaste contactpunt om security gebeurtenissen en security incidenten bij te melden, heeft de lead in het (beoordelings)proces-/onderzoek en is elke dag van de week 24/7 beschikbaar om deze gebeurtenissen en incidenten in behandeling te nemen.

Medewerkers melden alle security gebeurtenissen en security incidenten meteen, maar ***niet later dan één uur*** nadat de gebeurtenis is ontdekt, telefonisch bij Team P&S. Deze melder brengt ook zijn of haar leidinggevende (Afdelingsmanager of Proceseigenaar) op de hoogte; indien systemen/applicaties van VfPf of die namens VfPf beheerd worden betrokken zijn dan brengt de melder ook de Procesverantwoordelijke ICT van IV-Regieteam op de hoogte van de gebeurtenis of het incident.

Leveranciers melden alle security gebeurtenissen en security incidenten die zij ontdekken ***binnen 24 uur nadat de gebeurtenis is ontdekt*** bij de Afdelingsmanager van de van toepassing zijnde afdeling waarbinnen de gebeurtenis of het incident zich voordoet, de Proceseigenaar ICT én bij Team P&S.

4.3 Wat te verzamelen?

Als sprake is van een security gebeurtenis of security incident dan wordt zoveel mogelijk informatie verzameld. De Afdelingsmanager (dan wel de Proceseigenaar) van de van toepassing zijnde afdeling waarbinnen de gebeurtenis of het incident zich voordoet, wijst een functionaris aan die voor deze verzameling zorgdraagt; afstemming vindt plaats door de aangewezen functionaris met Team P&S. Als Team P&S vaststelt dat onvoldoende bewijsmateriaal voorhanden is dan worden aanvullende vragen uitgezet bij deze functionaris, andere functionarissen binnen VfPf of bij Leveranciers om ontbrekend bewijs zo snel mogelijk te verzamelen.

De volgende informatie wordt – voor zover mogelijk direct - verzameld:

- *de naam van de persoon en contactgegevens van de persoon die de melding doet;*
- *de datum en tijd waarop de melder de gebeurtenis heeft ontdekt en gemeld heeft aan Team P&S;*
- *korte beschrijving hoe de gebeurtenis ontdekt is;*
- *wat is de oorzaak van de gebeurtenis?*
- *wat is de aard van de inbreuk? (inbreuk op toegang tot, juistheid van en/of beschikbaarheid van data/informatie)*
- *wat voor soort data/informatie is betrokken bij de gebeurtenis? Interne, bedrijfsvertrouwelijke of vertrouwelijke informatie? En wat voort soort informatie daarbinnen (met name bijzondere gegevens, of gegevens van gevoelige aard, waaronder toegangs- of identificatiegegevens, financiële gegevens et cetera);*
- *wie zijn de betrokkenen?*
- *de datum en tijdstip (volledige duur van begin tot eind) van de gebeurtenis;*
- *welke systemen/applicaties zijn bij de gebeurtenis betrokken en in welke vorm zijn data/informatie opgeslagen (op papier, digitaal, op een verwijderbare gegevensdrager?*
- *welke leverancier(s) en andere ketenpartner(s) is/zijn bij de gebeurtenis betrokken?*
- *duurt de gebeurtenis nog voort of is deze gestopt en zo ja, hoe?*
- *om hoeveel records van data/informatie en om hoeveel betrokkenen ?*
- *indien mogelijk, een beschrijving welke technische beveiligingsmaatregelen aanwezig zijn (zoals versleuteling, afgeschermde omgevingen etc.);*
- *wat is naar de opvatting van de melder de ernst van de gevolgen voor betrokkenen?*

5. Behandeling van de gebeurtenis

De bij de security gebeurtenis of het security incident betrokken functionarissen behandelen in teamverband de melding en zoeken gezamenlijk naar de juiste oplossing om de inbreuk te stoppen, te beperken, de schade in te dammen, deze (zoveel als mogelijk) te herstellen en een oplossing te bedenken om te voorkomen dat het probleem zich herhaalt.

In het *'Logboek P&S I (…)'* komen diverse onderwerpen terug om te borgen dat adequaat en zonder verlies van tijd wordt gereageerd op security gebeurtenissen en security incidenten, zoals: *'Oorzaak- en omvanganalyse', 'Dreiging/kwetsbaarheid, risico en status', 'Correctieve maatregelen', 'Herstelacties'* en *'Corrigerende maatregelen'*.

5.1 Rollen en verantwoordelijkheden ná melding

In deze fase betreft het de behandeling van de security gebeurtenis of het security incident waarvoor een Incident response team niet opgericht hoeft te worden. In de basis zijn de volgende functionarissen als team betrokken.

Het IV-Regieteam biedt ondersteuning bij het onderzoeken van security gebeurtenissen en security incidenten. De Proceseigenaar ICT is verantwoordelijk voor het oplossen dan wel het laten oplossen van het aan het incident onderliggende ICT-probleem (of de aansturing hierop) en waar van toepassing het implementeren van correctieve, corrigerende en/of herstelacties. Indien nodig bepaalt de Procesverantwoordelijke ICT of andere leden uit het IV-Regieteam of externe expertise moet worden ingeschakeld.

In samenspraak met de Proceseigenaar ICT (als de gebeurtenis ziet op systemen/applicaties van VfPf of namens VfPf worden beheerd) en/of met de betrokken verantwoordelijke personen uit de afdeling waarbinnen het gemelde voorval zich voordoet, bepaalt Team P&S zo snel mogelijk – rekening houdend met de meldingstermijn van 72 uur - of sprake is van een security gebeurtenis of security incident uit paragraaf 3.

Team P&S heeft daarnaast een adviserende rol, monitort en bewaakt verder de voortgang van niet-opgeloste incidenten en coördineert het proces.

Daar waar sprake is van (de dreiging van) een inbreuk in verband met de persoonsgegevens, is de Functionaris voor gegevensbescherming (FG) adviserend bij de afhandeling van security gebeurtenissen en security incidenten. Team P&S stemt afhankelijk van de context acties af met de FG.

De Afdelingsmanager is eindverantwoordelijk voor het (laten) oplossen van een security gebeurtenis of een security incident. Deze is verantwoordelijk voor het besluiten om en (laten) realiseren van gepaste beveiliging van de onder zijn/haar verantwoordelijkheid uitgevoerde processen en de daarbij gebruikte processen, systemen/applicaties en data/informatie en zet alle medewerking in die hem of haar ter beschikking staat bij de analyse van het incident en de implementatie van de verbeter – en herstelmaatregelen.

5.2 Incident response team (IRT)

Het oprichten van een IRT is afhankelijk van de aard, omvang, ernst en impact van de gebeurtenis op de inbreuk op de Beschikbaarheid, Integriteit en Vertrouwelijkheid. De samenstelling van het IRT kan daarom wisselen. Het gaat hierbij om een security gebeurtenis of security incident met een hoge impact op de bedrijfsvoering van VfPf of het dagelijks leven van betrokkenen, waarbij directe mobilisering van het IRT vereist is. Als uit het security incident direct schade voortvloeit voor betrokkene(n) en/of VfPf dan worden door het IRT onmiddellijk passende maatregelen getroffen om de schade te beperken, te beëindigen en te herstellen.

Team P&S besluit, in samenspraak met de betrokken personen uit de van toepassing zijnde in- en externe afdelingen (zie paragraaf 5.1) , of een IRT moet worden opgericht. Team P&S coördineert en faciliteert de samenwerking van het IRT. Team P&S heeft daarnaast ook hier een adviserende rol. Team P&S monitort en bewaakt verder de voortgang van niet-opgeloste incidenten en coördineert het proces.

Indien sprake is van een inbreuk in verband met persoonsgegevens, dan vindt afstemming met de FG plaats en wordt gezamenlijk bepaald in welke mate de FG een rol heeft in het IRT. In het IRT neemt altijd de Afdelingsmanager zitting dan wel de door de Afdelingsmanager aangewezen Proceseigenaar of andere personen; wanneer de gebeurtenis ziet op systemen/applicaties van VfPf of die namens VfPf beheerd worden, dan is altijd een lid van het IV-Regieteam aanwezig en deze wordt door de Procesverantwoordelijke ICT beschikbaar gesteld.

Het IRT onderzoekt altijd de oorzaak van de gebeurtenis. Team P&S beoordeelt, in samenspraak met de leden van het IRT, van welke gradatie als bedoeld in paragraaf 3 sprake is. Indien nodig, bepaalt het IRT welke technische en organisatorische acties nodig zijn om de inbreuk en de daaraan ten grondslag liggende kwetsbaarheid en zwakke plek te verhelpen, de inbreuk te stoppen, eventuele verdere inbreuk en schade te voorkomen en welke herstelacties nodig zijn. Binnen het IRT neemt de Afdelingsmanager (dan wel de door de Afdelingsmanager aangewezen Proceseigenaar of andere personen) een besluit over de te nemen acties.

De Directie (en het MT) wordt van de oprichting van een IRT zo snel mogelijk, maar in ieder geval op de dag van oprichting, op de hoogte gesteld.

5.3. Calamiteit (dan wel verstoring cnf. A5.29)

Wanneer de behandelende teams - als bedoeld in paragraaf 5.1 en 5.2 - tot de conclusie komen dat de continuïteit van VfPf op het spel staat omdat kritieke processen, diensten en/of producten niet meer beschikbaar zijn of bedreigd worden niet meer beschikbaar te zijn, dan treden de acties van het *'Bedrijfscontinuïteitsplan (BCP) VfPf V1.0'* in werking. Het IRT meldt onverwijld het incident conform de in het BCP beschreven meldingswijze; de acties uit het Incident response plan lopen waar nodig parallel hieraan.

5.4 Onderzoek

Er wordt altijd een oorzaak- en omvanganalyse (Root cause analyse) uitgevoerd om de bron en oorzaak van de security gebeurtenis of het security incident te achterhalen en te (laten) verhelpen. Het (laten) uitvoeren van de oorzaakanalyse valt onder de verantwoordelijkheid van de Afdelingsmanager, tenzij deze een andere persoon daartoe aanwijst.

5.5 Verslaglegging en vastleggen bewijs

Bij de vastlegging van gebeurtenissen wordt altijd het template 'Logboek security gebeurtenissen' gehanteerd.[4] Team P&S initieert dit document en documenteert mede tijdens het gehele proces alle relevante feiten, activiteiten en bewijsstukken, waaronder in ieder geval de toedracht, de beoordeling, besluit(en) en getroffen acties, inclusief de relevante e-mails; betrokken teamleden vullen het logboek aan.

Team P&S maakt hiervoor een opslaglocatie aan op de *"Werkmap Privacy en Security - Documenten\17. Datalekken en incidenten"*. Dit document wordt gedeeld met de bij de security gebeurtenis/incident betroken personen.

5.6 Nadere communicatie en escalatie

De Directie wordt altijd geïnformeerd over security gebeurtenissen en security incidenten en de voortgang ervan, op de wijze zoals beschreven in dit document. Indien nodig, wordt afdeling Communicatie ook van de oprichting van het IRT op de hoogte gesteld en waar nodig ook betrokken; overige betrokkenen worden op basis van 'need-to-know' geïnformeerd.

Als Team P&S dan wel het IRT concludeert dat andere in- en externe personen, afdelingen of organisaties op de hoogte gesteld moeten worden van het bestaan van het security incident (of relevante details daarvan) dan communiceert Team P&S dat richting die personen, afdelingen en/of organisaties. Als Team P&S dan wel het IRT constateert dat bepaalde activiteiten en/of handelingen van Team P&S of het IRT op enigerlei wijze belemmerd of verstoord worden, dan escaleert Team P&S naar de Directie.

5.7 Melding Autoriteit Persoonsgegevens

Als Team P&S vaststelt, in samenspraak met de IRT-leden en na consultatie van de FG, dat sprake is van een meldingsplichtig datalek dan informeert en adviseert Team P&S de Directie. Na afstemming neemt de Directie het besluit om wel of niet over te gaan tot melding bij de Autoriteit Persoonsgegevens.

[4] Uitzondering hierop zijn phishingberichten als deze slechts gemeld worden; als op de phishing is geantwoord (door het drukken op een verdachte link, het openen van een onbetrouwbare bijlage etc.) dan wordt dit incident verder uitgewerkt in het logboek.

Na akkoord van de Directie wordt door Team P&S binnen de meldingstermijn van 72 uur (kalenderuren) een melding gedaan bij de Autoriteit Persoonsgegevens via het daarvoor bestemde loket. Elke beslissing van de Directie wordt gedocumenteerd.

Bij het bepalen of een melding gedaan moet worden bij de Autoriteit Persoonsgegevens sluit VfPf onder meer aan bij de criteria die hiervoor door deze Autoriteit gehanteerd worden.

5.8 Voorlopige Melding Autoriteit Persoonsgegevens

De mogelijkheid kan zich voordoen dat Team P&S dan wel het IRT niet binnen 72 uur kan vaststellen dat sprake is van een meldingsplichtig datalek als bedoeld in paragraaf 3.3. Om de termijn te bewaken wordt overwogen om het security incident in dat geval voorlopig aan te merken als een meldingsplichtig datalek.

Met de FG volgt eerst consultatie en Team P&S informeert en adviseert de Directie. Na akkoord van de Directie wordt door Team P&S een voorlopige melding gedaan bij de Autoriteit Persoonsgegevens via het daarvoor bestemde digitale loket. Alle acties worden voortgezet en indien voldoende duidelijkheid aan Team P&S wordt verschaft om het datalek te beoordelen, dan wordt de Directie door Team P&S geadviseerd om de melding in te trekken of definitief te maken. Elke beslissing van de Directie wordt gedocumenteerd.

5.9 Melding bij betrokkenen

Als Team P&S vaststelt, in samenspraak met de IRT-kleden en na consultatie van de FG, dat sprake is van een meldingsplichtig datalek dat óók bij betrokkenen moet worden gemeld, dan informeert en adviseert Team P&S de Directie. Als de Directeur akkoord is dan wordt in samenspraak met FG en afdeling Communicatie de wijze bepaald waarop de betrokkenen geïnformeerd worden. Elke beslissing van de Directie wordt gedocumenteerd.

Betrokkene wordt altijd zo snel mogelijk geïnformeerd over wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. Ook wordt betrokkene geïnformeerd over de acties die de organisatie verricht en die de betrokkene zelf kan nemen om schade te voorkomen. Onder bepaalde voorwaarden hoeft een melding aan betrokkene(n) niet plaats te vinden.[5]

6. Rapportage

Periodiek wordt de Directie door middel van de P&S-kwartaalrapportage geïnformeerd over security gebeurtenissen en security incidenten in de achterliggende periode. De rapportage wordt vervolgens in de eerstvolgende MT-vergadering ter kennisgeving aan het MT aangeboden.

7. Monitoring

In het logboek wordt vastgelegd wie of welke afdeling verantwoordelijk is voor het realiseren van acties en welke acties geïmplementeerd worden.

[5] In artikel 34, lid 3 van de AVG zijn drie voorwaarden opgenomen waaronder geen mededeling vereist is.

Team P&S registreert de acties in het Incidentenregister en monitort de voortgang vanuit de Operationele Planning in de Jaarkalender en volgt de voortgang. Indien nodig en afhankelijk van de voortgang stelt Team P&S interventies voor en/of adviseert bijsturende acties om de doelstelling te bereiken van het implementeren van de beheersmaatregelen om het probleem op te lossen.

8. Evalueren en leren

De organisatie wil leren van incidenten en daarom moeten incidenten geëvalueerd worden.

Periodiek (maximaal een half jaar na de gebeurtenis) vindt een evaluatie van elk security incident plaats conform de planning in de Operationele Planning van de Jaarkalender. Van de kennis die is verkregen door de security gebeurtenis of het security incident te analyseren en op te lossen wordt lering getrokken (worden trends ontdekt) door deze te gebruiken om de waarschijnlijkheid of impact van toekomstige incidenten te identificeren, te verkleinen en om zwakke plekken en kwetsbaarheden in bestaande (primaire) processen en architectuur te voorkomen, op te lossen en te verbeteren.

Als uit de evaluatie blijkt dat uitgebreidere of aanvullende acties nodig zijn om de frequentie, schade en kosten van toekomstige gebeurtenissen te beperken, dan worden deze ingezet na goedkeuring van de Afdelingsmanager of de door hem/haar aangewezen Proceseigenaar (dan wel een andere aangewezen persoon).

De praktijksituaties van security gebeurtenissen en security incidenten kunnen dienen als input in een gebruikersbewustzijnstraining als voorbeelden van wat kan gebeuren, hoe te reageren op dergelijke incidenten en hoe deze in de toekomst voorkomen kunnen worden.

Als uit de evaluatie blijkt dat dit Incident respons plan direct gewijzigd moet worden, dan wordt dit document zo snel mogelijk herijkt.

Tot slot is het belangrijk om de melder een terugkoppeling te geven over de uitkomsten van de gebeurtenis of het incident. Zo wordt het signaal afgegeven dat melden loont.