Incident Response Plan (IRP)

Team P&S

25 januari 2022 | Versienummer 1.0

Classificatie: Classificatiegroep 1 (Intern gebruik)

Vervangingsfonds
Participatiefonds

Versiebeheer

Versie	Datum	Wijziging	Auteur(s)
0.1	8-1-2021	Integratie documenten en informatie	J. van Drunen, Avensus & M. Wieërs privacy en security officer
0.2	12-1-2021	Initiële aanpassing en wijziging	M. Wieërs, privacy en security officer
0.21	15-1-2021	Wijziging	M. Wieërs, privacy en security officer
0.22	3-2-2021	Afstemming	Team P&S + Jolanda van Drunen en Mark Engels
0.23-0.50	feb 2021	Wijziging	M. Wieërs, privacy en security officer
0.6	27-5-2021	Enkele wijzigingen in indeling	Ieke Coppens, privacy en security officer
0.60	31-5-2021	Gezamenlijke review	M. Wieërs en Ieke Coppens, privacy en security officers
0.61	7-6-2021	Gezamenlijke review	M. Wieërs en Ieke Coppens, privacy en security officers
0.61	8-6-2021 en 14-6-2021	Wijziging en gezamenlijke review	M. Wieërs en Ieke Coppens, privacy en security officers
0.7	16-6-2021	Review	J. van Drunen, Avensus
0.71	22-6-2021	Wijziging	M. Wieërs, privacy en security officer
0.8	24-6-2021	Gezamenlijke review	M. Wieërs, H. Coppens en J. van Drunen
0.9	13-7-2021	Wijziging	M. Wieërs, privacy en security officer
0.91	23-11-2021	Werksessie IRP	IV-Regieteam & Team P&S
0.99	1-12-2021	Wijzigingen na bespreking	IV-Regieteam & Team P&S
0.991	8-12-2021	Wijziging na bespreking SPAR	Team P&S en J. van Drunen
1.0	25-1-2022	Finalisering na akkoord directeur	M. Wieërs, privacy en security officer

Goedkeuring/vaststelling

Gremium	Datum	Besluit
Directeur	25-1-2022	Akkoord

Inhoudsopgave

1. Relatie van dit plan met ISO27001

Deze procedure is bedoeld als implementatie van de volgende ISO27001 beheersmaatregelen:

- **A.12.4.1 Gebeurtenissen registreren**
  Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligings-gebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.
- **A.16.1.1 Verantwoordelijkheden en procedures**
  Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatie-beveiligingsincidenten[1] te bewerkstelligen.
- **A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen**
  Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd.
- **16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging**
  Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.
- **A.16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen**
  Informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.
- **A.16.1.5 Respons op informatiebeveiligingsincidenten**
  Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.
- **A.16.1.6 Lering uit informatiebeveiligingsincidenten**
  Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
- **A.16.1.7 Verzamelen van bewijsmateriaal**
  De organisatie moet procedures definiëren en toepassen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.

[1] Binnen het VfPf wordt voor informatiebeveiligingsincidenten het woord ‘Security incident’ gehanteerd.

2. Inleidende opmerkingen

2.1 Doelstelling

De doelstelling van het VfPf bij dit plan is dat alle gebeurtenissen en kwetsbaarheden, die verband houden met systemen/applicaties en de data/informatie die zich daarin bevinden, in een zo vroeg mogelijk stadium gesignaleerd, gemeld, behandeld en geregistreerd worden. Alle gebeurtenissen worden altijd beoordeeld en geanalyseerd. 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 beter kunnen tijdig corrigerende maatregelen worden genomen.

In het kader van de plan-do-check-act-cyclus moet er 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 en om dit plan te optimaliseren. 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/scope

Dit document richt zich op het gehele proces van het beheer van securityincidenten waaronder datalekken. Dit plan heeft dus géén betrekking op preventieve beheersmaatregelen die securityincidenten en datalekken moeten voorkomen. In dit document leggen we het kader vast voor de melding, behandeling en beoordeling van securityincidenten en datalekken. Met deze procedure wordt uitvoering gegeven aan het vastgestelde P&S-beleid. Bij de beoordeling van een incident zal vastgesteld moeten worden of het incident een informatiebeveiligingsincident (hoofdstuk 3) betreft of een datalek (hoofdstuk 4).

Een security incident vindt plaats wanneer de Beschikbaarheid, Integriteit en/of Vertrouwelijkheid van data/informatie wordt verstoord. Het gaat hierbij dus niet alleen om inbrekers of virussen op het netwerk, maar ook om (stroom-) storingen, het verlies van documenten, het achterlaten van een document bij een printer of het ontbreken (of fout lopen) van een back-up met als gevolg het niet beschikbaar zijn van data, applicaties, websites, printers, et cetera. Als bij dit soort gebeurtenissen persoonsgegevens betrokken zijn is sprake van een datalek. In sommige gevallen moet zo'n datalek worden gemeld bij de Autoriteit Persoonsgegevens (AP), de "privacy-waakhond", en soms óók bij de betrokkenen om wiens gegevens het gaat. Er zijn situaties denkbaar waarbij het incident zo ernstig is dat de continuïteit van VfPf op het spel komt te staan omdat (dreigt dat) kritieke processen, diensten en/of producten niet meer beschikbaar zijn: dit noemen we een calamiteit.2 De gevolgen van calamiteiten voor de security maatregelen die VfPf heeft genomen heeft vallen buiten de scope van dit document en worden behandeld in het Plan Security maatregelenplan bij calamiteiten.

2.3 Verantwoordelijkheden

Dit plan is gericht op iedereen die voor het VfPf werkt. Of een medewerker nu in vaste dienst is of op tijdelijke basis voor VfPf werkt dan wel voor een leverancier van VfPf werkt. Medewerkers melden alle gebeurtenissen en zwakke plekken zo snel mogelijk telefonisch bij Team P&S. 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.

[2] In het Plan Securitymaatregelen bij calamiteiten VfPf word een drietal calamiteiten onderscheiden: 1. Wegvallen van medewerkers in sleutelposities; 2. Uitval van systemen voor elektronische toegang voor beveiligde ruimten; 3. Uitval van kritische systemen.

Alle medewerkers en medewerkers van leveranciers zijn op de hoogte van deze werkwijze rondom security gebeurtenissen en zwakke plekken.

3.1 Wat is een security incident?

Het VfPf omschrijft een security incident als: een gebeurtenis die plaatsvindt door techniek of door menselijk handelen waarbij de Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van data/informatie en/of de systemen/applicaties van VfPf wordt verstoord.

- *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.*

Voorbeelden van security incidenten zijn:

- *Het niet beschikbaar zijn van data/informatie en systemen/applicaties voor VfPf en voor schoolbesturen*
- *Verlies of diefstal van waardepapier, dossier, usb-stick, tablet of andere gegevensdragers*
- *Een hack van een informatiesysteem, waarbij een derde partij stiekem toegang heeft tot informatie om deze te wijzigen*
- *Een medewerker vindt een vertrouwelijk document bij de printer.*
- *Niet naleven van beleid of richtlijnen*
- *Inbreuk op fysieke beveiligingsvoorzieningen*
- *Toegangsovertredingen*
- *Beschadigen of vernielen van (kritische) apparatuur*
- *Virusbesmetting als gevolg van het aanklikken van een onbetrouwbare bijlage*
- *Onbevoegd inzien van vertrouwelijke informatie*
- *Onbedoelde openbaarmaking van vertrouwelijke informatie*
- *Geen gescreend personeel*
- *Storingen in software- of hardware*
- *Illegaal kopiëren van gegevens*
- *E-mail met onversleutelde vertrouwelijke informatie*
- *Kenbaar maken van of onzorgvuldig omgaan met wachtwoorden*
- *Zwakke plekken in systemen en applicaties*

3.2 Wat is een datalek?

Als er bij een security incident ook persoonsgegevens zijn betrokken hebben we het over een datalek. Persoonsgegevens zijn gegevens die ofwel direct over iemand gaan, ofwel (zonder al te veel moeite) naar deze persoon te herleiden zijn. Bij een datalek is sprake van een inbreuk op de persoonsgegevens per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van die persoonsgegevens.

Voorbeelden van datalekken zijn:

- *het verlies van een USB-stick met niet-versleutelde persoonsgegevens;*
- *een cyberaanval waarbij persoonsgegevens zijn buitgemaakt;*
- *een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn gemaakt;*
- *een e-mail met persoonsgegevens 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.*

3.3 Gradaties van security incidenten

Bij een security incident wordt Beschikbaarheid, Integriteit en/of de Vertrouwelijkheid van data/informatie en of onze systemen/applicaties van het VfPf bedreigd. Als er bij een security incident persoonsgegevens betrokken zijn, spreken we over een datalek. Een datalek is dus ook altijd een security incident. Sommige datalekken moet VfPf op grond van de Algemene verordening gegevensbescherming (AVG) melden bij de Autoriteit Persoonsgegevens (AP). En sommige datalekken moeten óók worden gemeld bij de betrokkenen van wie er persoonsgegevens bedreigd zijn of worden.

Een security gebeurtenis kan de volgende gradaties kennen. Afhankelijk van de gradatie varieert ook de communicatie en het escalatieniveau. We onderscheiden bij security gebeurtenissen de volgende gradaties.

1. **Eerste graad**: een security gebeurtenis die geen datalek is. Er is een kwetsbaarheid ontdekt die niet is misbruikt en waarbij geen persoonsgegevens betrokken zijn. Van een security gebeurtenis van de eerste graad spreken we ook als de kwetsbaarheid wel is misbruikt maar vastgesteld wordt dat er geen persoonsgegevens bij betrokken zijn.

2. **Tweede graad:** een security gebeurtenis die tegelijk een datalek is maar niet hoeft te worden gemeld bij de Autoriteit Persoonsgegevens (de AP) omdat Team P&S heeft vastgesteld dat het onwaarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van betrokkenen inhoudt.

3. **Derde graad:** een security gebeurtenis die tegelijk een datalek is én gemeld moet worden bij de AP vanwege de vaststelling door Team P&S dat de inbreuk waarschijnlijk een risico inhoudt voor de rechten en vrijheden van betrokkenen.

4. **Vierde graad:** een security gebeurtenis, tegelijk AP-meldingsplichtig én meldingsplichtig bij de betrokkene(n) vanwege de vaststelling door Team P&S dat de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van betrokkenen.

4 Beschrijving acties bij een security gebeurtenis

4.1 Actie Ontdekken, herkennen en melden bij Team P&S

In de keten van VfPf hebben in ieder geval de volgende afdelingen en personen de verantwoordelijkheid security gebeurtenissen 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.
- **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.

- **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.
- **NCSC en OCW**: security-dreigingen die relevant zijn voor VfPf kunnen worden gemeld bij VfPf (Team P&S), zodat deze kunnen worden gemonitord.

Team P&S is het vaste contactpunt om security gebeurtenissen bij te melden. Team P&S heeft de lead in het proces en is 24/7 beschikbaar om security gebeurtenissen in behandeling te nemen.

De ontdekker meldt een security gebeurtenis meteen, maar niet later dan een uur nadat de gebeurtenis is ontdekt, in ieder geval **telefonisch** bij Team P&S. De ontdekker verzamelt van een security gebeurtenis zoveel mogelijk informatie. Daarbij worden de volgende gegevens aangeleverd voor zo ver deze bekend zijn:

- *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?*

De ontdekker van een security gebeurtenis staat Team P&S in de informatievoorziening bij als Team P&S tot de conclusie komt dat sprake is van een security incident.

4.2 Actie Beoordelen en herstelacties

Team P&S laat zo snel mogelijk na melding van de gebeurtenis bewijs verzamelen en bepaalt aan de hand van de aangeleverde informatie van de ontdekker of er voldoende informatie beschikbaar is om vast te stellen of de security gebeurtenis als een security incident gekwalificeerd moet worden. Als vastgesteld wordt dat onvoldoende bewijsmateriaal voorradig is, dan worden aanvullende vragen uitgezet bij de ontdekker of andere personen. Team P&S laat een oorzaakanalyse uitvoeren om de bron en oorzaak van het security incident te achterhalen en te (laten) verhelpen. In de regel wordt de oorzaakanalyse uitgevoerd door de proces- of systeemeigenaar, tenzij de proces- of systeemeigenaar een andere persoon daartoe aanwijst.

Op basis van de aard, omvang en context van de security gebeurtenis besluit Team P&S, in samenspraak met het IV Regieteam en/of de proces- of systeemeigenaar, of een Incident Response Team (IRT) moet worden opgericht/bijeengeroepen en wie in het IRT plaatsnemen. Uitgangspunt is dat beide leden van Team P&S in dit IRT vertegenwoordigd zijn: één lid borgt de bewaking van het proces en de ander verzorgt de inhoudelijke expertise.

Team P&S coördineert en faciliteert de samenwerking van het IRT (waaronder het aanmaken van een what'sapp-groep aan (of een ander medium) en een voor alle leden toegankelijke werkmap). Standaard brengt Team P&S zo snel mogelijk na ontvangst en eerste beoordeling van de melding het incident response team (IRT) bij elkaar, tenzij Team P&S van mening is dat Team P&S het security incident zelfstandig kan afhandelen.

Zodra voldoende informatie voorhanden is, onderzoekt het IRT of sprake is van een security incident als bedoeld in hoofdstuk 3, en zo ja, van welke gradatie sprake is. Het oordeel van Team P&S is daarbij uiteindelijk doorslaggevend.

Voor zover de oorzaak van het security incident bekend is, bepaalt het IRT welke technische en organisatorische maatregelen nodig zijn om de inbreuk en de daaraan ten grondslag liggende kwetsbaarheid en zwakke plek te verhelpen, de inbreuk te stoppen en eventuele verdere inbreuk te voorkomen. Team P&S adviseert deze beheersmaatregelen aan de proces-/systeemeigenaar. Die neemt over de te nemen beheersmaatregelen een definitief besluit.

Als het security incident ook een datalek is waaruit direct schade voortvloeit voor betrokkene, neemt Team P&S (dan wel het IRT) onmiddellijk passende maatregelen om de schade te beperken, te beëindigen en te herstellen. De proces- of systeemeigenaar en de directie worden hierbij zoveel als het incident toelaat betrokken en worden in ieder geval op de hoogte gesteld van de maatregelen.

Bij het bepalen van de gradaties 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')*.

Ten aanzien van de betrokkene wordt bij schade in ieder geval met het volgende rekening gehouden:

- Wat kan worden gedaan om betrokkene te ondersteunen in het beperken van de schade door een datalek? Bijv. door het verstrekken van instructies over wachtwoorden aanpassen, blokkeren van credit cards etc.
- Op welke wijze wordt deze nazorg geleverd? Bijv. door het inrichten van een helpdesk, het openstellen van een telefoonnummer etc.
- Wie worden hierbij betrokken?

Als vastgesteld wordt dat de inbreuk ook tot schade voor het VfPf heeft geleid, wordt zo snel mogelijk bepaald welke maatregelen nodig zijn om die schade te beperken, te beëindigen en te herstellen. Daarbij wordt in ieder geval met het volgende rekening gehouden:

- Wat is de precieze schade? Reputatieschade, omzetschade, gijzelsoftware etc.
- Maakt het datalek de uitvoering van een bedrijfsproces onmogelijk en bestaat daarvoor een alternatieve werkwijze?
- Wat voor acties worden ondernomen om de reputatieschade te beperken en om de reputatie te herstellen?
- Wat voor acties worden ondernomen rondom de afwikkeling van aansprakelijkheidsstelling en boetes?
- Welke acties worden ondernomen ter voorkomen en communicatie aan medewerkers?

4.3 Actie Communiceren en escaleren

Als wordt besloten tot de oprichting van een IRT dan wordt de directeur en ook de Functionaris voor gegevensbescherming (FG) daarover geïnformeerd. Daarbij worden voorlopige inzichten en conclusies van Team P&S dan wel het IRT gedeeld waar mogelijk. De afdeling Communicatie wordt ook van de oprichting van het IRT op de hoogte gesteld met als doel dat de afdeling Communicatie kan aanhaken als nodig. De personen die security incidenten hebben gemeld, worden geïnformeerd over de resultaten nadat het security incident is behandeld en afgesloten.

Als Team P&S concludeert dat andere in- en externe personen 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 en/of organisaties.

Als Team P&S 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 directeur.

Als Team P&S inschat dat de ernst van het incident zodanig is dat acties nodig zijn waarvoor een MT-beslissing nodig is, wordt het MT op de hoogte gesteld en door Team P&S geadviseerd.

4.4 Actie Melden

4.4.1 Voorlopige Melding AP

Als Team P&S/IRT niet binnen 72 uur kan vaststellen dat sprake is van een meldingsplichtig datalek derde en/of vierde graads-incident als bedoeld in hoofdstuk 3), dan merkt Team P&S het security incident voorlopig aan als een meldingsplichtig datalek (3e graads incident) om de termijn te redden. Team P&S verricht vervolgens een voorlopige melding bij de AP via het Meldloket Datalekken. Zowel de Directie als de FG worden hiervan op de hoogte gebracht.

4.4.2 Melding AP

Als Team P&S (dan wel het IRT) vaststelt dat sprake is van een meldingsplichtig datalek (3^e graads security gebeurtenis), dan informeert Team P&S de AP binnen 72 uur (kalenderuren). De melding wordt verricht via de website van de AP aan de hand van het daarvoor beschikbare Meldformulier. Zowel de Directie als de FG worden hiervan op de hoogte gebracht.

4.4.3 Melding betrokkene(n)

Als Team P&S (dan wel het IRT) vaststelt dat sprake is van een meldingsplichtig datalek dat óók bij betrokkenen moet worden gemeld (4^e graads security gebeurtenis), dan bepaalt team P&S in samenspraak met de afdeling Communicatie de wijze waarop de betrokkenen geïnformeerd worden. Zowel de Directie als de FG worden hiervan op de hoogte gebracht.

In ieder geval wordt betrokkene 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 maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen. Op dit uitgangspunt zijn uitzonderingen denkbaar, bv. als passende en technische maatregelen zijn genomen of als het onevenredige inspanningen vergt om betrokkenen te informeren.

4.5 Actie Vastleggen en verzamelen van bewijsmateriaal

Team P&S hanteert bij de vastlegging altijd het template 'Logboek security gebeurtenissen'. Hierin wordt in ieder geval het volgende opgenomen:

- een samenvatting van de security gebeurtenis
- advisering op security incident, inclusief maatregelen en input IRT
- besluiten

Team P&S documenteert gedurende het beoordelingsproces alle relevante activiteiten, waaronder in ieder geval de resultaten van de beoordeling en genomen besluiten, voor latere analyse. Team P&S maakt hiervoor een opslaglocatie aan waar bewijsstukken en informatie dan wel documentatie over het security incident verzameld en veiliggesteld wordt. Door het bijhouden van registraties wordt het mogelijk gemaakt voor Team P&S om patronen in kwetsbaarheden waar te nemen, te monitoren, te beoordelen en te rapporteren met als doel: het voorkomen dan wel terugdringen van de kans dat kwetsbaarheden zich zullen materialiseren.

De administratie en/of andere bewijsstukken over het security incident worden gedocumenteerd in een daarvoor bestemde map onder een unieke titel op Sharepoint (link invoegen).

5. Actie Rapportage

Periodiek wordt de directeur middels de kwartaalrapportage geïnformeerd over security incidenten in de achterliggende periode. De rapportage wordt vervolgens in de eerstvolgende MT-vergadering ter kennisgeving aan het voltallige MT aangeboden.

6. Actie monitoring

De aangewezen eigenaar draagt er zorg voor dat de beheersmaatregel geïmplementeerd wordt en geeft een planning inclusief capaciteitsraming af wanneer de maatregel in place is.

Team P&S registreert de door de directeur aangewezen beheersmaatregelen in de Jaarkalender en volgt daarmee de voortgang. Indien nodig en afhankelijk van die voortgang stelt Team P&S interventies voor dan wel adviseert bijsturende acties om de doelstelling te bereiken van het implementeren van de beheersmaatregelen.

7. Evalueren

Jaarlijks vindt een evaluatie van security incidenten plaats. Van de kennis die is verkregen door het security incident te analyseren en op te lossen wordt lering getrokken door deze te gebruiken om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen. De informatie die is verkregen uit de evaluatie van informatiebeveiligingsincidenten wordt gebruikt om terugkerende of ingrijpende incidenten te identificeren en om zwakke plekken en kwetsbaarheden in bestaande (primaire) processen en architectuur op te lossen en te verbeteren.

Als uit de evaluatie blijkt dat uitgebreidere of aanvullende beheersmaatregelen nodig zijn om de frequentie, schade en kosten van toekomstige gebeurtenissen te beperken, dan worden deze ingezet.

De praktijksituaties van actuele informatiebeveiligingsincidenten worden gebruikt in een gebruikersbewustzijnstraining als voorbeelden van wat kan gebeuren, hoe te reageren op dergelijke incidenten en hoe deze in de toekomst te voorkomen.

8. RASCI-tabel

Actie	Ontdekker/melder[3]	Team P&S	Leverancier	Keten proceseigenaar	directie
Ontdekken, herkennen en melden bij Team P&S	Responsible (R)	Informed (I)	R	I	Accountable (A)
Beoordelen	I	R	Consulted (C)	C	A/I
Repareren, herstel	I	I	C/I	R	A/I
Communiceren, rapporteren en escaleren	I	R	I	I	A/I
Evalueren	C/I	C/I	C/I	R	A/I
Vastleggen, monitoren	C	R	C	C/I	A

[3] Dit kan een medewerker van een leverancier zijn.

Bijlage 1: Stroomschema incident