

<b>Hoofdproces: Informatiebeveiliging</b>	
<b>Document: 3 Melden en afhandelen incidenten VWUH</b>	<b>2022-2023</b>
Eigenaar: Bestuur VWUH.	Vastgesteld op 13-3-2023 door het Bestuur.
Gebruikers: alle medewerkers	Dit document is niet ingetrokken.

### 3. Melden en afhandelen incidenten VWUH

#### Inhoud

1	Doel van de procedure	2
2	Reikwijdte en gebruikers	2
2.1	Reikwijdte	2
2.2	Gebruikers	2
3	Relatie met andere documenten	2
4	Incidenten	3
4.1	Toelichting en voorbeelden	3
4.2	Classificatie incidenten	<b>Fout! Bladwijzer niet gedefinieerd.</b>
5	Meldprocedure	4
5.1	Melden incidenten	4
5.2	Afhandelen incidenten	5
5.2.1	Direct	5
5.2.2	Corrigerende maatregel	5
5.3	Administratie	5
5.4	Evaluatie en rapportage incidenten	5
6	Constateren kwetsbaarheden	6
7	Vaststellen doeltreffendheid	6
7.1	Administraties	6
7.2	Registraties	6
7.3	Criteria	6
8	Bijlagen	7
8.1	Bijlage 1: Protocol datalekken	7
8.1.1	Wat is een datalek?	7
8.1.2	Melding bij Autoriteit Persoonsgegevens	7
8.1.3	Melden aan betrokkenen	8

<b>Hoofdproces: Informatiebeveiliging</b>	
<b>Document: 3 Melden en afhandelen incidenten VWUH</b>	<b>2022-2023</b>
Eigenaar: Bestuur VWUH.	Vastgesteld op 13-3-2023 door het Bestuur.
Gebruikers: alle medewerkers	Dit document is niet ingetrokken.

## 1 Doel van de procedure

Voor VWUH is een stelselmatige afhandeling van informatiebeveiligingsincidenten belangrijk. Niet alleen uit oogpunt van bescherming van het bedrijfsbelang, maar ook in het belang van de beveiliging van informatie. Een goede afhandeling van incidenten kan de impact ervan minimaliseren en aanvullende risico's helpen beheersen. Voorts draagt een gedegen registratie en analyse van incidenten bij aan het treffen van adequate maatregelen, zodanig dat herhaling kan worden voorkomen. Belangrijk doel is het samen werken aan het verbeteren van de kwaliteit van werken.

## 2 Reikwijdte en gebruikers

### 2.1 Reikwijdte

De reikwijdte van dit document komt overeen met die van hoofdstuk 1. *Beleidsdocument informatiebeveiliging VWUH.*

### 2.2 Gebruikers

Gebruikers van dit document zijn:

- Security Officer.
  - o Draagt zorg voor de correctheid van het document.
- Bestuur.
  - o Moet het document vaststellen.
- Alle (vrijwillige) medewerkers van VWUH.
  - o Moeten zich conformeren aan de regels zoals gesteld in het document.

## 3 Relatie met andere documenten

Dit document heeft een relatie met documenten uit het ISMS (Information Security Management System) van VWUH.

Gebruikt de reikwijdte en doelstellingen zoals gegeven in hoofdstuk 1. **Beleidsdocument informatiebeveiliging VWUH.**

- Levert input op de gedragsregels die weergegeven staan in hoofdstuk 2. **Regels behandelen bedrijfsmiddelen en informatie.**
- Leidt tot de noodzaak van het uitvoeren van acties en het bijhouden van registraties. Deze staan weergegeven in hoofdstuk 5. **Jaarplanning informatiebeveiliging VWUH.** In deze jaarplanning staat ook de meta-informatie van het huidige document gegeven.

Uit alle documenten uit het ISMS blijkt dat er, voor specifieke onderwerpen, informatie-beveiligingsincidenten gemeld dienen te worden. Vanuit dat oogpunt hebben **alle** documenten uit het ISMS van VWUH een relatie met dit huidige document.

<b>Hoofdproces: Informatiebeveiliging</b>	
<b>Document: 3 Melden en afhandelen incidenten VWUH</b>	<b>2022-2023</b>
Eigenaar: Bestuur VWUH.	Vastgesteld op 13-3-2023 door het Bestuur.
Gebruikers: alle medewerkers	Dit document is niet ingetrokken.

## 4 Incidenten

### 4.1 Toelichting en voorbeelden

In dit hoofdstuk worden een aantal voorbeelden genoemd van informatiebeveiligingsincidenten. Er is sprake van een informatiebeveiligingsincident wanneer er een dreiging ontstaat voor de *beschikbaarheid van informatie* of informatiesystemen (de informatie is niet beschikbaar op het moment dat de organisatie deze nodig heeft),

de *integriteit van informatie* (de informatie is niet correct, volledig en/of door ongeautoriseerde derden gemanipuleerd) en tenslotte

de *exclusiviteit van informatie* (inzage van de informatie is niet uitsluitend voorbehouden aan de daartoe gemachtigde functionarissen).

Voorbeelden van informatiebeveiligingsincidenten zijn:

- Verlies, diefstal of onbevoegde inzage van (zeer) vertrouwelijke gegevens.
- (On)opzettelijk lekken van gegevens.
- Niet nakomen van gemaakte AVG afspraken.
- Ongeautoriseerde toegang tot beveiligde (digitale) gebieden en/of ruimten (bijv onaangekondigde binnenkomst van buiten VWUH).
- Onzorgvuldige omgang met beveiligingsbeleid (omgang wachtwoorden, clean-desk, etc.).
- Ontvangen van verdachte e-mail.
- Diefstal van hard- of software.
- Inbraak of pogingen daartoe.
- Onveilige situaties van allerlei aard.
- Schending van de beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie.
- Kwijtraken van bedrijfsmiddelen, zoals laptops en sleutels.

Technische kwetsbaarheden (bijv : Als de stroom uitvalt zal ook het automatisch in het slot vallen van onze "voor deur" wegvallen, waardoor deze open staat en het mogelijk is dat willekeurig wie onze ruimtes kan binnenkomen.

Houd er rekening mee dat een informatiebeveiligingsincident niet in hoeft te houden dat er daadwerkelijk iets fout is gegaan. Situaties waarin zaken fout hadden kunnen gaan, moeten ook gemeld worden. Ook verbeterpunten en niet effectieve maatregelen zijn informatiebeveiligings-incidenten.

<b>Hoofdproces: Informatiebeveiliging</b>	
<b>Document: 3 Melden en afhandelen incidenten VWUH</b>	<b>2022-2023</b>
Eigenaar: Bestuur VWUH.	Vastgesteld op 13-3-2023 door het Bestuur.
Gebruikers: alle medewerkers	Dit document is niet ingetrokken.

## 4.2. *Classificatie incidenten*

We onderscheiden, naar hun ernst, twee categorieën incidenten:

- Ernstig.
- Regulier.

Een incident valt in de categorie “Ernstig”, wanneer aan één of meer van de volgende voorwaarden is voldaan:

1. Het incident is mogelijk een datalek, of kan dit worden, in de zin van de AVG
2. Het incident kan leiden tot het verlies van beschikbaarheid, integriteit of vertrouwelijkheid, met mogelijk een verstoring van de bedrijfsprocessen van VWUH of haar cliënten en/of kan leiden tot imagoschade voor VWUH of haar cliënten.

(Wanneer een medewerker informatie en persoonsgegevens over en van een client bijvoorbeeld op een onbeveiligde USB-stick heeft gezet en deze USB buiten het kantoor van VWUH is verloren, of iemand neemt informatie op papier mee en dat kwijt raakt).

Een incident valt in de categorie ‘Regulier’ wanneer:

1. Het incident zeker niet kan leiden tot een datalek.
2. Het incident niet kan leiden tot imagoschade of een verstoring van de bedrijfsprocessen van VWUH of haar cliënten.

(Een medewerker documenten met gegevens van cliënten bijvoorbeeld heeft opgeslagen op het bureaublad van een van de laptops op kantoor).

## 5 Meldprocedure

Er kan sprake zijn van een datalek of een incident.

In deze paragraaf wordt het melden van een incident besproken. In paragraaf 8 komt het melden van een datalek aan de orde.

### 5.1 *Melden incidenten*

Incidenten moeten gemeld worden middels het daartoe beschikbare document (melden incident) dat te vinden is op de website van VWUH. Iedereen heeft de plicht incidenten te melden. Dit kan op de website van [www.vwuh.nl](http://www.vwuh.nl). Ga naar [Meer over ons](#). Onder het kopje ‘Belangrijke documenten’ is het document ‘[melden van incidenten](#)’ te vinden. Dat kan ingevuld worden, vermeld zo concreet mogelijk wat het incident is. Dit document sturen naar [AVG@vwuh.nl](mailto:AVG@vwuh.nl).

Degenen die incidenten melden, wordt gevraagd om de volgende informatie te geven:

- Een korte omschrijving van het incident.
- Welke datum en tijd het incident heeft opgetreden.
- Waar het incident zich heeft voorgedaan (fysieke locatie en/of systeem).
- De mogelijke oorzaken van het incident.
- Of het incident een probleem is voor: de beschikbaarheid van informatie, de integriteit van informatie en/of de vertrouwelijkheid van informatie.

<b>Hoofdproces: Informatiebeveiliging</b>	
<b>Document: 3 Melden en afhandelen incidenten VWUH</b>	<b>2022-2023</b>
Eigenaar: Bestuur VWUH.	Vastgesteld op 13-3-2023 door het Bestuur.
Gebruikers: alle medewerkers	Dit document is niet ingetrokken.

- Omschrijf om welke soorten informatie het gaat (bijvoorbeeld documenten, mails, dossiers) geef ook de klasse aan van elke informatiesoort.

Iedereen heeft de plicht incidenten te melden.

Incidenten die vallen in de categorie “Ernstig” moeten zo snel mogelijk gemeld worden:

- Gedurende openingstijden/kantoortijden van VWUH moet de melding gedaan worden door telefonisch contact met het kantoor van VWUH op 0343-413004.
- Buiten openingstijden/kantoortijden moet de melding gedaan worden door te bellen naar de coördinator (Security Officer). Na werktijd kan naar haar privénummer gebeld worden.

## 5.2 Afhandelen incidenten

Na een incident coördineert de Security Officer de corrigerende acties.

### 5.2.1 Direct

De Security Officer:

- Doorloopt wanneer sprake kan zijn van een Datalek het “Protocol Datalekken” (zie bijlage B, par 8.1).
- Bespreekt, wanneer het incident kan leiden tot een verstoring van de werkprocessen van VWUH, met het betreffende bestuurslid of zijn/haar vervanger welke maatregelen nodig zijn.
- Verzamelt wanneer nodig bewijsmateriaal, zoals logbestanden.
- Neemt maatregelen die direct te nemen zijn.

### 5.2.2 Corrigerende maatregel

Nadat het incident voor de korte termijn is afgehandeld, gaat de Security Officer na of een corrigerende maatregel nodig is. Voorbeelden van een corrigerende maatregel zijn:

- Het toevoegen van een actie project aan het 3. *Behandelplan informatiebeveiliging VWUH*.
- Het toevoegen van een controle aan de 5. *Jaarplanning informatiebeveiliging VWUH*.
- Aanpassen of opstellen van beleid of procedures.
- Het verspreiden van een nieuwsbrief onder medewerkers om bewustzijn te verhogen.

## 5.3 Administratie

De Security Officer zorgt voor de volgende administraties (op tabblad 5 van de *Jaarplanning*):

- Overzicht incidenten, met de informatie die is gemeld.
- De corrigerende acties die zijn gepland of uitgevoerd.
- Eventueel: het verzamelde bewijsmateriaal, zoals bijvoorbeeld incident-gerelateerde auditverslagen.
- Eventueel: of het incident is gemeld als datalek.
- Eventueel: het resultaat van de analyse naar de oorzaak van het incident.

<b>Hoofdproces: Informatiebeveiliging</b>	
<b>Document: 3 Melden en afhandelen incidenten VWUH</b>	<b>2022-2023</b>
Eigenaar: Bestuur VWUH.	Vastgesteld op 13-3-2023 door het Bestuur.
Gebruikers: alle medewerkers	Dit document is niet ingetrokken.

Het kan zijn dat een incident impact heeft op cliënten of andere belanghebbenden van VWUH. De Security Officer weegt af of er extern gecommuniceerd moet worden over een incident. Pas nadat toestemming is gekregen van het Bestuur borgt de Security Officer dat de communicatie plaatsvindt.

## **5.4 Evaluatie en rapportage incidenten**

De Security Officer analyseert jaarlijks de incidenten, ze gebruikt hierbij de documenten melden incidenten die via de website zijn binnen gekomen. Dit heeft twee doelen:

1. Evaluatie. Het stelt de Security Officer in staat om trends te ontdekken en lering te trekken uit de informatiebeveiligingsincidenten.
2. Input voor de rapportage aan het bestuur. Door over de informatiebeveiligingsincidenten te rapporteren krijgt het Bestuur inzicht in wat er speelt op het gebied van informatiebeveiliging.

De Security Officer stelt een registratie (*Registratie analyse incidenten*) op, deze bevat:

- Een overzicht van de (groepen) incidenten die zich hebben voorgedaan.
- Of er trends zijn in de incidenten.
- Wat de oorzaak van deze trends is.
- Welke acties noodzakelijk zijn om deze trends in te toekomst te voorkomen, en hoe dit geborgd wordt.

De Security Officer neemt de registratie in eigen beheer.

## **6 Constateren kwetsbaarheden**

De Security Officer is op de hoogte van nieuwe informatie over digitale veiligheid die gepubliceerd wordt op de website van het Nationaal Cyber Security Centrum (NCSC). Ernstige digitale veiligheidsincidenten moeten in het kader van de Wet beveiliging netwerk- en informatiesystemen (Wbni) gemeld worden op de website van het NCSC. Wanneer zich een incident mbt digitale veiligheid voordoet die relevant is voor VWUH meldt de Security Officer dit als incident en behandelt deze volgens de gestelde procedure.

## **7 Vaststellen doeltreffendheid**

De doeltreffendheid van de in dit document opgenomen aanwijzingen wordt jaarlijks beoordeeld door de Security Officer aan de hand van de volgende administraties, registraties en criteria.

### **7.1 Administraties**

Op basis van dit document moeten de volgende administraties aanwezig zijn:

- Rapportages.

### **7.2 Registraties**

Op basis van dit document moeten de volgende registraties aanwezig zijn:

- Informatiebeveiligingsincidenten.
- Registratie en analyse incidenten.

<b>Hoofdproces: Informatiebeveiliging</b>	
<b>Document: 3 Melden en afhandelen incidenten VWUH</b>	<b>2022-2023</b>
Eigenaar: Bestuur VWUH.	Vastgesteld op 13-3-2023 door het Bestuur.
Gebruikers: alle medewerkers	Dit document is niet ingetrokken.

### 7.3 Criteria

De volgende criteria bepalen of de doeltreffendheid voldoende is:

- Uit een steekproef blijkt dat negen van de tien gemelde incidenten voldoen aan de eisen zoals gesteld in dit document.
- In het laatste managementrapport is een analyse gegeven van de incidentmeldingen in het jaar voorafgaand aan het managementrapport.
- Uit de incidentmeldingen blijkt dat datalekken op een juiste manier afgehandeld zijn en dat hiervoor de juiste registraties aanwezig zijn.
- Er is een *Registratie analyse incidenten* aanwezig, jonger dan 1 jaar oud.

In alle andere gevallen wordt de doeltreffendheid van dit document beoordeeld als onvoldoende.

P.S.: Deze criteria zijn nog niet SMART geformuleerd, omdat er momenteel nog geen stuurcijfers beschikbaar zijn. Als het ISMS meer volwassen is en er meer stuurcijfers beschikbaar zijn worden waar mogelijk en relevant, doelstellingen SMART geformuleerd.

## 8 Bijlagen

### 8.1 Bijlage 1: Protocol datalekken

#### 8.1.1 Wat is een datalek?

Er is sprake van een datalek wanneer gegevens die direct of indirect herleidbaar zijn tot een persoon in ongeautoriseerde handen komen of wanneer deze persoonsgegevens ten onrechte worden vernietigd. Vanuit het oogpunt van het medisch beroepsgeheim heeft privacy in de zorg bovendien nog een extra dimensie die de impact van een datalek vergroot.

Niet elk beveiligingsincident is een datalek. *Er is sprake van een datalek als er bij het beveiligingsincident persoonsgegevens verloren zijn gegaan, in ongeautoriseerde handen zijn gekomen of als onrechtmatige verwerking van persoonsgegevens redelijkerwijs niet uit gesloten kunnen worden. Ook is er geen sprake van een datalek als er een zwakke plek is in de beveiliging, waardoor mogelijk een datalek heeft kunnen gebeuren.*

#### 8.1.2 Melding bij Autoriteit Persoonsgegevens

Er zijn situaties mogelijk waarin een datalek niet gemeld hoeft te worden. Kijk voor de actuele regelgeving op de website van de Autoriteit Persoonsgegevens. Een factor die hierbij een rol speelt is de aard van de gelekte persoonsgegevens. Een melding is noodzakelijk indien de persoonsgegevens van gevoelige aard zijn. Voorbeelden hiervan zijn:

- *Bijzondere persoonsgegevens zoals bedoeld in artikel 16 Wbp.*  
Dit zijn persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

<b>Hoofdproces: Informatiebeveiliging</b>	
<b>Document: 3 Melden en afhandelen incidenten VWUH</b>	<b>2022-2023</b>
Eigenaar: Bestuur VWUH.	Vastgesteld op 13-3-2023 door het Bestuur.
Gebruikers: alle medewerkers	Dit document is niet ingetrokken.

- *Gegevens over de financiële of economische situatie van betrokkene.*  
Hieronder vallen bijvoorbeeld gegevens over (problematische) schulden, salaris- en betalingsgegevens.
- *(Andere) gegevens die kunnen leiden tot stigmatisering of uitsluiting van betrokkene.*  
Hieronder vallen bijvoorbeeld gegevens over gokverslaving, prestaties op school of werk of relatieproblemen.
- *Gebruikersnamen, wachtwoorden en andere inloggegevens.*  
De mogelijke gevolgen voor betrokkenen hangen af van de verwerking en van de persoonsgegevens waar de inloggegevens toegang tot geven. Bij de afweging moet worden betrokken dat veel mensen wachtwoorden hergebruiken voor verschillende verwerkingen.
- *Gegevens die kunnen worden misbruikt voor (identiteits)fraude.*  
Het gaat hierbij onder meer om biometrische gegevens, kopieën van identiteitsbewijzen en om het Burgerservicenummer (BSN).

Andere factoren die een rol spelen zijn de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt.

Let op! Als de aard van de gegevens daar aanleiding toe geeft kan het zijn dat een datalek waarbij de persoonsgegevens van slechts één persoon betrokken zijn, gemeld moet worden bij de Autoriteit Persoonsgegevens.

Melden van een datalek moet binnen 72 uur plaatsvinden via een webformulier op de website van de Autoriteit Persoonsgegevens (<https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0>).

### **8.1.3 Melden aan betrokkenen**

Datalekken die gemeld zijn bij de Autoriteit Persoonsgegevens hoeven niet altijd aan betrokkenen gemeld te worden. Hiervoor moet een aparte afweging gemaakt worden. Een datalek wordt gemeld aan betrokkenen indien het datalek waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Betrokkenen kunnen door het verlies, onrechtmatig gebruik of misbruik in hun belangen worden geschaad. Bijvoorbeeld onrechtmatige publicatie, aantasting in eer en goede naam, (identiteits)fraude of discriminatie. Als er persoonsgegevens van gevoelige aard zijn gelekt dan moet dit, zoals de wet voorschrijft onverwijld, aan de betrokkenen en de Autoriteit Persoonsgegevens gemeld worden.

Betrokkenen hoeven niet geïnformeerd te worden indien de persoonsgegevens onbegrijpelijk dan wel ontoegankelijk zijn voor derden door beschermende cryptografische bewerkingen zoals encryptie en hashing.