

RWS ONGECLASSIFICEERD

Handboek Security

Deel VI De Basis Security Maatregelen

Datum	7 juni 2017
Status	Definitief

Colofon

Metagegevens

Proces:	Aanleg & Onderhoud
Proceseigenaar:	Jean-Luc Beguin
Netwerk:	Droog, Nat
Hoofdkennisveld:	Veiligheid en Crisis
Kennisveld:	Security
Soort document:	Kader (deel I heeft de status van een kader, deel II tot en met IV hebben de status van handreiking, de overige delen zijn informatie)
Datum vaststelling:	
Vastgesteld door:	
Van kracht vanaf:	
Overgangsregeling:	
Beveiliging:	Ongeclassificeerd
Beheerder:	GPO, afdeling Advies Technisch Management, Dirk-Jan Molenaar
Informatie:	Kaderadviseurs GPO/PPO
Verbetervoorstellen:	Dirk-Jan Molenaar
Toepassingsgebied:	Projecten voor aanleg en onderhoud (GPO/PPO) Beheer van objecten (OAM)
Versienummer:	3.2.0
Houdbaar tot:	Juni 2018
Monitoring gebruik:	GPO, afdeling Advies Technisch Management

Context

Procesdoel	uniformering van processen en voorzieningen, nodig voor borging van fysieke beveiliging van objecten
Inhoudelijk doel	Beheersing van alle fysieke beveiligingsaspecten van een object

Gebruikersgroepen

IPM rolhouders, projectadviseurs integrale veiligheid, assetmanagers	
Rol	Coördineren, initiëren, uitvoeren, communiceren, monitoren
benodigde kennis	Basiscursus integrale veiligheid in projecten

Hoofdproces

Aanleg & Onderhoud

Relatie met andere RWS standaarden

Wettelijk	Zie deel IV, hoofdstuk 2, Van kracht zijnde voorschriften en normen voor de securityvoorzieningen
Bovenliggend	Kader Veiligheidsmanagement RWS, 14 september 2011, WVL
Nevenliggend	Kader Integrale Veiligheid in Projecten 3.1

Toepassingsbereik

- Intern RWS, bij:
- Aanlegprojecten, van contractvoorbereiding tot oplevering;

- Onderhoudsprojecten, van contractvoorbereiding tot einde contract.
- Assetmanagement, areaalbeheer

Afwijken van kader

Conform de regels van de Werkwijzer RWS met toestemming vooraf van:

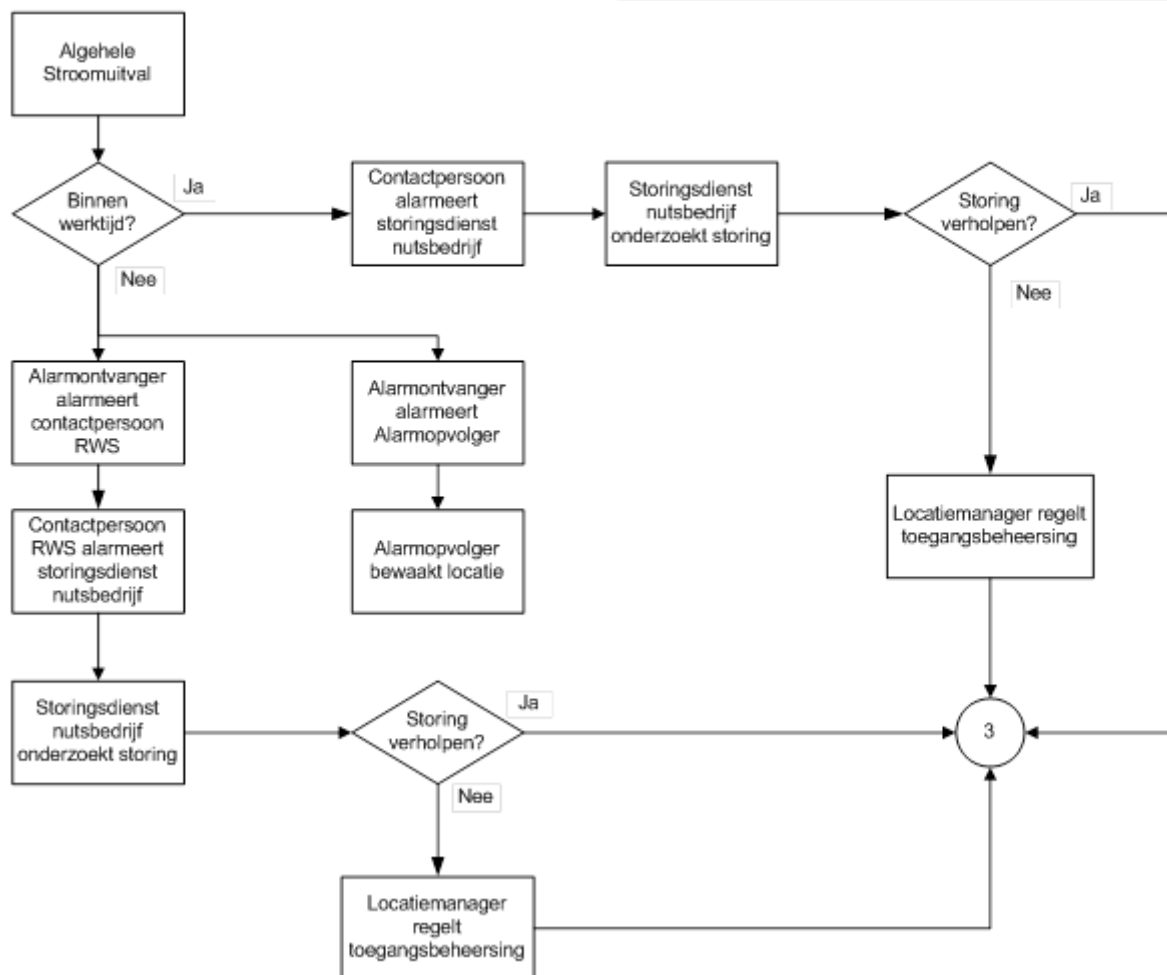
- de interne opdrachtgever;
- (tijdens verkenning en planuitwerking:) het Programmabureau Verkenningen & Planstudies voor het Hoofdwegennet en Hoofdvaarwegennet en het Programmabureau Aanleg Hoofdwatersysteem;
- (tijdens realisatie:) de portfoliomanager.

Leg afwijking met bijbehorende toestemming vast in het projectarchief. Geef de afwijking door aan de Kaderbeheerder (zie hierboven), voor het interne leerproces en verbetering van het Kader.

Inhoud

1	Gedragsregel beveiliging van informatie en eigendommen	10
2	Gedragsregel beveiliging voor bezoekers en derden	13
3	Gedragsregel voor gebruik e-mail- en internetverkeer	14
4	Securityprocedures RWS	17
5	Kaderstellende securityprocedure inhuur securitydienstverleners RWS	19
5.1	Organisatie en bedrijfsvoering beveiliging	19
5.2	Alarmopvolging	19
5.3	Sleutelservice (Beveiligingsdienst)	20
5.4	Brand-, sluit- en controleronden (Beveiligingsdienst)	20
5.5	Klachtbehandeling	20
5.6	Geheimhouding	20
6	Standaard alarmprotocollen bij security-incidenten RWS	21

Procedure ALGEHELE STROOMUITVAL



30

Wijzigingenoverzicht

Datum	Versie	Wijziging
December 2013	1.1	Typefouten hersteld en arceringen verwijderd
Maart 2014	1.2	Waardering wegcategorieën aangepast
Mei 2014	1.3	Consistentie in terminologie aangebracht
December 2014	2.0	Actualisering op basis van ervaringen met toepassing in de praktijk (indelingscriteria, weging categoriseringsfactoren), aanvullingen met uitgewerkte objecttypen en combinaties van objecttypen en de samenhang met Cybersecurity
Maart 2015	2.1	Versienummer gewijzigd
Juni 2015	3.0	Aanpassingen o.b.v. de ervaringen vanuit het project IMPAKT in de BSN-opbouw.
December 2015	3.1	Bijlage 7 verplaatst naar Deel V.
Juni 2017	3.2	Colofon aangepast naar aanleiding van wijzigingen in deel II en III (objecttypen toegevoegd)

1 Gedragsregel beveiliging van informatie en eigendommen

Algemeen

Elke medewerker draagt zorg voor de effectieve opberging of vernietiging van vertrouwelijke informatie op papier, vanaf het moment dat die niet meer voor de eigen werkuitvoering of die van een collega nodig is. Vernietiging in een papierversnipperaar of beveiligde papiercontainer.

Bij tijdelijk verlaten van de werkplek

Indien een medewerker de eigen werkruimte voor langere tijd verlaat, draagt hij/zij er zorg voor dat:

- Vertrouwelijke informatie en/of documenten zijn opgeborgen in het bureau of een kast;
- Is afgemeld op het systeem en de apparatuur is uitgeschakeld;
- De eigen laptop gelocked is opgeborgen;
- Waardevolle privé-eigendommen afgesloten zijn opgeborgen.

Bij (aangekondigde) bezoekers op de werkplek

Elke medewerker zorgt ervoor dat bij aangekondigde bezoekers in de werkruimte de onder zijn/haar hoede verkerende vertrouwelijke documenten effectief zijn afgeschermd.

Bij beëindiging werkdag

Elke medewerker zorgt ervoor, dat:

- Aan het einde van zijn of haar werkdag de eigen werkplek is ontdaan van informatie die niet voor buitenstaanders is bestemd;
- Aan het einde van zijn of haar werkdag is uitgelogd op het systeem en dat de apparaten zijn uitgeschakeld, tenzij dit uitdrukkelijk is uitgezonderd;
- De vertrouwelijke documenten die bij hem/haar in beheer zijn, afgesloten zijn opgeborgen na einde werktijd.

Laatst vertrekkende medewerker werkruimte

De laatste vertrekkende medewerker controleert bij het verlaten van de werkruimte of:

- de ramen deugdelijk zijn gesloten;
- alle apparatuur is uitgeschakeld;
- waardevolle spullen afgesloten zijn opgeborgen.

Bij vergaderingen/besprekingen

Elke medewerker draagt er zorg voor, dat tijdens pauzes en bij beëindiging van besprekingen en/of vergaderingen zowel binnen als buiten de lokaliteiten van Rijkswaterstaat:

- vertrouwelijke documenten niet onbeheerd in de bespreekruimte worden achtergelaten;
- aktetassen en aktetassen niet onbeheerd worden achtergelaten;
- laptops en overige informatiedragers niet onbeheerd worden achtergelaten.

In de auto

Bij het verlaten van de auto binnen werktijd, draagt elke medewerker er zorg voor dat:

- vertrouwelijke documenten worden meegenomen of in de kofferbak wordt opgeborgen;
- aktetassen/aktekoffers niet onbeheerd worden achtergelaten;
- laptops en overige informatiedragers worden meegenomen of in de kofferbak worden opgeborgen.

Bij het verlaten van de auto na werktijd, draagt elke medewerker er zorg voor dat;

- vertrouwelijke documenten/informatie worden meegenomen in huis of hotel;
- laptops en overige informatiedragers nooit in de auto worden achtergelaten, ook niet in de kofferbak.

Thuis

Elke medewerker draagt er zorg voor, dat thuis:

- vertrouwelijke documenten beschermd tegen vernieling/vernietiging en diefstal zijn opgeborgen;
- laptops beschermd tegen diefstal zijn opgeborgen.

2 Gedragsregel beveiliging voor bezoekers en derden

(Bestaande procedures van RWS invoegen)

3 Gedragsregel voor gebruik e-mail- en internetverkeer

Doel van de afspraken

Deze regeling geeft de wijze aan waarop binnen RWS wordt omgegaan met e-mail- en internetgebruik. Deze omvat gedragsregels ten aanzien van verantwoord e-mail- en internetgebruik en regels over de wijze waarop controle op e-mail- en internetgebruik plaats vindt.

De controle op persoonsgegevens over e-mail- en internetgebruik vindt plaats met als doel:

- systeem- en netwerkbeveiliging
- bescherming van bedrijfsgeheimen
- voorkomen van negatieve publiciteit
- tegengaan van "verboden gebruik"
- kosten- en capaciteitsbeheersing

Algemene uitgangspunten

De controle op e-mail- en internetgebruik zal overeenkomstig deze afspraak uitgevoerd worden. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de Wet bescherming persoonsgegevens (WBP) en in overleg met de Ondernemingsraad gehandeld worden.

Gestreefd wordt naar een goede balans tussen controle op verantwoord e-mail- en internetgebruik en bescherming van de privacy van werknemers op de werkplek.

Persoonsgegevens over e-mail- en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden.

E-mailgebruik

Werknemers mogen

1. het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.
2. Het versturen van e-mailberichten moet voldoen aan de volgende voorwaarden
 - Een correcte vermelding van afzender
 - Duidelijke onderwerpaanduiding indien het een privé-mail betreft
3. het is niet toegestaan om:
 - Dreigende, beledigende, seksueel getinte dan wel discriminerende berichten te versturen
 - Kettingbrieven te versturen
 - Berichten te versturen die conflicteren met de belangen van RWS

Internetgebruik

1. Werknemers mogen het internetsysteem voor persoonlijke doeleinden gebruiken mits niet storend voor de dagelijkse werkzaamheden en het computernetwerk.
2. Het is niet toegestaan om:
 - Sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten.
 - Op internet in strijd met de wet of onethisch te handelen.

- Software en applicaties te downloaden.

Controle

1. Controle op e-mail- en internetgebruik vindt slechts plaats in het kader van in artikel 1.2 genoemde doelen.
2. Bij RWS vinden de volgende controles plaats:
 - Voor het tegengaan van virussen en andere schadelijke programma's, in het kader van **systeem- en netwerkbeveiliging**, wordt het e-mail- en internetgebruik op geautomatiseerde wijze gecontroleerd.
 - Controle op het uitlekken van **bedrijfsgeheimen** vindt plaats op basis van steekproefsgewijze contentfiltering. Een verdacht bericht wordt apart gezet voor nader onderzoek.
 - Controle in het kader van het voorkomen van **negatieve publiciteit** vindt plaats op basis van contentfiltering. Verdachte berichten worden geautomatiseerd terug gestuurd naar de afzender en "verboden" sites geblokkeerd.
 - Controle in het kader van het tegengaan van **"verboden gebruik"** vindt in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.
 - Controle in het kader van **kosten- en capaciteitsbeheersing** wordt beperkt tot verkeersgegevens (tijd, hoeveelheid, omvang, ed.)
3. Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een werknemer of een groep werknemers ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaats vinden.
4. Controle beperkt zich in principe tot verkeersgegevens van het gebruik van e-mail en internet. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.
5. "Verboden" e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Overige controle vindt slechts steekproefsgewijs plaats.
6. Werknemers ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken.

4 Securityprocedures RWS

Uitgifte Rijkswaterstaateigendommen

De op persoon uit te reiken Rijkswaterstaateigendommen, welke noodzakelijk zijn om toegang tot de werkplek te verkrijgen, alsmede de bedrijfsmiddelen ten behoeve van het persoonlijk functioneren worden bij uitgifte en inname geregistreerd. Voor de uitgifte en inname wordt door de medewerker getekend.

Autorisatieregeling medewerkers toegang gebouwen en terreinen

Rijkswaterstaat bepaalt waar en wanneer medewerkers toegang hebben tot de terreinen en de gebouwen. De toegangsautorisatie is zowel gespecificeerd naar dagen als tijdstippen. De autorisatieregeling is ook van toepassing op medewerkers van derdenbedrijven.

Aanwezigheidsregistratie medewerkers

Van alle op de terreinen en in gebouwen aanwezige medewerkers (Rijkswaterstaat en derdenbedrijven) wordt ten behoeve van een effectieve ontruiming in geval van een calamiteit de aanwezigheid in een gebouw of op een terrein geregistreerd.

Herkenbaarheid medewerkers, inhuurpersoneel, leveranciers

Alle op de terreinen en in gebouwen aanwezige medewerkers worden voorzien van een personeelsbadge. De personeelsbadge is voorzien van een pasfoto met de personalia van de badgehouder. De badge dient tijdens het verblijf op het terrein en in de gebouwen zichtbaar te worden gedragen. De lay-out van de personeelsbadge maakt onderscheid tussen Rijkswaterstaat, aannemer en overige derdenbedrijven.

Bezoekersregeling

Voor bezoekers geldt een legitimatieplicht. Bezoekers worden gedurende het verblijf op het terrein of in het gebouw door de ontvangende medewerker begeleid. Bezoekers dragen tijdens het verblijf een bezoekersbadge.

Legitimatieplicht

Op vordering van een daartoe geautoriseerde medewerker dient een ieder zich op de terreinen en in de gebouwen van Rijkswaterstaat te kunnen legitimeren.

5 Kaderstellende securityprocedure inhuur securitydienstverleners RWS

Onder beveiligers wordt zowel verstaan de Particuliere alarmcentrale als de Beveiligingsdienst of Toezichtcentrale

5.1 Organisatie en bedrijfsvoering beveiligers

1. De beveiligers voldoet aan alle wettelijk voorwaarden en eisen, alsmede aan die gesteld door de branche-organisatie Vereniging Particuliere Beveiligingsorganisaties (VPB). De beveiligers overlegt aan Rijkswaterstaat de daarop betrekking hebbende documentatie.
2. De beveiligers is 24 uur per dag op een nader aan te geven wijze telefonisch bereikbaar.
3. De beveiligers beantwoordt elk verzoek om inlichtingen binnen 1 werkdag en spreekt concreet de afhandeling van het verzoek met de vertegenwoordiger van Rijkswaterstaat af.
4. De beveiligers bezit een kwaliteitszorgsysteem en handelt daarnaar. De beveiligers overlegt aan Rijkswaterstaat de daarop betrekking hebbende documentatie.
5. Het documentenbeheer bij de beveiligers is zodanig geregeld, dat beveiligingsgegevens van Rijkswaterstaat voor onbevoegden niet herleidbaar zijn. De beveiligers overlegt aan Rijkswaterstaat de daarop betrekking hebbende documentatie.
6. De uitvoering geschiedt alleen door gekwalificeerde beveiligingsmedewerkers. De beveiligers overlegt aan Rijkswaterstaat de daarop betrekking hebbende documentatie.
7. De beveiligingsmedewerkers ontvangen vóór aanvang van de werkzaamheden schriftelijk alsmede mondeling uitvoeringsinstructies. Deze instructie wordt herhaald indien feiten en/of omstandigheden op de werkplek zijn gewijzigd.
8. De beveiligingsmedewerkers worden tijdens de uitvoering van hun werkzaamheden minimaal eenmaal per kwartaal gecontroleerd op een juiste uitvoering van de werkzaamheden.
9. De beveiligingsmedewerkers handelen naar de algemene instructie van de beveiligers, welke aan Rijkswaterstaat ter beschikking wordt gesteld.

5.2 Alarmopvolging

1. Een alarmmelding door een alarmgever wordt binnen 1 minuut door de eigen centrale van de beveiligers aangenomen.
2. De alarmopvolgingstijd (aannemen melding alarmgever – ter plaatse risico-object) is onder alle omstandigheden maximaal 20 minuten.
3. De inspectie van de buitenzijde van het risico-object van Rijkswaterstaat bij alarmmelding omvat alle gevelopeningen, voor zover bereikbaar.
4. Na uitvoering van deze inspectie wordt de alarmgever onmiddellijk geïnformeerd.
5. In geval van braaksporen wordt de komst van de politie en/of sleutelhouder afgewacht. De beveiligers consolideert tot dat moment de aangetroffen situatie.
6. Per alarmopvolging wordt aan Rijkswaterstaat gerapporteerd:

- a. Tijdstip alarmmelding
- b. Tijdstip aankomst bij risico-object
- c. Tijdstip afhandeling alarmopvolging
- d. Bijzonderheden t.a.v. het risico-object
- e. Bijzonderheden t.a.v. omgeving
- f. Ondernomen acties

5.3 Sleutelservice (Beveiligingsdienst)

1. De sleutels van de risico-objecten zijn gecodeerd op een wijze, dat herleiding tot het risico-object voor buitenstaanders niet mogelijk is.
2. Het beheer van de sleutels in de surveillanceauto's is zodanig, dat onbevoegden onder geen enkele voorwaarde de beschikking over sleutels kunnen krijgen.
3. Het beheer van de sleutels in de gebouwen van de beveiligers is zodanig, dat onbevoegden niet de beschikking over de sleutels van de risico-objecten kunnen krijgen.

5.4 Brand-, sluit- en controleronden (Beveiligingsdienst)

1. De surveillant vangt op het overeengekomen tijdstip daadwerkelijk met de werkzaamheden aan.
2. Per risico-object wordt een op het object toegesneden Rijkswaterstaat-instructie gevolgd.
3. De beveiliger draagt zorg voor een regeling van de werkwijze en procedures t.a.v. de door Rijkswaterstaat aan te geven wijzigingen van aanvangstijden, aard en omvang van de werkzaamheden.

5.5 Klachtbehandeling

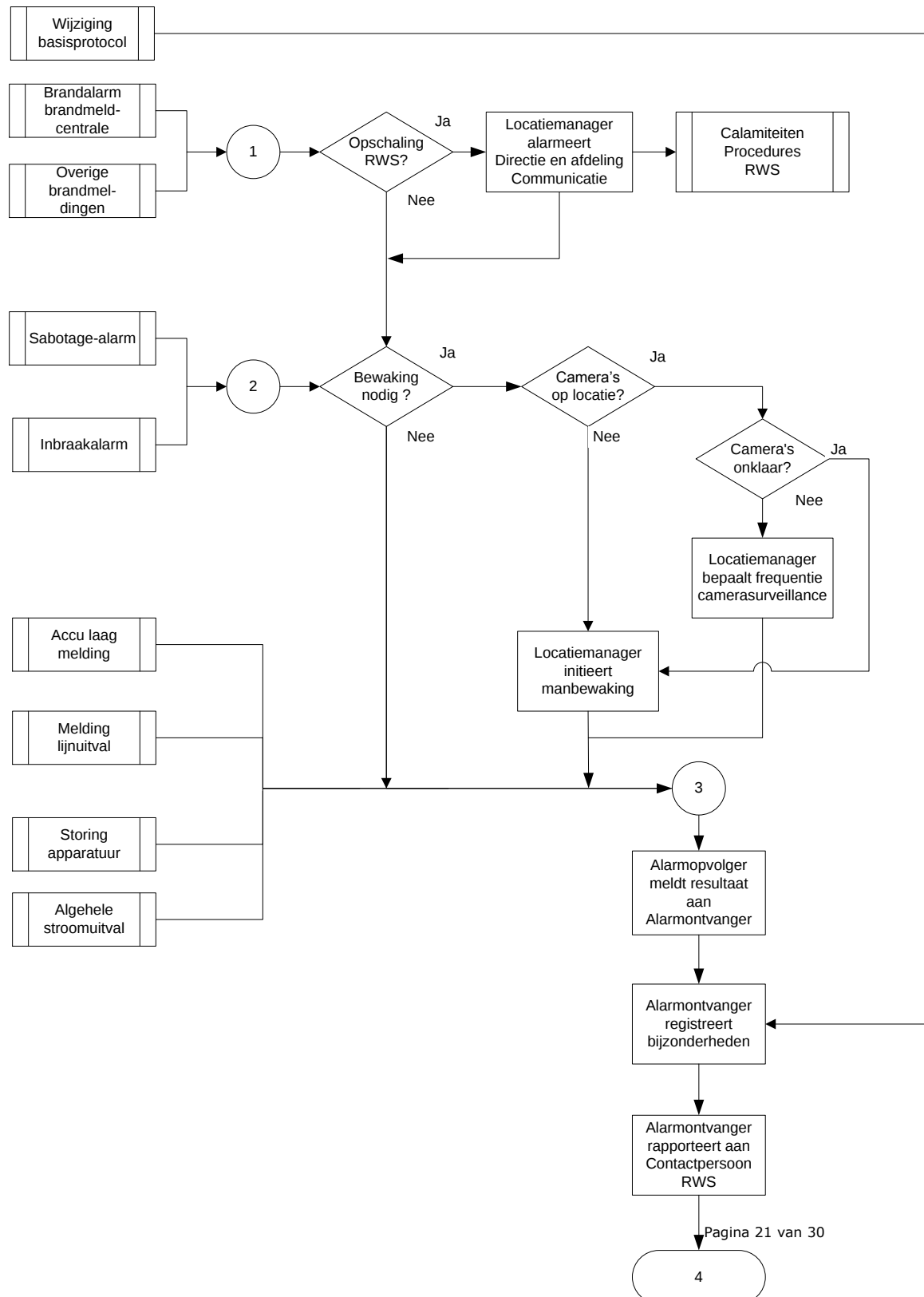
Klachten over de performance van de beveiliger worden binnen 1 werkdag primair getoetst aan de in de overeenkomst opgenomen prestatie-afspraken. De beveiliger behandelt de klacht conform de eigen klachtenregeling, waarvan een exemplaar aan Rijkswaterstaat ter beschikking wordt gesteld. De klachtafhandeling wordt schriftelijk gemotiveerd. Rijkswaterstaat ontvangt binnen een nader vast te stellen tijd de schriftelijke afhandeling van de door de beveiliger afgehandelde klacht.

5.6 Geheimhouding

De beveiliger verplicht zich jegens Rijkswaterstaat om de gegevens die hij uit hoofde van zijn werkzaamheden voor Rijkswaterstaat verkrijgt, strikt vertrouwelijk in ontvangst te nemen en niet anders dan met schriftelijke toestemming van Rijkswaterstaat aan derden kenbaar te maken.

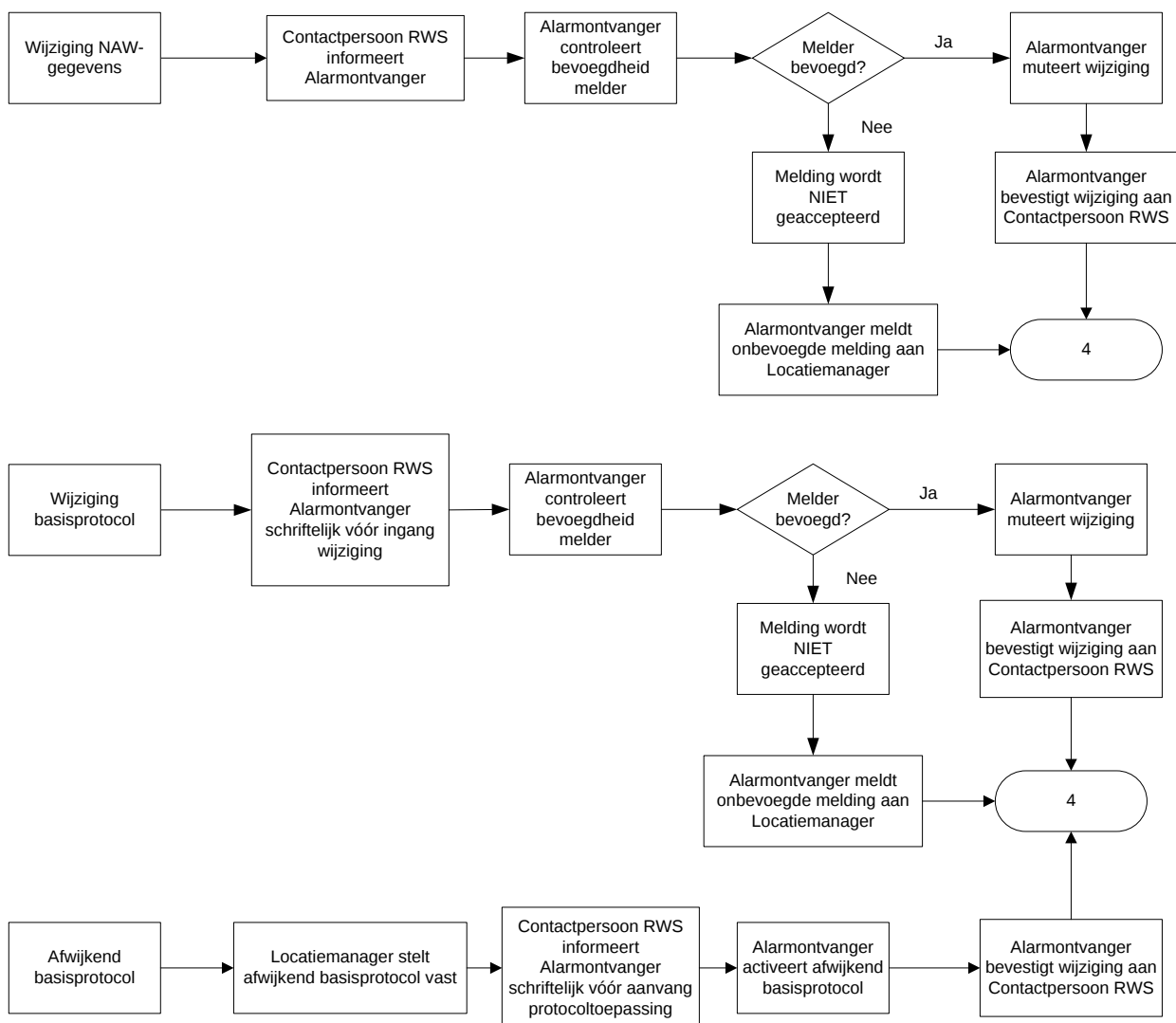
6 Standaard alarmprotocollen bij security-incidenten RWS

Structuur stroomschema's alarmafhandeling Rijkswaterstaat

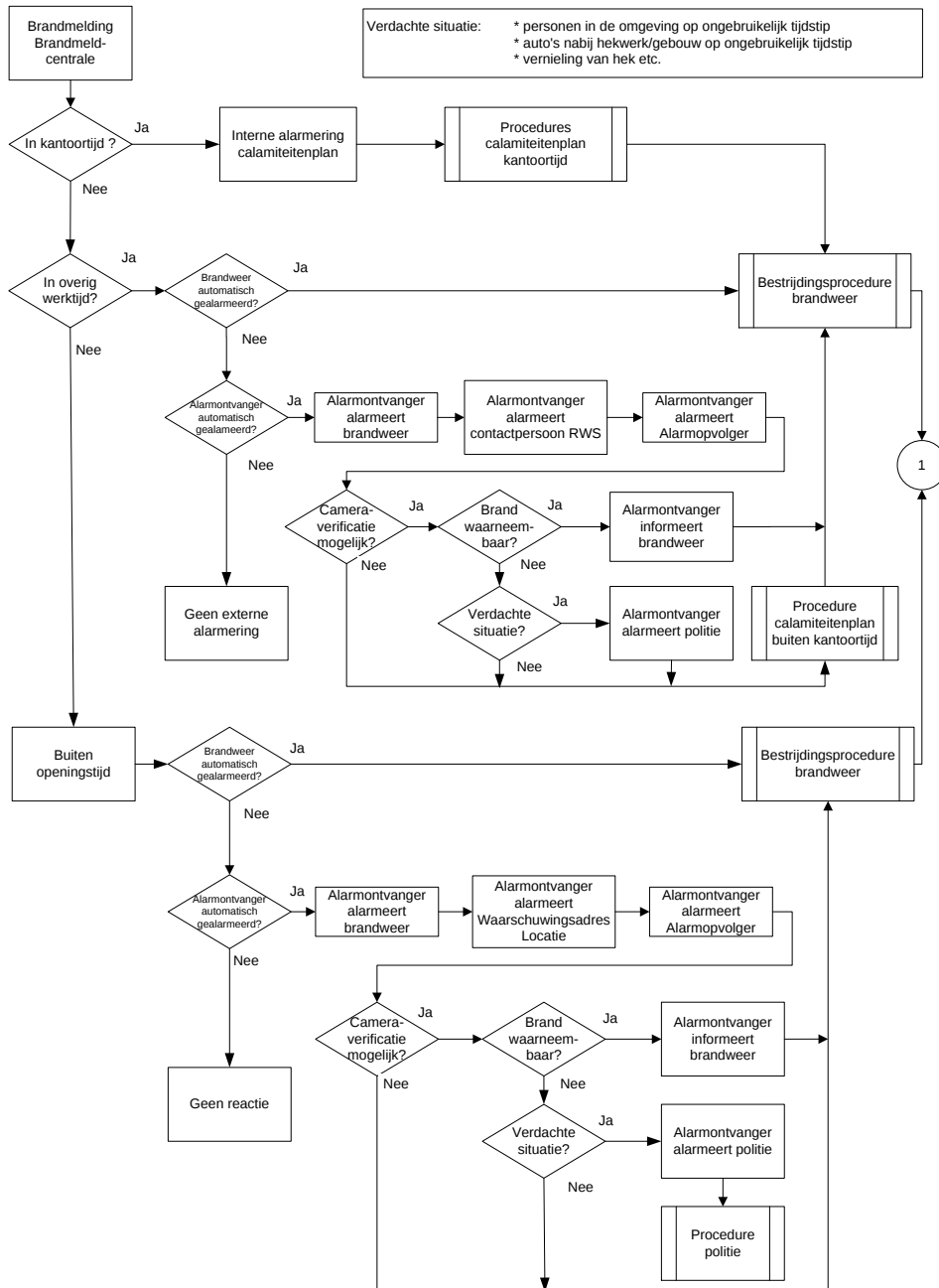


Procedure WIJZIGING BASISPROTOCOL Alarmontvanger

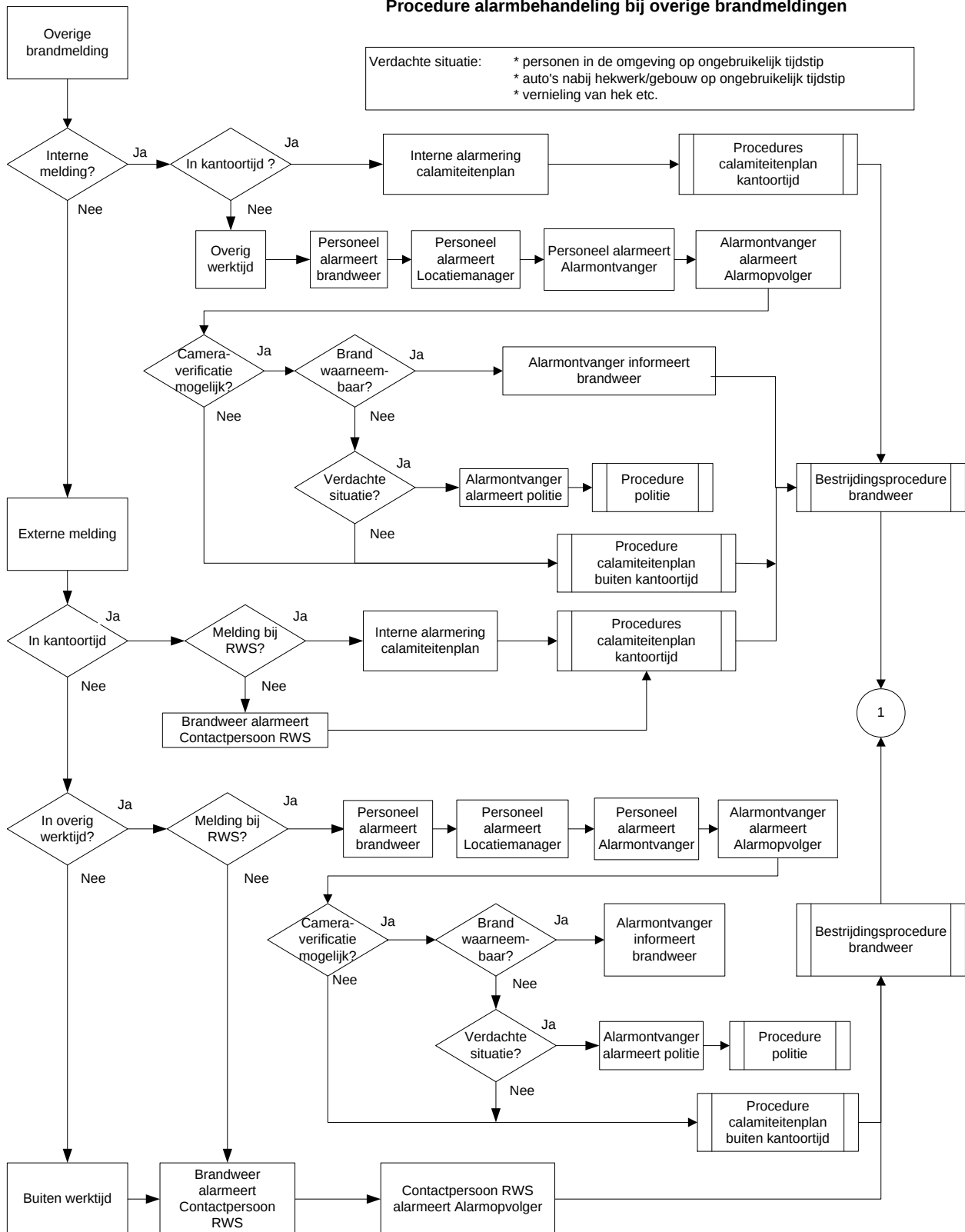
Afwijkend basisprotocol: Basisprotocol voor RWS-locatie met afwijkend beveiligingsniveau (bijv. bij alertering)



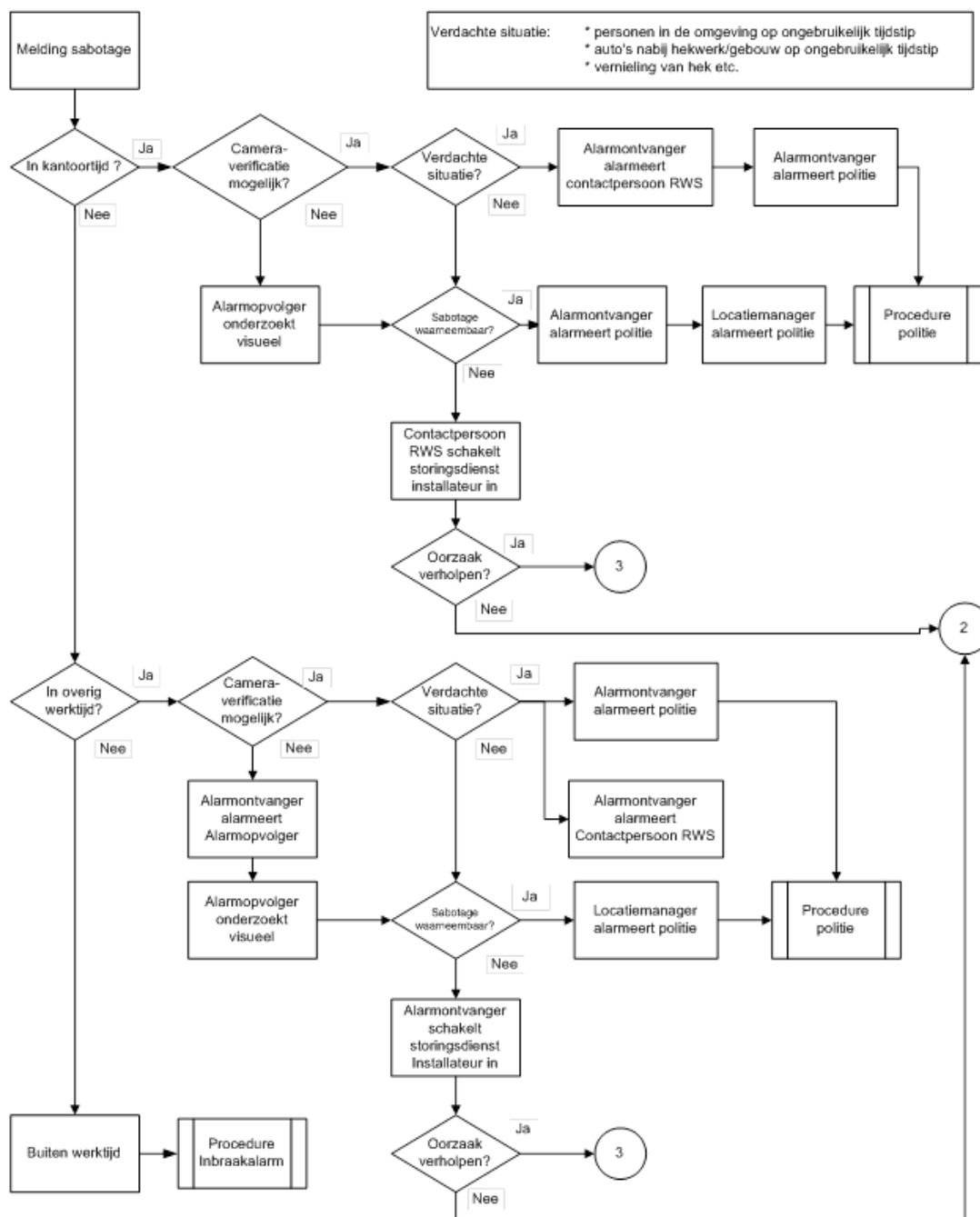
Procedure alarmbehandeling BRAND bij melding brandmeldcentrale



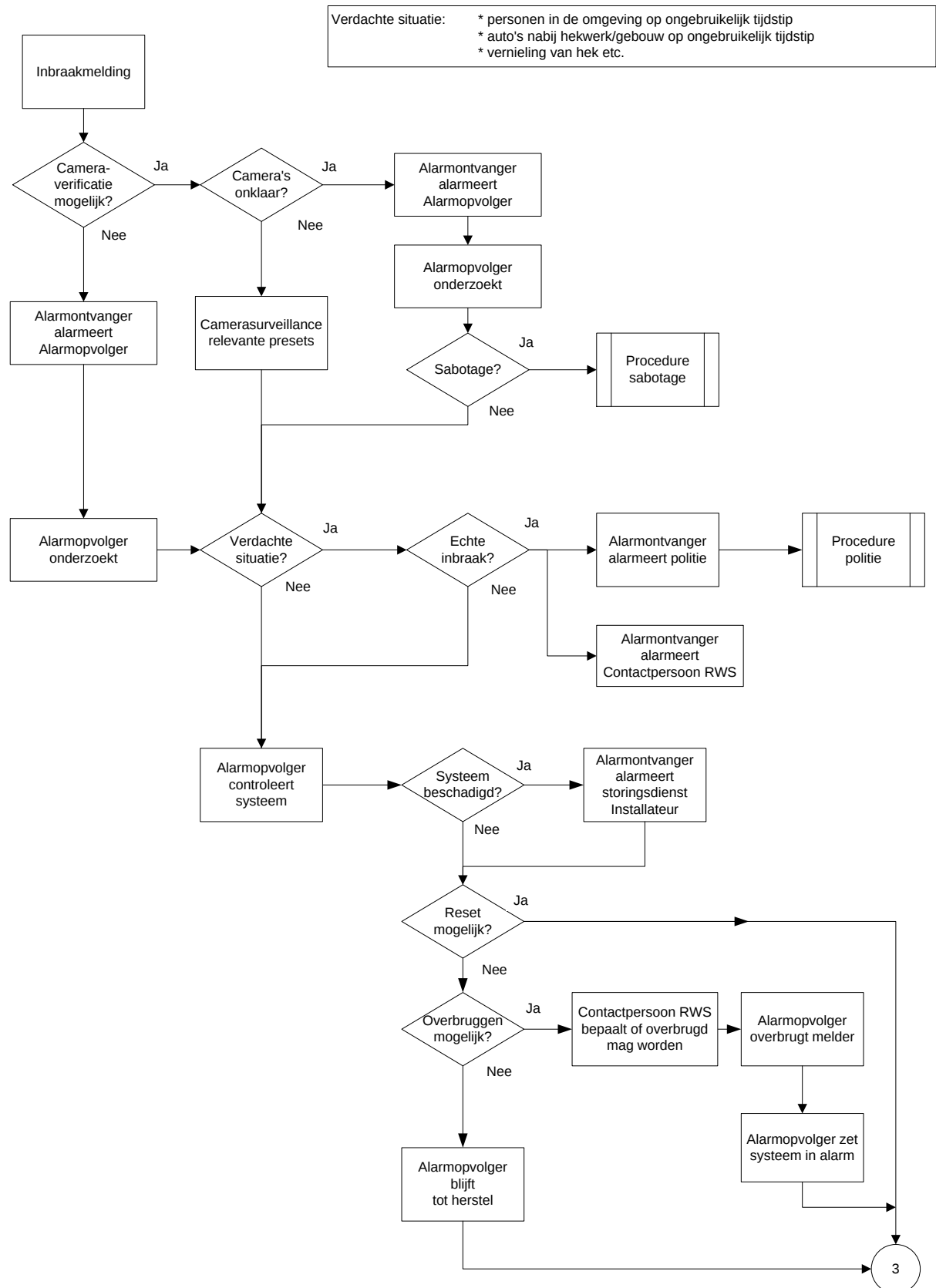
Procedure alarmbehandeling bij overige brandmeldingen



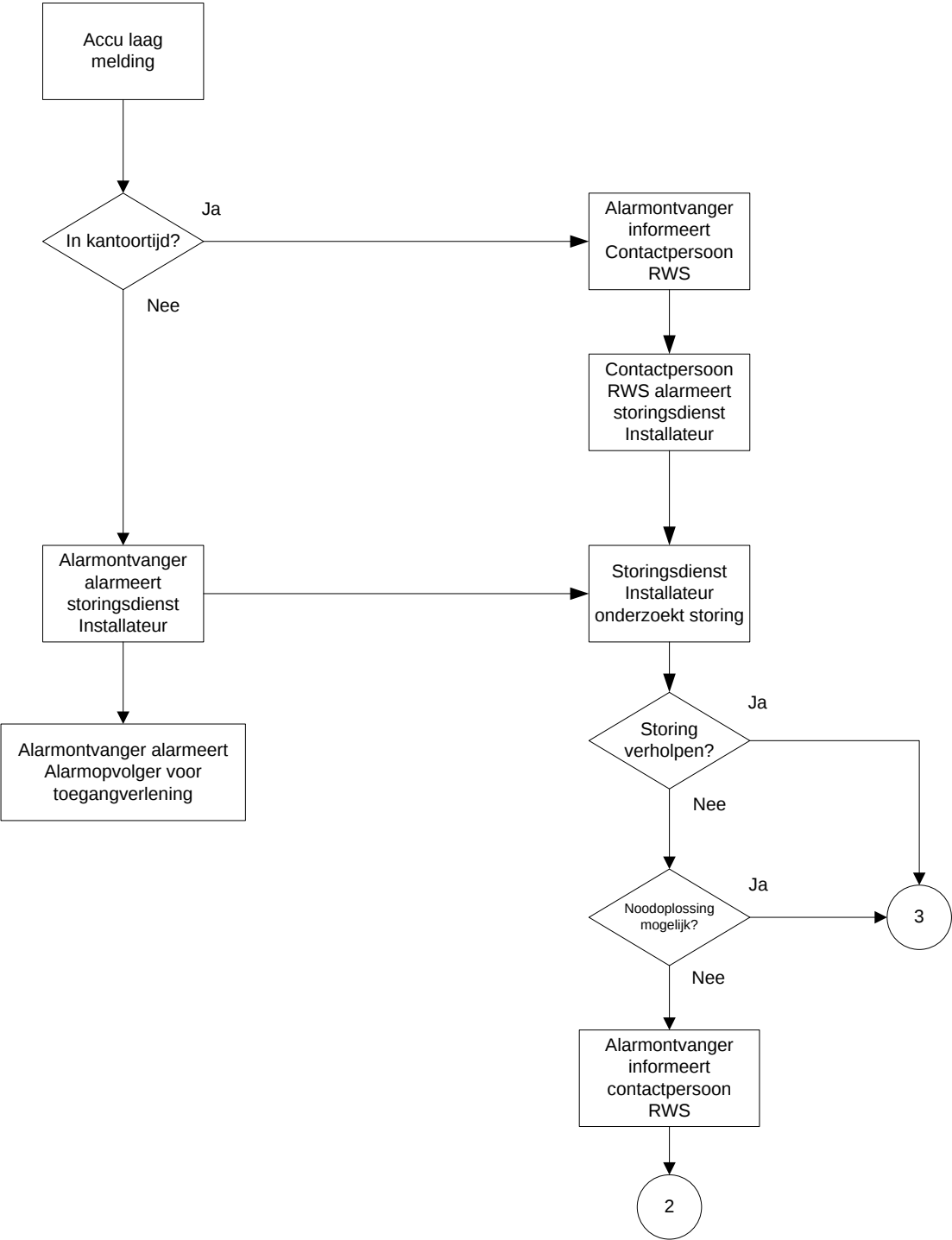
Procedure alarmbehandeling SABOTAGE security-installatie



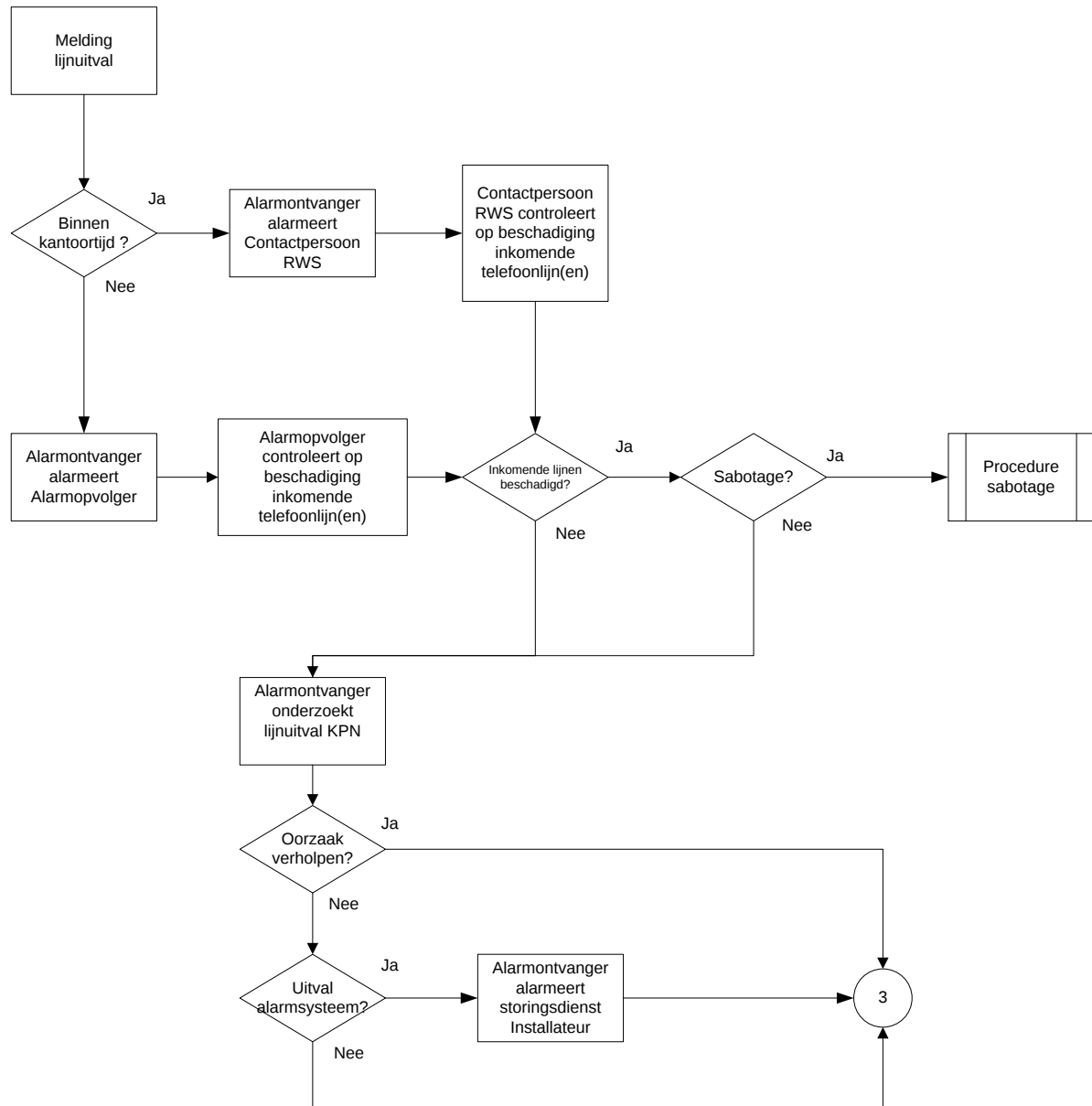
Procedure alarmafhandeling INBRAAK

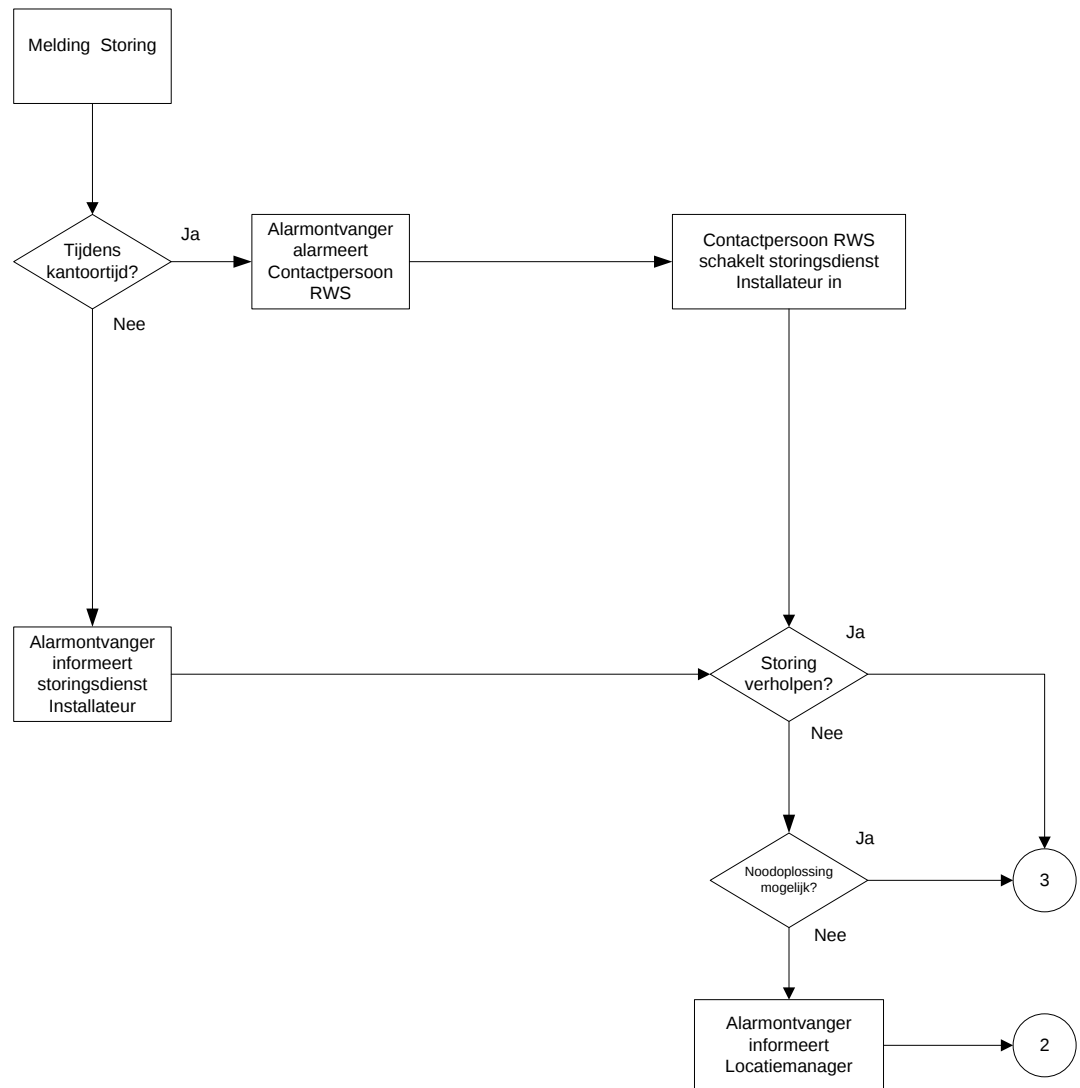


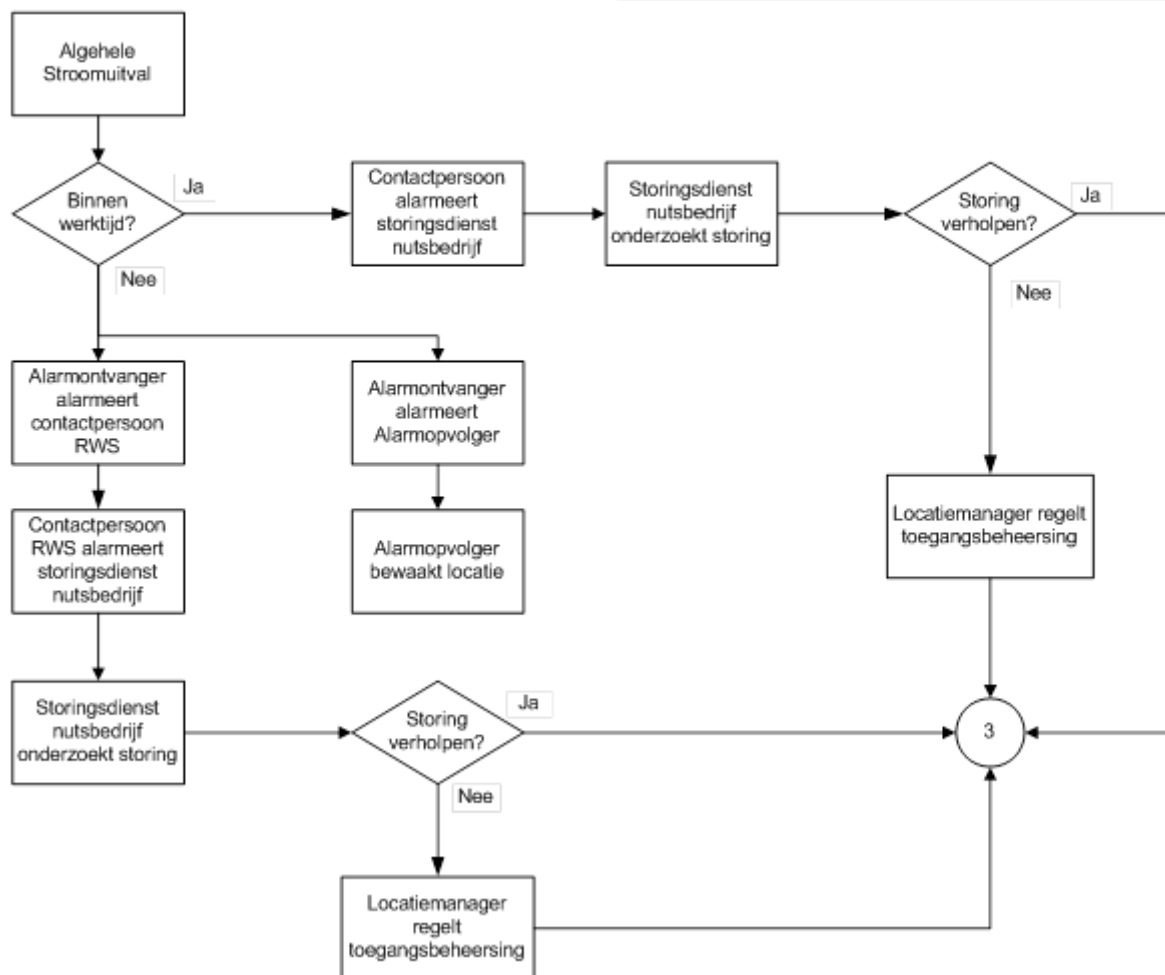
Procedure accu laag melding



Procedure melding lijnuitval





Procedure ALGEHELE STROOMUITVAL


Handboek Security

Nummer:	1364
Versie:	2.4
Status:	In beheer
Type:	Kader
Inhoudelijk beheerder:	Dirk-Jan Molenaar
Verantwoordelijke afdeling:	Afd. Advies Technisch Management
Netwerken:	Hoofdvaarwegennet, Hoofdwatersysteem, Hoofdwegennet
Rollen:	Technisch Manager
Fase:	Planuitwerking, Realisatie, Onderhoud
Proceseigenaar	Proceseigenaar Aanleg en Onderhoud