



Softwarebeheer en backup - restore

Procesbeschrijving voor IA-systemen

District:

Datum	12 november 2016
Status	Definitief
Classificatie	RWS Bedrijfsinformatie: RWS-I

Colofon

Uitgegeven door	RWS IMPAKT
Informatie	
Telefoon	
Fax	
Uitgevoerd door	Project IMPAKT
Opmaak	Rijkshuisstijl
Datum	12 november 2016
Status	Definitief
Versienummer	3.0
Bron	Generieke Procesbeschrijving Softwarebeheer en backup-restore v3.0

Versiebeheer

Versie	Datum	Wijzigingen
0.1	26-11-2014	Initiële opzet van de procesbeschrijving
0.2	21-01-2015	Commentaar op versie 0.1 verwerkt en deelproces Backup en restore opgenomen
0.3	06-02-2015	Aangepast aan template procesbeschrijving en commentaar op versie 0.1 verwerkt
0.4	08-02-2015	Review Koos van der Spek – VKA
0.5	23-02-2015	Aanpassingen procedures/opmaak/aanvullingen EvdZ
0.6	02-03-2015	Aanpassingen werkinstructies
0.7	05-03-2015	QC – Koos van der Spek – VKA
0.8	10-03-2015	Aanpassingen verwerkt n.a.v. QC
0.9	23-03-2015	Processchema's opgenomen
0.91	02-04-2015	Commentaar verwerkt van Ico Jacobs op versie 0.8
1.0	08-05-2015	Baseline versie vastgesteld door Arthur de Graaf TM
1.1	02-06-2015	Aanpassingen verwerkt n.a.v. review Otto Poley en Erwin van der Zwan o.b.v. review regio NN
1.2	16-11-2015	Verwerking commentaar i.h.k herziening beheerprocessen door Cleo van Engelen
1.2(KS)	28-11-2015	QC Koos van der Spek – VKA
2.0	30-11-2015	Definitieve versie na verwerking QC
2.1	02-12-2105	Aanpassingen lay-out
2.2	27-05-2016	Wijzigingen n.a.v. review RWS
2.3	26-08-2016	QC Koos van der Spek – VKA
2.4	01-09-2016	Ter acceptatie aangeboden aan RWS
3.0	12-11-2016	Definitief na acceptatie RWS

1 Inleiding

1.1 Algemeen

Dit document beschrijft het proces softwarebeheer voor de industriële automatisering van RWS en welke rollen en verantwoordelijkheden betrokkenen hebben. Tevens beschrijft dit document de activiteiten die ten behoeve van dit proces moeten worden uitgevoerd.

Softwarebeheer is het proces dat op gestructureerde wijze wijzigingen ten aanzien van (besturings-)software ontvangt en registreert, analyseert, toetst, plant, uitvoert en documenteert.

Uitgangspunten bij de beheerprocessen zijn:

- Bestaande praktijken en inbedding in bestaande structuren;
- Rolverdeling hanteren zoals die voorkomt uit het Ondernemingsplan 2015;
- Werken aan één RWS en samenwerking in de keten staat centraal.

1.2 Doel

Het doel van het proces softwarebeheer is:

- verhogen van de beschikbaarheid van het object;
- verhogen van de veiligheid van het object;
- verhogen van de efficiëntie van de werkzaamheden bij RWS;
- kwaliteitsborging bij wijzigingen;
- verhogen van de servicegraad aan de klant (door de ON);
- kostenbeheersing.

Het proces softwarebeheer zorgt ervoor dat de beschikbaarheid en integriteit van de IA-systemen kan worden gewaarborgd en dat er kwaliteitsborging is bij wijzigingen.

Uitsluitend geautoriseerde personen kunnen de software ter beschikking krijgen en wijzigen.

1.3 Bereik

Dit document richt zich op het softwarebeheer van industriële automatiseringssystemen (IA) van Rijkswaterstaat.

Met IA-systemen worden de geautomatiseerde systemen bedoeld die gebruikt worden voor het aansturen, meten en, eventueel op afstand, bedienen van fysieke installaties, objecten of technische apparatuur voor het openen of sluiten van bijvoorbeeld sluisen, bruggen, stuwen, spuien, vistrappen, slagbomen, enzovoort. Onder IA vallen logische technische componenten (zoals PLC's) maar ook SCADA (Supervisory Control and Data Acquisition) systemen¹. In dit document wordt verder over IA-systemen gesproken.

Het proces softwarebeheer omvat de programmatuur van de IA-systemen van een object en richt zich op de betrokken organisaties en afdelingen zoals de objecteigenaar, objectbeheerder en opdrachtnemer(s). Dit document beschrijft o.a. de bewaarfunctie en de uitgifte en inname van software.

Onder software worden alle logisch programmeerbare instructiesets verstaan welke aanwezig kunnen zijn op IA-systemen, waaronder; firmware, systeemsoftware,

¹ De termen "IA" en "SCADA systemen" worden vaak door elkaar gebruikt. Een PLC (Programmable Logic Controller) is ook een component van IA.

besturingssoftware, PLC-software, applicatiesoftware (SCADA), engineering software. Aanpassingen aan configuratie instellingen en parameters vallen hier ook onder.

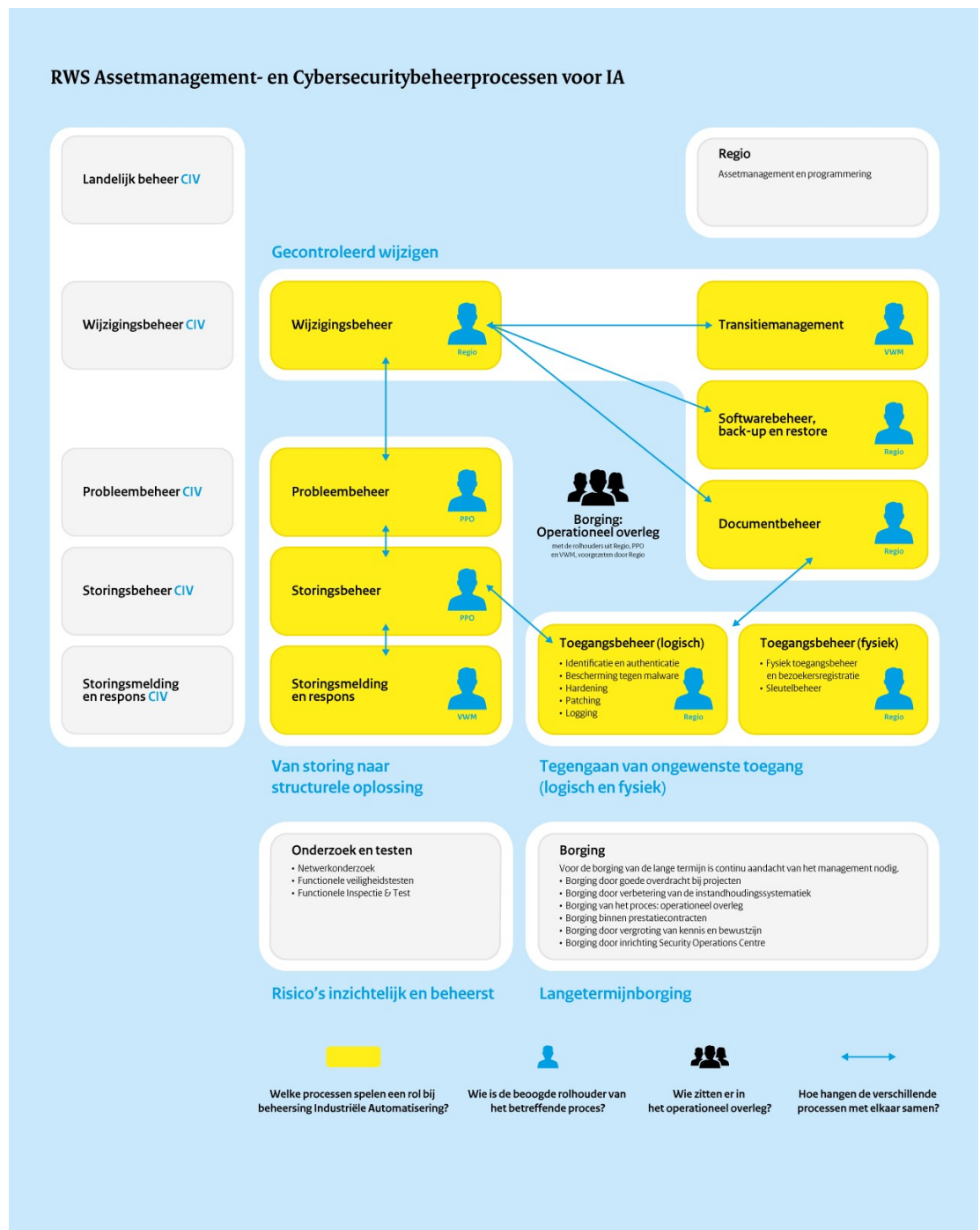
1.4 Raakvlakken met andere beheerprocessen

Het proces softwarebeheer maakt deel uit van het proces configuratiebeheer. Er is een directe relatie met wijzigingsbeheer en met de overige operationele cybersecurity processen.

In onderstaande figuur is een overzicht van de Asset Management (AM) en Cybersecurity (CS) processen voor IA (Industriële Automatisering) weergegeven.

De gele vlakken zijn beheerprocessen, de richting van de pijlen geeft de informatiestroom weer en dus ook de onderlinge relatie. De grijze vlakken geven de beheerprocessen weer van de CIV voor het beheer van eventuele onderliggende netwerken en aanverwante Missie Kritieke Systemen (MKS), zoals IVS90 en Digitaal Journaal. Indien uit de beheerprocessen blijkt dat er aanvullende middelen nodig zijn dan worden deze conform het reguliere assetmanagement aangevraagd. Zie het grijze vlak 'Assetmanagement en programmering' rechtsboven in de figuur.

Wijzigingen aan de software, die volgen vanuit het proces wijzigingsbeheer, dienen gedocumenteerd en opgeslagen te worden via het proces softwarebeheer. Het proces voorziet tevens in de inname (backup) en uitgifte van software.



Figuur 1: RWS AM en CS beheerprocessen en onderlinge relaties voor IA

1.5 Leeswijzer

- Hoofdstuk 2: Organisatorische aspecten en verantwoordelijkheden
- Hoofdstuk 3: Werkinstructies
- Bijlage A: Lijst met begrippen en afkortingen
- Bijlage B: Softwarebeheer en documentatie
- Bijlage C: Regio/Object specifieke details
- Bijlage D: Overzicht uitgangspunten en beleidsbepalingen

1.6 Bronnen

De algemene beleidsbepalingen ten aanzien van informatiebeveiliging zijn opgenomen in de *Baseline Informatiebeveiliging Rijkswaterstaat (BIR), v1.01, 11 november 2013*.

Aanvullende bepalingen zijn opgenomen in de *Cybersecurity Implementatierichtlijn Objecten - RWS versie 1.01 d.d. 02 december 2013*.

2 Organisatie

2.1 Algemeen

Het is de wens van RWS dat de Regio zelf de software (backups) beheert, of dit door een gespecialiseerde partij laat uitvoeren. Indien er wijzigingen aan de software van een IA systeem van een object plaatsvinden dan vraagt de opdrachtnemer de software op bij de Regio. Deze stelt de software beschikbaar aan de opdrachtnemer. Na afloop van de werkzaamheden wordt een backup van de nieuwe software door de opdrachtnemer opgeleverd aan de (softwarebeheerder van de) Regio. De Regio blijft eindverantwoordelijk voor de software.

2.2 Functies, rollen en verantwoordelijkheden

De (gegevens)beheerder (configuratiemanager) is verantwoordelijk voor het gegevens- en software beheer bij de Regio. De verantwoordelijke beheerder is verantwoording verschuldigd aan objectbeheerder.

De volgende directe rollen komen voor in dit proces:

Rol	Beschrijving	Functie/Persoon
Objectbeheerder	Eigenaar van de objecten waarvoor softwarebeheer benodigd is.	Districtshoofd
Rolhouder	Persoon die verantwoordelijk is voor het proces softwarebeheer.	Asset Manager
Software beheerder	1 ^{ste} verantwoordelijke voor het softwarebeheer. Legt de configuratie van alle in gebruik zijnde IA-componenten vast en houdt dit actueel.	Medewerker Informatie Voorziening (MIV'er)
IA Adviseur	Geeft advies over voorgestelde of noodzakelijk softwarewijzigingen	IA Adviseur (Regio)
Aanvrager (kan ON zijn)	Organisatieonderdeel van RWS (bv PPO) of externe organisatie (bv ON) die een verzoek indient om uitgifte van software met bijbehorende documentatie.	District/PPO/ON

Indirecte rollen		
Rol	Beschrijving	Functie/Persoon
Technisch Manager	Verantwoordelijk voor de (inhoudelijke) afspraken met de ON in geval van wijzigingen in de software.	Technisch Manager (PPO)
Opdrachtnemer (ON)	Externe partij die het beheer van de IA systemen uitvoert	

2.3

RACI

In onderstaande RACI-matrix is een voorbeeld gegeven van de activiteiten die onder andere in hoofdstuk 3 staan aangegeven. Hierbij is aangegeven welke rollen welke verantwoordelijkheden hebben. Daartoe zijn per activiteit letters aan rollen toegekend. Zie voor de betekenis van elke letter de legenda onder de matrix.

	Objectbeheerder	Softwarebeheerder (MIV-er)	Rollhouder proces (Asset Manager)	IA Adviseur	Technisch Manager	Opdrachtnemer
Procedure softwarebeheer						
3.1 Identificatie en authenticatie	A	R	I	CI	CI	CI
3.2 Uitgifte software	A	R	I	CI	CI	CI
3.3, 3.4, 3.5, 3.6 Inname software (huidig en nieuw object)	A	R	I	CI	CI	CI
3.7 Bewaking datums	A	R	I	I	I	I
3.8 Opheffen (component van een) object	A	I	R	CI	CI	CI
3.9 (Her-)inventarisatie software	A	CI	CI	CI	I	R
3.10 Backup van de software	A	I	I	CI	I	R
3.11 Restore van de software	A	I	I	CI	I	R
3.12 Kluisprocedure	A	I	R	CI	CI	I
3.13 Kwaliteit software en documentatie	A	I	CI	CI	CI	R

Legenda:

- R = Responsible:
Degene (rol) die de activiteit uitvoert.
Deze letter dient bij elke activiteit aan 1 rol te worden toegekend.
- A = Accountable:
Degene (rol) aan wie door de verantwoordelijke (R) verantwoording wordt afgelegd.
Deze letter dient bij elke activiteit aan 1 rol te worden toegekend.
- C = Consulted:
Degene (rol) die een bijdrage kan leveren in het beoogde resultaat van de activiteit.
Deze letter kan aan meerdere rollen worden toegekend.
- I = Informed:
Degene (rol) die geïnformeerd wordt.
Deze letter kan aan meerdere rollen worden toegekend.

3 Werkinstructies

Dit hoofdstuk geeft op hoofdlijnen weer hoe de meest voorkomende beheerprocessen t.a.v. software bij IA-systemen dienen te verlopen. Het proces softwarebeheer bestaat uit de volgende procedures:

1. Identificatie en autorisatie;
2. Uitgifte software;
3. Inname software;
4. Gewijzigde software delen;
5. Inname nieuw object;
6. Verlenging online uitgifte;
7. Bewaking datums;
8. Opheffen van een object;
9. (Her-)inventarisatie software;
10. Backup van software;
11. Restore van software;
12. Kluisprocedure.
13. Kwaliteit software en documentatie

Specifieke details hoe e.e.a. dient te verlopen bij de Opdrachtnemer, zijn de verantwoordelijkheid van de Opdrachtnemer en worden hier niet verder beschreven.

3.1 Identificatie en autorisatie

Deze procedure beschrijft de wijze waarop een opdrachtnemer (en ook een leverancier/fabrikant van een systeem) door Rijkswaterstaat geautoriseerd kan worden om industriële software te kunnen verkrijgen en te gebruiken.

Criteria om een opdrachtnemer te autoriseren zijn meestal het verkrijgen van een (onderhouds) contract waarin ook het wijzigingen van software is opgenomen. Dit kan ook voor onderaannemers gelden. De toegekende autorisatie is per persoon geldig. Opdrachtnemers kunnen niet zelfstandig onderaannemers autoriseren.

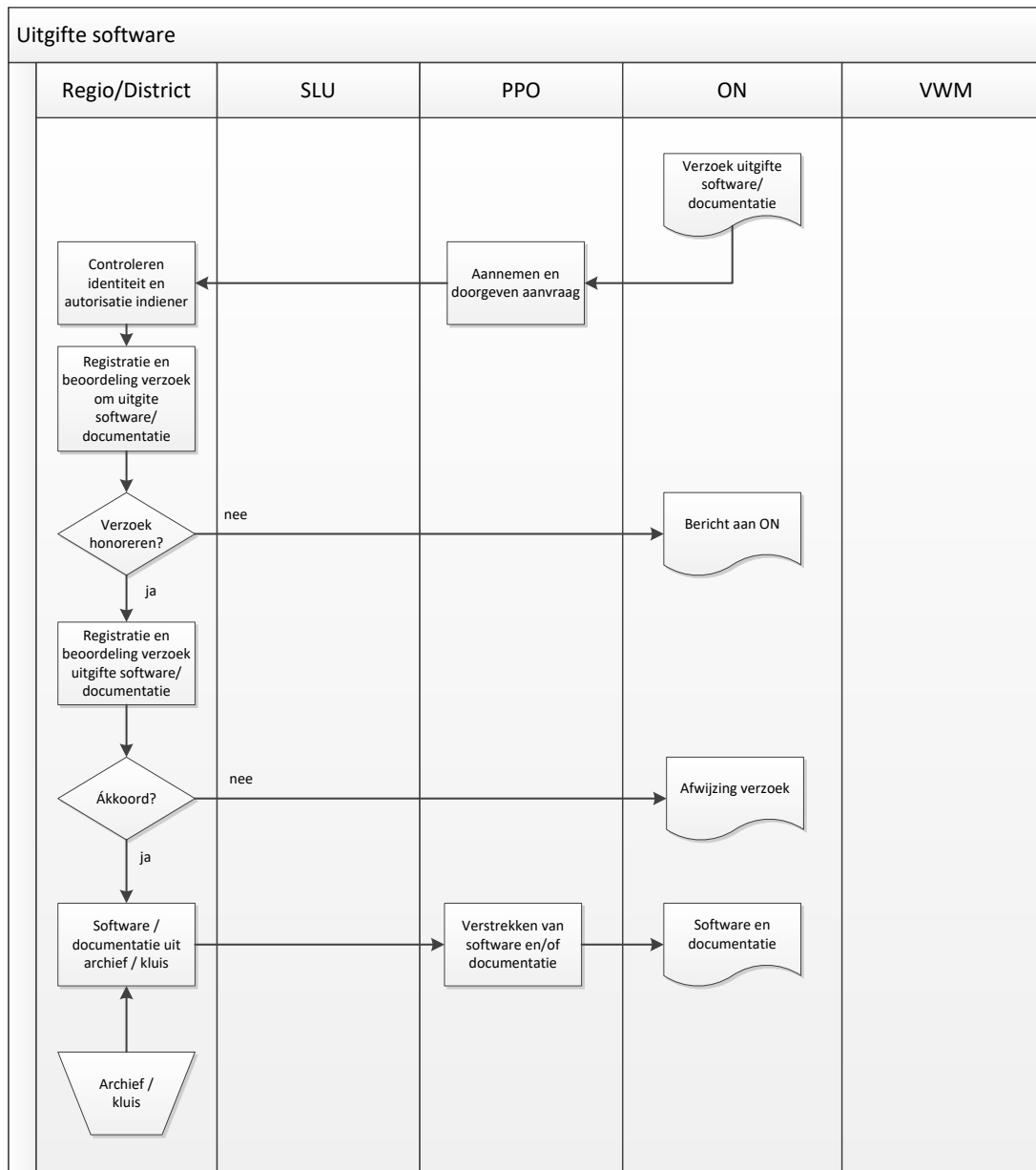
De volgende activiteiten worden bij deze procedure uitgevoerd door de softwarebeheerder:

1. Controleer de inhoud van het ontvangen formulier en gegevens van de indiener.
2. Informeer de indiener over gehonoreerd of afgewezen verzoek.
3. Stuur, bij ontbrekende informatie, een verzoek naar de indiener om aanvullende informatie.
4. Actualiseer de autorisatietabel van geautoriseerde personen voor indienen verzoek.

In onderstaande tabel zijn de geautoriseerde organisaties en functionarissen weergegeven.

Geautoriseerde ON/ fabrikant/leverancier	Geautoriseerde personen

3.2 Uitgifte software



Deze procedure beschrijft de werkwijze waarop de reguliere uitgifte van software aan een opdrachtnemer plaatsvindt.

Er worden 3 verschillende uitgiftes onderscheiden:

- Ter informatie: De verstrekte versie van de Industriële Software is enkel informatief. Modificaties zullen niet worden geaccepteerd en zullen niet worden ingenomen.
- Offline modificatie: Deze versie van de Industriële Software geldt vanaf het moment van lenen tot het moment van terugbrengen of tot het verlopen van de uitleentermijn niet als de leidende versie. Er kunnen wijzigingen door derden aan dezelfde versie van de software worden aangebracht. Deze wijze van uitgifte wordt uitsluitend gedaan als er een (spoed)reparatie nodig is en de software op dat moment al is uitgeleend. Na de reparatie dient de oplossing alsnog in de 'online' versie te worden ondergebracht inclusief bijbehorende testen etc. Deze werkwijze heeft daarom niet de voorkeur: er dient zoveel mogelijk gebruik te worden gemaakt van de 'online' modificatie.
- 'Online' modificatie: Deze versie geldt vanaf het moment van uitgifte tot het moment van terugbrengen of tot het verlopen van de uitleentermijn als de leidende versie. Anderen kunnen niet gelijktijdig deze versie van de software aanpassen. Alleen bij calamiteiten kan de software worden aangepast door een derde. De uitleentermijn is maximaal 1 maand.

N.B: De term 'online' kan soms verwarring oproepen. Het betreft niet een 'online' aanpassing van de software maar het aanpassen van de originele software zodat er weer een nieuwe versie ontstaat. In de praktijk zal een kopie van de actuele en meest recente versie van de originele software beschikbaar worden gesteld. Na aanpassing en testen etc wordt deze via het proces wijzigingsbeheer weer ingediend en geldt vanaf dat moment als nieuwe 'originele' versie van de software.

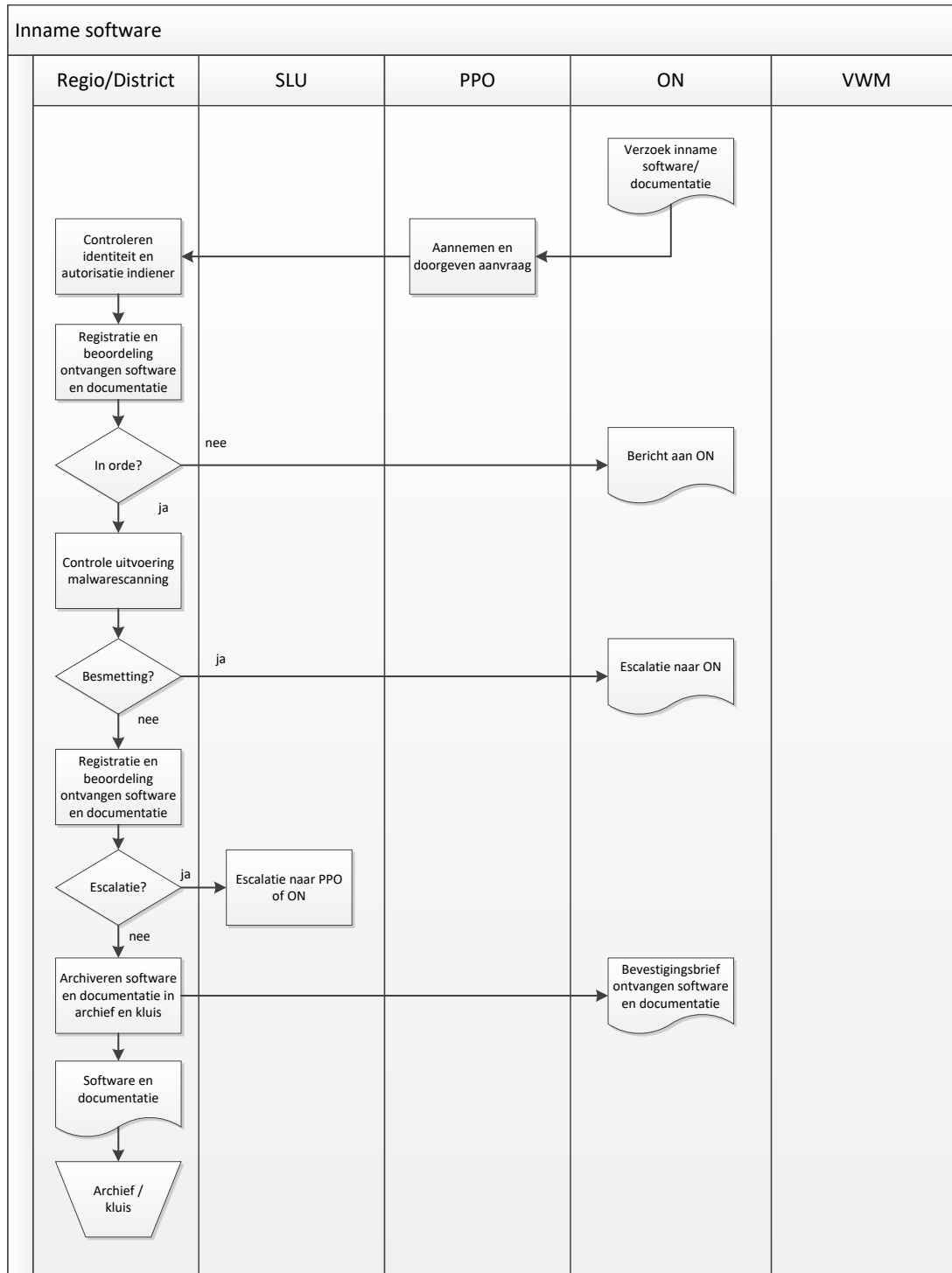
De volgende activiteiten worden bij deze procedure uitgevoerd door de softwarebeheerder:

1. Controleer de autorisatie en identificatie van de indiener van het verzoek voor uitgifte software.
2. Registreer en beoordeel het verzoek voor beschikbaar stellen software, inclusief bijbehorende documentatie.
3. Registreer beschikbaar gestelde software.

PPO voert de volgende activiteiten uit:

1. Neemt de aanvraag in ontvangst en stuurt deze door naar de regio om in behandeling te worden genomen.
2. Als de aanvraag door de regio is gehonoreerd, stuurt PPO de software en/of documentatie door naar de opdrachtnemer.

3.3 Inname software



Deze procedure beschrijft de werkwijze waarop de gewijzigde software weer wordt ingenomen. Hiertoe behoort ook de bijbehorende documentatie, testprotocollen en een bewijs van acceptatie door de projectleider van het project (waarbij de software is gewijzigd). Het project is verantwoordelijk voor de goede werking van de software.

De volgende activiteiten worden bij deze procedure uitgevoerd door PPO:

- Ontvang het verzoek om software in te leveren en stuur deze door naar de regio voor verdere afhandeling

De volgende activiteiten worden bij deze procedure uitgevoerd door de softwarebeheerder:

1. Controleer de identiteit en de autorisatie van de indiener van het verzoek voor inleveren van software.
2. Registreer en beoordeel het verzoek voor het inleveren van software en bijbehorende documentatie.
3. Registreer de metadata van de gewijzigde software en bijbehorende documentatieset.
4. Beoordeel versienummer, datum en of de software aanpassingen/update conform een wijzigingsprocedure is uitgevoerd en een SAT heeft plaatsgevonden.
5. Beoordeel vormvereisten van ontvangen software en bijbehorende documentatie en stuur bericht als hier niet aan is voldaan.
6. Voer controle op malware uit op de gegevensdrager met software.
7. Informeer, bij gesignaleerde besmetting op gegevensdrager en/of de software, de objectbeheerder direct en neem actie naar de leverancier (ON) van de software.
8. Registreer bevindingen malwarescan in beheersysteem.
9. Registreer geaccepteerde nieuwe software en bijbehorende documentatie en verstuur een innamebrief als bewijs van inname.
10. Archiveer nieuwe software en bijbehorende documentatie in kluis c.q. archief en eventueel ook digitaal in een systeem.

De volgende activiteiten worden bij deze procedure uitgevoerd door SLU:

- Als er op verzoek van de regio escalatie noodzakelijk is naar aanleiding van de ontvangen software en/of bijbehorende documentatie, dan zal de SLU hierbij een actieve rol vervullen.

3.4 Gewijzigde software delen

Uitgeleende software komt slechts eenmalig voor. Software wordt alleen weer ingenomen van de 1^{ste} partij aan wie deze is uitgeleend in het kader van het aanbrengen van wijzigingen. Er wordt geen software teruggenomen van anderen dan de organisatie aan wie is uitgeleend. Er is daarom geen procedure om andere partijen te informeren over een eventuele nieuwe versie van de software noodzakelijk.

3.5 Inname nieuw object

Bij een nieuw object of na een grote renovatie wordt - voor ingebruikname - de software in het softwarebeheer opgenomen.

De softwarebeheerder volgt de normale controles en innameprocedure. Bij goedkeuring van de documentatie en software wordt een innamebrief opgesteld als bewijs van ontvangst. Hiervan wordt een registratie bijgehouden en wordt de software en de bijbehorende documentatie in de kluis opgeborgen en (waar van toepassing) in een digitaal archief gearchiveerd.

3.6 Verlenging online uitgifte

Deze procedure beschrijft de werkwijze waarop verlenging aangevraagd kan worden voor 'online' uitgegeven software als die langer dan 1 maand uitgeleend is.

Er wordt een controle gedaan op ontvangen verzoeken voor uitgifte van de software zodat de volgorde hiervan kan worden bepaald voor de uitgifte.

Van de ontvangen en goedgekeurde software en bijbehorende documentatie, wordt een innamebrief opgesteld als bewijs van inname.

De volgende activiteit wordt bij deze procedure uitgevoerd door de aanvrager:

1. Dien verzoek in om verlenging van de 'online' uitgegeven software.

De volgende activiteiten worden bij deze procedure uitgevoerd door de softwarebeheerder:

2. Controleer of er een wachtrij is van ontvangen verzoeken voor uitgifte van dezelfde software.
3. Bepaal de volgorde van de ingediende verzoeken als er een wachtrij is.
4. Informeer de aanvragers over de volgorde, de aanpak en de planning van de ontvangen verzoeken.
5. Controleer de ontvangen nieuwe versie van de software en de documentatie op vormvereisten, volledigheid en malware.
6. Informeer opdrachtnemer bij ontbrekende software of bij gesignaleerde besmetting op gegevensdrager en/of op de software.
7. Registreer de bevindingen van de malwarescan in het beheersysteem.
8. Verstuur een afwijzing naar de indiener als niet is voldaan aan de vormvereisten en/of volledigheid of als malware is ontdekt en maak een nieuwe afspraak.
9. Stel een innamebrief op bij geaccepteerde software en bijbehorende documentatie als bewijs van inname.
10. Registreer de geaccepteerde software en documentatie in het beheersysteem.
11. Informeer de aanvrager over de toegekende verlenging met 1 maand en registreer dit in het beheersysteem.
12. Archiveer de nieuwe versie van de software en bijbehorende documentatie in de kluis en het archief.

3.7 Bewaking datums

Deze procedure beschrijft de werkwijze waarop de data van uitgiftes beheerd worden.

Kort voor aanvang van de einddatum verstuurt de softwarebeheerder een herinnering waarin wordt aangegeven dat voor de einddatum de software en bijbehorende documentatie moet zijn ingeleverd of dat een verzoek om verlenging moet worden ingediend.

De volgende activiteiten worden bij deze procedure uitgevoerd door de softwarebeheerder:

1. Registreer de datum van de herinnering in een administratie één week voor de formele einddatum van een inname.
2. Verzend een herinneringsbericht naar de aanvrager dat de einddatum over 1 week eindigt en dat de software dan moet zijn ingediend of dat een verlenging moet worden aangevraagd.
3. Informeer de opdrachtgever/objectbeheerder bij het overschrijden van de einddatum die vervolgens contact opneemt met de aanvrager.
4. Escaleer het contact met de aanvrager door de projectleider als een reactie of een actie uitblijft op het voorgaande bericht aan aanvrager.

3.8 Opheffen (component) van een object

Wanneer een object geheel of gedeeltelijk wordt opgeheven of afgestoten, wordt dit vastgelegd in de registraties en wordt alle software en documentatie gearchiveerd. Dit proces zal via de Asset Manager verlopen. De aanvrager/initiatiefnemer komt via het Districtshoofd bij de Asset Manager en hij geeft dat weer door aan de softwarebeheerder/MIV-er.

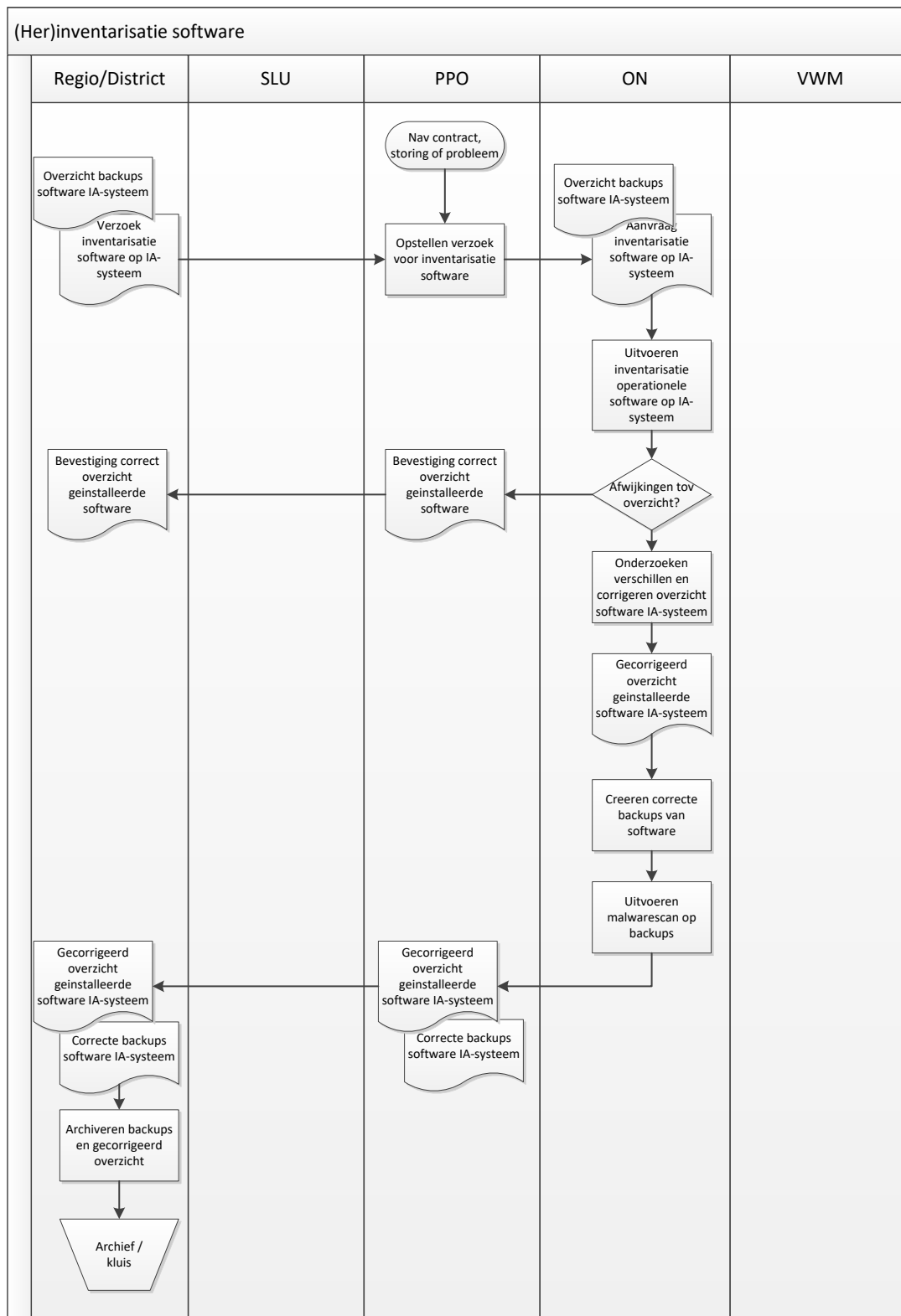
De volgende activiteit wordt bij deze procedure uitgevoerd door de aanvrager:

1. Dien verzoek in voor het opheffen van een object.

De volgende activiteiten worden bij deze procedure uitgevoerd door de softwarebeheerder, nadat tot opheffing van het object is besloten:

1. Controleer de autorisatie en identificatie van de organisatie en de indiener.
2. Registreer de opheffing van het object in de registraties en beheersystemen.
3. Breng de software en de bijbehorende documentatie over naar het archief.

3.9 (her-)inventarisatie software



Deze procedure beschrijft de wijze waarop de (her) inventarisatie en verificatie plaatsvindt van de backup- en systeemgegevens.

Deze procedure start met het verstrekken van een opdracht voor het uitvoeren van een inventarisatie van de geïnstalleerde software van (componenten) van het object. Het resultaat is een inventarisatielijst van geïnstalleerde software die wordt vergeleken met de informatie zoals geregistreerd in administraties of beheersystemen.

Indien van toepassing wordt een verschillenlijst opgesteld die aan de objectbeheerder wordt aangeboden om de oorzaken van de verschillen in softwareversies te verklaren en de objectbeheerder te voorzien van een actuele backup van de betreffende software.

De volgende activiteiten worden bij deze procedure uitgevoerd of gecoördineerd door de softwarebeheerder na afstemming met de projectmanager PPO:

1. Verstrek de opdracht voor het uitvoeren van een (her-)inventarisatie van de software.
2. Stel de lijst met backup gegevens op met de specificaties van ieder object en stel deze beschikbaar aan de uitvoerende organisatie.
3. Controleer en actualiseer de lijst met de geïnstalleerde software.
4. Meldt de uitgevoerde controle af als de lijst volledig overeenkomt met de geïnstalleerde software.
5. Corrigeer de lijst met de juiste backup- en systeemgegevens en stel een rapport op met de afwijkingen.
6. Verstuur de gecorrigeerde lijst met het rapport naar de objectbeheerder voor verder onderzoek naar de verschillen.
7. Verzoek de veroorzaker om een correcte backup van de software door middel van de procedure uitgifte en inname regulier.
8. Voer een controle uit op de gegevensdrager met de backup van de software op malware.
9. Informeer objectbeheerder bij gesignaleerde besmetting op gegevensdrager en/of op de software en onderneem actie naar de leverancier (ON) van de software.
10. Registreer de bevindingen van de malwarescan in het beheersysteem.
11. Verstrek actuele backup- en systeemgegevens.

3.10 Backup van software

De softwarebeheerder houdt een overzicht bij van alle systemen, de software versies, de aanwezige backups en de data waarop die backups gemaakt zijn.

Op het medium dient een duidelijke vermelding aanwezig te zijn van de volgende gegevens:

- Van welk systeem of component de back-up is gemaakt;
- Versie nummer;
- Datum waarop de back-up gemaakt is;
- Indien het medium een onderdeel is van meerdere media (zoals meerdere Cd's/Dvd's, USB-sticks) dan dient een volgnummer aanwezig te zijn waaruit blijkt welk nummer uit hoeveel het betreft (1 van 2 etc.)
- Lijst van aanwezige software met hun bron, datum, versie en controlewaarden.

Er dient door de Opdrachtnemer (ON) en de software beheerder een actuele registratie gevoerd te worden van alle software en de door ON gemaakte backups.

Iedere backup krijgt een datum en een volgnummer mee die gehanteerd kan worden bij de restore procedure. Deze registratie wordt onmiddellijk bijgewerkt en moet direct ter beschikking worden gesteld aan de IA-coördinator.

De integriteit en beschikbaarheid van de laatste drie versies van de PLC/SCADA systemen, programmatuur en besturingssystemen dient gewaarborgd te worden door het maken en testen van systeemimages/backups, conform een geborgde procedure:

- systeemimages/backups worden gemaakt na iedere (functionele) systeemwijziging.
- Wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd;
- Van iedere ontvangen gegevensdrager meteen backup van software wordt een malwarescan uitgevoerd op de gegevensdrager en op de software.
- Deze backups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als een calamiteit zich voordoet op de locatie waar het systeem zich bevindt;
- Er worden twee backups op geografisch gescheiden locaties bewaard;
- Backups en de ruimte waarin ze zijn opgeslagen behoren fysiek goed te worden beschermd volgens dezelfde normen die gelden voor de hoofdlocatie en zijn alleen toegankelijk voor bevoegden;
- Backups worden bewaard tot het moment van uitdienstname van betreffend systeem.

Van alle software dat op een werkstation, OS(windows, Linux etc.) draait moet een complete PC image gemaakt worden in combinatie met een back-up van het project zelf en een back-up van de ontwikkel software.

Van alle PLC's moet een download gemaakt worden van de daadwerkelijke actieve software evenals de source code. Bestaat er voor de PLC een vast ontwikkelstation dan moet hier ook een back-up van worden gemaakt.

In verband met mogelijk opnieuw inrichten van de systemen dient van alle ontwikkel- en back-up tools de installatie-software beschikbaar zijn. Er dient een sluitende registratie van de gebruikte licenties beschikbaar te zijn.

Van alle "overige" systemen dienen de configuratiebestanden beschikbaar te zijn, die teruggezet kunnen worden zonder alle systeeminstellingen opnieuw te hoeven configureren.

Een volledig overzicht van alle configuratie instellingen dient beschikbaar te zijn.

Alle configuratiewijzigingen dienen geregistreerd te worden.

Na iedere configuratie wijziging dient een back-up gemaakt te worden en een malwarescan te worden uitgevoerd.

De softwarebeheerder dient backups te maken van:

Systeem software

- OS Image
- Source code project
- Runtime code project
- Ontwikkel en backup tools (installatie Cd's)
- OS installatie CD
- Back-up / restore werkbeschrijving
- Licenties
- Functionele beschrijving

Apparatuur software

- Ontwikkel software
- Applicatie software
- Back-up / restore werkbeschrijving
- Functionele beschrijving

Fabriekssoftware

- Configuratie bestand / Parameters
- Back-up software
- Back-up / restore werkbeschrijving
- Functionele beschrijving

Voor elk type software wordt een afzonderlijke set van backups verwacht.

Er dient bij het maken van backups rekening te worden gehouden dat er backups worden gemaakt van alle IA-systemen waarin zich software kan bevinden zoals SCADA werkstations, Engineering Stations, PLC's, frequentieregelaars, toerenbewaking, scanners en gelijklooptregelingen.

Backups dienen altijd op minimaal twee locaties in een kluis aanwezig te zijn. Die kluis mag zich echter nooit in de technische (computer) ruimte bevinden.

NB: Gegevensdragers zoals USB sticks of externe harddisk met software van RWS IA-systemen mogen niet gebruikt worden voor andere doeleinden of het opslaan van informatie of gegevens van andere (niet-RWS) omgevingen. Voor aanvang van een kopieeractie van software op een gegevensdrager moet een malwarescan worden uitgevoerd met actuele beveiligingssoftware.

Daarnaast dient een kopie van de software op een geografisch gescheiden locatie opgeslagen te worden.

De ON mag een derde kopie voor direct gebruik in zijn bezit hebben. Alle kopieën moeten in de genoemde registratie zijn geregistreerd.

De backup wordt door de ON gemaakt en beschikbaar gesteld aan de softwarebeheerder van RWS. Hierbij moet een software opleverlijst worden meegeleverd.

3.11 Restore van software

Het terugzetten van een back-up kan op verschillende manieren gebeuren. Het kan gaan om het vervangen (terugzetten) van de volledige set met software die op een systeem geïnstalleerd is. Het kan gaan om het terugzetten van individuele bestanden of het terugzetten van alle bestanden die in een bepaalde periode werden aangemaakt.

Herstelprocedures moeten jaarlijks of tweejaarlijks worden gecontroleerd en getest, om te waarborgen dat ze doeltreffend zijn, dat ze werken en dat ze kunnen worden uitgevoerd binnen de daarvoor overeengekomen tijd.

Jaarlijks wordt een recovery test gedaan om te zien of de media nog leesbaar is.

Herstelprocedures zijn onderdeel van de disaster recovery planning. Voor de testomgeving geldt dat ook daarvan na iedere wijziging een backup gemaakt dient te worden. Voorkomen moet worden dat die backups dagelijks op hetzelfde medium worden gemaakt.

De Opdrachtnemer evalueert maandelijks de gemelde incidenten en storingsmeldingen betreffende backups en treft waar nodig maatregelen.

Voor het uitvoeren van een restore van software moet toestemming worden gevraagd aan de objectbeheerder van RWS. Mogelijk moet er een stremmingsverzoek worden ingediend. Die moet twee maanden van te voren (dus voor de restore) worden aangevraagd.

N.B: Als een backup teruggezet moet worden, dan wordt deze opgevraagd bij de softwarebeheerder van RWS (de Regio).

3.12 Kluisprocedure

De software en bijbehorende documentatie dienen op een (centraal gelegen) locatie opgeslagen te worden in een brandwerende kluis. Deze kluis dient op een logische locatie binnen het areaal te staan waarbij deze 24/7 bereikbaar is maar nooit op het object zelf of in technische (computer) ruimtes. Voorbeelden zijn een nautische centrale of verkeerscentrale.

In de kluizen zit dezelfde software als in 'het beheersysteem' is opgenomen of op de netwerkschijf is opgeslagen (afhankelijk van de bestandsgrootte) op gegevensdragers. Deze gegevensdragers zijn per object opgenomen in een map, aangevuld met eventuele installatiesoftware en verdere documentatie per apparaat.

De kluis bevat per object en/of apparaat een map met gegevensdrager(s) en documentatie. De map is voorzien van locatie, objectnaam, datum en inhoudsblad.

Tijdens een calamiteit kan het noodzakelijk zijn dat een backup van de software uit de kluis nodig is om modificaties toe te passen voor het oplossen van een storing. Hiervoor moet een verzoek worden ingediend om over de backup van de software te kunnen beschikken.

De aanvrager dient een verzoek in per e-mail om uitgifte van de software uit de kluis. De softwarebeheerder volgt de normale uitgifte- en inname procedures. Hij vraagt de kluisbeheerder om toegang tot de kluis.

3.13 Kwaliteit software en documentatie

Om de kwaliteit van de dienstverlening te borgen dienen de volgende maatregelen uit te worden gevoerd:

1. Vóór opname van Software en back-up bestanden in het software archief wordt door ON gecontroleerd en opgeleverd op:
 - Uiterlijke kenmerken van de bestanden, geen 0 Kb bestand.
 - Verklaring goede werking.
 - Testprotocol en ondertekend testrapport.
 - Bewijs van acceptatie.
 - Documentatie van de software.
 - Versie/releasenr.
 - Bovengenoemde bestanden in één Zip-bestand (ingepakt).
 - Zowel de gegevensdrager als de software is gescand op malware.
2. Het bepalen van de 0-status zal gebeuren aan de hand van checklists, die tijdens de 0-inventarisatie worden opgesteld. Tijdens de beheerfase zullen de checklists worden onderhouden.
3. Halfjaarlijks wordt er een herinventarisatie uitgevoerd, waarin gecontroleerd wordt of de runtime software in overeenstemming is met de applicatiesoftware op

de op locatie aanwezige ontwikkelomgevingen en met de software in het software archief. In overleg met de beheerder zal deze update activiteit worden ingepland. Ook bij de herinventarisaties zal gewerkt worden met checklists, die dienen te worden afgetekend door de beheerder.

Per object en/of apparaat wordt een map met gegevensdrager(s) en documentatie aangelegd. De map is voorzien van voorblad met locatie, objectnaam en datum, een inhoudsblad en kent tenminste de volgende indeling:

- Voorblad met object, locatie (technische ruimte) en datum
- Inhoudsblad
- Apparatuur type model, fabricaat, serienummer(s)
- Software registratieformulier (op papier en DVD)
- Back-up van software (op DVD voorzien van dezelfde tekst als op voorblad)
- Back-up en restore procedure(s) (op papier en DVD)
- Installatiesoftware (op DVD)
- Softwarelicenties (op papier en DVD)
- Documentatie (op papier en DVD)
- Overige

Bijlage A – Lijst Begrippen en Afkortingen

Term	Beschrijving/toelichting
AM	Asset Management
Bekende fout	Zie known error
BIR	Baseline Informatiebeveiliging Rijkswaterstaat
BopA-netwerk	Het in beheer van Rijkswaterstaat Dienst CIV zijnde datanetwerk voor Bediening op Afstand.
CCTV	Closed Circuit TeleVision, Gesloten videosysteem voor inwinnen, verwerken en presenteren en opslaan van camerabeelden.
CIV	Centrale Informatievoorziening
CM	Contractmanager
CMP	Centrale Meldpunt
CS	Cybersecurity
Deelinstallatie	Onderdeel van de technische installaties van een object zoals: - 3B, bediening, besturing en bewaking -CCTV - Audio - Marifonie - Radar – Transmissie.
DH	Districtshoofd
FB	Functioneel beheerder
FIB	Functioneel installatiebeheerder. Vormt samen met de TIV'er de Installatieverantwoordelijke
HO	Hoofd Operator
IA	Industriële Automatisering
ICS	Industrial Control Systems
IMPAKT	Impulsprogramma Aanpak Kritieke Technische Infrastructuur
IV	Informatie Voorziening
IVS90 systeem	Informatie Verwerkend systeem Scheepvaart. Tot een IVS90 systeem behoort het "werkstation" met toetsenbord en muis, hetgeen wordt gebruikt als landelijk scheepvaart registratiesysteem.
KA	Kantoor Automatisering
Known error	Een known error is een probleem met een gedocumenteerde onderliggende oorzaak.
Logging	Vastlegging van systeemhandelingen (Bron: BIR)
Malware	Malware is een samentrekking van de woorden 'malicious' (Engels voor kwaadaardig) en 'software' en vormt een verzamelnaam voor schadelijke of kwaadaardige software zoals virussen, wormen en spyware.
MKO	Missie Kritieke Ondersteuning
Natte objecten	Natte objecten betreffen sluiskolken, beweegbare bruggen, stuwen, spuien, vispassages, voedingsduiker, pompgemalen, etc.
Object	Een fysiek onderdeel van het te realiseren werk, die een oplossing is voor de gedefinieerde functie(s).
OG	Opdrachtgever
OIV	Operationeel Installatie Verantwoordelijke

OMS	Onderhoudsmanagement Systeem
ON	Opdrachtnemer
OvD	Officier van Dienst
PBM	Probleemmanager
PLC	Programmable Logic Controller
PPO	Rijkswaterstaat Programma's, Projecten en Onderhoud
Probleem	(1) Een probleem is een storing waarbij het noodzakelijk is, los van de afhandeling van de storing, diepgaander op de oorzaak in te gaan of er een structurele oplossing voor te vinden. (2) Een probleem is een ongewenste situatie, die niet opgelost kan worden binnen één proces zoals storingsbeheer en die vraagt om een structurele analyse en oplossing.
Quick fix	Een wijziging die snel kan worden toegepast om een probleem op te lossen.
RWS	Rijkswaterstaat
SCADA	Supervisory Control and Data Acquisition systemen
SM	Storingsmanager
SOC	Security Operations Center (CIV)
SP	Specialist
Storing	Ongeplande onderbreking of kwaliteitsvermindering van een IA-dienst.
Systeem	Samenhangend geheel objecten die functies vervullen welke op basis van een klantbehoefte een prestatie moet leveren.
TB	Technisch beheerder
TIV	Technisch Installatie Verantwoordelijke
Trojan	Een trojan is een programma, dat naast de voorgespiegelde functionaliteit, ongemerkt en bewust een niet aan de gebruiker kenbaar gemaakte activiteit ontplooit, die mogelijk de integriteit van het geïnfecteerde systeem aantast.
Virus	Een virus is een stukje programmatuur dat zichzelf doelbewust, in al dan niet gewijzigde vorm, kan vermenigvuldigen. De nakomelingen van het virus moeten volgens deze definitie zelf ook weer virussen zijn. Voor de verspreiding is het virus afhankelijk van dragers die het virus bevatten.
VWM	Rijkswaterstaat Verkeer- en Watermanagement, Landelijk organisatieonderdeel belast met het verkeersmanagement op de (vaar)wegen.
Wijzigingsoverleg	Overleg waarin door de deelnemers besluiten worden genomen over wijzigingsverzoeken.
WM	Wijzigingsmanager
Workaround	Een wijze waarop met een probleem kan worden omgegaan terwijl er nog geen structurele oplossing is voor het probleem.
Worm	Een worm is een stukje programmatuur dat zichzelf doelbewust vermenigvuldigt. De nakomelingen van de worm zijn kopieën van het origineel en verspreiden zich door gebruik te maken van de netwerkfaciliteiten van zijn gastheer.

Bijlage B - Softwarebeheer en documentatie

Om softwarebeheer goed uit te kunnen voeren, moet een aantal zaken duidelijk zijn vastgelegd. Om overzicht te geven staan in dit hoofdstuk enkele opmerkingen ten aanzien van de verschillende documenten en registraties kort beschreven. Normaliter worden deze door de Opdrachtnemer aangeleverd of opgesteld.

NB: De aanwezigheid van duidelijke, volledige en correcte documentatie speelt tevens een belangrijke rol bij decharge van een nieuwbouwproject of als een nieuwe externe partij wordt gecontracteerd voor beheer en onderhoud van een systeem.

3.14 Softwareregistraties en Configuratie Management Database (CMDB)

De (RWS) gegevens- of softwarebeheerder (configuratiemanager) houdt een overzicht bij van alle IA-systemen en software waarbij tenminste locatie, (technische) ruimte, functie, merk, type, model, serienummer, software versienummer, licentiecodes, gebruikersnamen en eventuele netwerkgegevens (MAC en IP-adres) worden vastgelegd.

Er dient (door de Opdrachtnemer) een actuele registratie gevoerd te worden van alle IA-systemen en software.

NB: Wachtwoorden van persoonsgebonden accounts worden niet opgeslagen in registraties en mogen niet in leesbare vorm worden verstuurd via post of e-mail. Zie Procesbeschrijving Identificatie en Authenticatie voor account- en wachtwoordprocedures.

3.15 Handleidingen

In handleidingen van systemen moet duidelijk zijn uitgelegd hoe software dient te worden onderhouden, aangepast en hoe backups kunnen worden aangemaakt of teruggehaald. In handleidingen dient tevens duidelijk te worden gemaakt hoe actuele overzichten van geïnstalleerde software en versies kunnen worden verkregen.

3.16 Fysieke en technische hulpmiddelen

De volgende hulpmiddelen kunnen worden gebruikt voor beveiligd opslaan of vervoeren van software:

- CD-ROM of DVD in kluis;
- CD-ROM of DVD in verzegelde enveloppe voor transport, en/of;
- Beveiligde USB stick of externe harddisk (met AES265 encryptie) waarbij het wachtwoord in een gesloten enveloppe in een kluis op twee locaties wordt bewaard.

Daarnaast mag voor het softwarebeheer gebruik worden gemaakt van door RWS goed te keuren technische hulpmiddelen zoals een centrale repository, registratie- of softwaremanagementsysteem.

Let op dat softwaremanagementsystemen moeten zijn voorzien van sterke encryptie en een sterk toegangswachtwoord.

Bijlage C – Regio/Object specifieke details

Beschrijving en contactgegevens

Proceduredetails	Toelichting/opmerkingen/bijzonderheden
Regio	
Object(en)	
Centrale Bedienpost	Centrale bedienpost, adres, telefoonnummer, e-mail
Centrale Meldpost of regionaal Nautisch Centrum	Nautisch Centrum, adres, telefoonnummer, e-mail
Manager	Naam, functie, RWS-afdeling of bedrijfsnaam, telefoonnummer, e-mail
Beheerder	Naam, functie, RWS-afdeling of bedrijfsnaam, telefoonnummer, e-mail
Opdrachtnemer	Bedrijfsnaam en contactpersoon naam, functie, RWS-afdeling of bedrijfsnaam, telefoonnummer, e-mail
Locatie van kluis registratielijst(en)	
Syste(e)m(en)	
Account(s)	

Software opleverlijst <OBJECT/DATUM>

Systeem	Software	Versie	Omschrijving	Bestand	Identificatie (SHA265 hash)

Bijlage D – Uitgangspunten Softwarebeheer

1. Beleidsuitgangspunten

Deze procedure is van toepassing op de software van de IA-systemen en is ondergeschikt aan de *Baseline Informatiebeveiliging RWS v1.01* en de *Cybersecurity Implementatie richtlijn Objecten - RWS versie 1.01*.

De uitgangspunten zijn niet altijd implementeerbaar in IA-systemen. Afwijkingen van deze procedure en het genoemde beleid zullen altijd gedocumenteerd moeten worden en geaccordeerd door de regiomanager.

2. Besturingssoftware

De Opdrachtnemer dient zijn Onderhoudswerkzaamheden met betrekking tot het beheer van besturingssoftware (software op PLC's e.d.) zodanig te verrichten, dat geborgd wordt dat het Functioneren en Presteren van het Areaal niet in gevaar komt ten gevolge van wijzigingen of fouten in de besturingssoftware.

De Opdrachtnemer dient op alle besturingssoftware het versiebeheer uit te voeren en wijzigingen in besturingssoftware te beheersen. Het moet altijd mogelijk zijn terug te vallen op een oudere versie.

Na het aanbrengen van wijzigingen in de besturingssoftware dient de Opdrachtnemer:

1. de nieuwe versie naast de oudere versie(s) op te slaan;
2. alle wijzigingen in de software te documenteren in, voor zover van toepassing, het functioneel ontwerp, technisch ontwerp en de beheerders- en gebruikershandleidingen.

De Opdrachtnemer dient na een wijziging de betreffende besturingssoftware inclusief bijbehorende documentatie in tweevoud aan de Opdrachtgever over te dragen op een daartoe geschikte gegevensdrager.

3. Gebruik van accounts en wachtwoorden

De software moet voorzieningen hebben om het gebruik van accounts en wachtwoorden mogelijk te maken voor identificatie en authenticatie van geautoriseerde gebruikers. Zie hiervoor de procesbeschrijving *Identificatie en Authenticatie*.

4. Anti-malware

Er zijn maatregelen om verspreiding van malware en virussen tegen te gaan en daarmee schade te beperken (bijv. quarantaine en compartimentering). Alle gebruikte beheersystemen, laptops, gegevensdragers et cetera dienen te zijn voorzien van actuele antimalware en -virus maatregelen.

Zie procesbeschrijving *Malwarescanning* voor het adequaat uitvoeren van preventieve maatregelen.

5. Reservekopieën (back-ups)

Er worden niet meer kopieën van back-ups gemaakt dan strikt noodzakelijk.

Van IA-systemen zoals SCADA en PLC's worden back-ups bewaard op het lokale Engineering Station op het object indien aanwezig.

Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en fouterstel van verwerkingen.

Back-upstrategieën zijn vastgesteld op basis van de soort gegevens (bestanden, databases, enz.), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd.

Van back-up activiteiten en de archieflocatie van de media wordt een registratie bijgehouden, met een kopie op een andere locatie. De andere locatie is zodanig gekozen dat een incident/calamiteit op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie.

De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups.

6. Beveiligen van systeemdocumentatie

Systeemdokumentatie die vertrouwelijke informatie bevat is niet vrij toegankelijk.

7. Uitwisselen van media en software

Software van IA-systemen wordt – bij transport en opslag - altijd opgeslagen op beveiligde gegevensdragers welke zijn voorzien van sterke encryptie (AES265).

Indien mogelijk wordt binnenkomende programmatuur (zowel op fysieke media als gedownload) gecontroleerd op ongeautoriseerde wijzigingen aan de hand van een door de leverancier via een gescheiden kanaal geleverde checksum of certificaat.

Alleen met toestemming van RWS mag apparatuur van derden worden gekoppeld aan RWS systemen en netwerken. Alle apparatuur moet vooraf zijn gecontroleerd op malware en veilig zijn geconfigureerd (*hardening*). Beheerlaptops, USB sticks en andere draagbare media mogen niet voor andere (privé) doeleinden worden gebruikt.

8. Beheersing van operationele programmatuur

Alleen geautoriseerd personeel mag functies en software installeren of activeren.

Programmatuur behoort pas te worden geïnstalleerd op een productieomgeving na een succesvolle test en acceptatie.

Geïnstalleerde programmatuur, configuraties en documentatie worden bijgehouden in een configuratiedatabase.

Er wordt alleen door de leverancier onderhouden (versies van) software gebruikt. Van updates wordt een log bijgehouden.

De toegang tot broncode wordt zoveel mogelijk beperkt om de code tegen onbedoelde wijzigingen te beschermen. Alleen geautoriseerde personen hebben toegang.